

TQI402 Series

Wireless Access Point

TQI402

TQmI402



Management Software User's Guide

Version 6.0.1-7.1

Copyright © 2021 Allied Telesis, Inc.

All rights reserved.

This product includes software licensed under the BSD License. As such, the following language applies for those portions of the software licensed under the BSD License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Allied Telesis, Inc. nor the names of the respective companies above may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright(c) 2019 Allied Telesis, Inc.-All rights reserved. Copyright (c) [dates as appropriate to package] by The Regents of the University of California - All rights reserved. Copyright (c) 2000-2003 by Intel Corporation - All rights reserved. Copyright (c) 1997-2003, 2004 by Thomas E. Dickey <dickey@invisible-island.net> - All rights reserved. Copyright (c) 2001-2009 by Brandon Long (ClearSilver is now licensed under the New BSD License.) Copyright (c) 1984-2000 by Carnegie Mellon University - All rights reserved. Copyright (c) 2002,2003 by Matt Johnston - All rights reserved. Copyright (c) 1995 by Tatu Ylonen <ylo@cs.hut.fi> - All rights reserved. Copyright 1997-2003 by Simon Tatham. Portions copyright by Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A. Copyright (c) 1989, 1991 by Free Software Foundation, Inc. (GNU General Public License, Version 2, June 1991). Copyright (c) 2002-2005 by Jouni Malinen <jkmaline@cc.hut.fi> and contributors. Copyright (c) 1991, 1999 by Free Software Foundation, Inc. (GNU Lesser General Public License, Version 2.1, February 1999). Copyright (c) 1998-2002 by Daniel Veillard - All rights reserved. Copyright (c) 1998-2004 by The OpenSSL Project - All rights reserved. Copyright (c) 1995-1998 by Eric Young (eay@cryptsoft.com) - All rights reserved.

This product also includes software licensed under the GNU General Public License available from:

<http://www.gnu.org/licenses/gpl2.html>

Allied Telesis is committed to meeting the requirements of the open source licenses including the GNU General Public License (GPL) and will make all required source code available.

If you would like a copy of the GPL source code contained in this product, please send us a request by registered mail including a check for US\$15 to cover production and shipping costs, and a CD with the GPL code will be mailed to you.

GPL Code Request

Allied Telesis Labs (Ltd)

PO Box 8011

Christchurch, New Zealand

No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis™ and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated.

Ethernet™ is a trademark of the Xerox Corporation.

Wi-Fi®, Wi-Fi Alliance®, WMM®, Wi-Fi Protected Access® (WPA), the Wi-Fi CERTIFIED logo, the Wi-Fi logo, the Wi-Fi ZONE logo, and the Wi-Fi Protected Setup logo are registered trademarks of the Wi-Fi Alliance. Wi-Fi CERTIFIED™, Wi-Fi Multimedia™, WPA2™ and the Wi-Fi Alliance logo are trademarks of the Wi-Fi Alliance.

Microsoft is a registered trademark of Microsoft Corporation.

All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Preface	13
Safety Symbols Used in this Document	14
Contacting Allied Telesis	15
Chapter 1: Getting Started	17
Features	18
Management Tools	19
Web Browser	19
Vista Manager EX and AWC Plug-in	19
Vista Manager mini and AWC Plug-in	19
SNMPv1, v2c, and v3	20
Starting the First Management Session	21
Starting the First Management Session with a Direct Connection	22
Starting the First Management Session without a DHCP Server	22
Starting a Management Session	24
Management Windows	26
Main Menu	26
Navigation	27
Sub-menu	27
Content	27
Saving and Applying Your Changes	28
Ending Management Sessions	29
What to Configure First	30
Default Radio1 and Radio2 Settings	31
Chapter 2: Easy Setup	35
Easy Setup Window	36
Wired Settings	37
Radio1 Settings	39
Radio2 Settings	43
Administrator Settings	47
AWC Smart Cluster (AWC-SCL)	49
Planning an AWC Smart Cluster	51
Building a New Cluster or Adding Access Points to an Existing Cluster	53
Viewing the Members of Clusters	56
Viewing the Members of Clusters	56
Managing AWC Smart Clusters	58
Configuring the Radios in AWC Smart Clusters	59
Disabling AWC Smart Cluster	61
Cell Type and Single Channel Type Radio Modes	63
Chapter 3: Basic Settings	65
Assigning a Dynamic IP Address from a DHCP Server	66
Assigning a Static IP Address to the Access Point	69
Setting the Date and Time with the Network Time Protocol (NTP)	71
Manually Setting the Date and Time	74
Configuring the Web Browser Interface	76

Configuring SNMPv1, SNMPv2 and SNMPv3.....	78
Configuring SNMP Traps.....	83
Displaying the System Log.....	85
Enabling or Disabling the LEDs.....	86
Enabling or Disabling the Reset Button.....	87
Chapter 4: Web Browser Interface	89
Configuring the Web Browser Interface.....	90
Changing the Manager's Login Name and Password	92
Setting the Language of the Web Browser Interface.....	94
Chapter 5: 2.4GHz and 5GHz Radios	95
Configuring the Radios.....	96
Configuring Basic Radio Settings.....	96
Configuring Advanced Radio Settings	100
Displaying Radio Status	104
Dynamic Frequency Selection.....	107
Setting the Country Code Setting.....	108
Chapter 6: Virtual Access Points	109
VAP Introduction.....	110
VAP Guidelines	110
Configuring Basic VAP Parameters.....	111
Generating Quick Response (QR) Codes for VAPs	114
Configuring Captive Portal.....	116
Captive Portal Configurations	116
Port Numbers	117
Requiring Wireless Clients to Click the Agree Button to Access to the Network	117
Delegating a Proxy Server to Interact with Wireless Clients	120
Delegating RADIUS Servers and a Proxy Server	122
Delegating RADIUS Servers to Authenticate Wireless Clients	125
Redirecting to an External Authentication Page.....	126
Creating Pages in HTML for a Proxy Server.....	127
Requirements for the click_through_login.html and click_through_login_fail.html	127
HTML Code and Display Examples of Login Page	128
Creating Login Pages in HTML When External RADIUS is Selected	128
Requirements for the radius_login.html and radius_login_fail.html	128
HTML Code and Display Examples of Login Page	129
Configuring VAP Security	130
No Security.....	130
WPA Personal (Pre-Shared Key).....	131
WPA Enterprise.....	133
Configuring MAC Access Control Settings.....	138
Configuring Area Authentication	140
Configuring Application Proxy.....	140
Authenticating Clients with Both the On-board MAC Filter and RADIUS Server	141
Authenticating Wireless Clients with an External RADIUS Server.....	142
Configuring VAP Fast Roaming.....	146
Configuring Advanced VAP Settings	148
Configuring the MAC Address List	150
Displaying VAP and LAN Ports Statistics.....	152
Chapter 7: Quality of Service	155
Introduction to Quality of Service.....	156
Configuring QoS Basic Settings	158
Configuring AP EDCA Parameters.....	159
Configuring Station EDCA Parameters	162

Chapter 8: LAN Port	165
Configuring the Management VLAN	166
Displaying the Status of LAN Port.....	168
Chapter 9: Wireless Distribution System Bridges	171
Introduction to Wireless Distribution System Bridges	172
WDS Bridge Elements	174
Radio	174
VAP0	174
Radio Channel.....	174
Parent and Child.....	174
Security.....	175
Dynamic Frequency Selection	175
Guidelines	176
Preparing Access Points for a WDS Bridge.....	177
Chapter 10: Monitoring	179
Displaying Basic System Information.....	180
Displaying Neighboring Access Points.....	183
Displaying Associated Clients	184
Chapter 11: System Log	187
Displaying the System Log.....	188
Sending Log Messages to a Syslog Server	190
Chapter 12: Maintenance	193
Downloading the Configuration of the Access Point to Your Computer.....	194
Restoring a Configuration to the Access Point.....	196
Restoring the Default Settings to the Access Point.....	197
Uploading New Management Software to the Access Point.....	198
Rebooting the Access Point.....	200
Collecting Technical Support Information to a File.....	201

List of Figures

Figure 1: Log On Window	24
Figure 2: Sample Management Window	26
Figure 3: Main Menu Button	27
Figure 4: Easy Setup Menu Selection	36
Figure 5: Wired Settings in the Easy Setup Window	37
Figure 6: Radio1 Settings in the Easy Setup Window	39
Figure 7: Radio2 Settings in the Easy Setup Window	43
Figure 8: Administrator Settings in the Easy Setup Window	47
Figure 9: AWC-SCL Settings Window	54
Figure 10: AWC-SCL Status Window	56
Figure 11: Network DHCP Window	66
Figure 12: Network Static IP Address Window	69
Figure 13: Time Window - NTP Option.....	71
Figure 14: Daylight Savings Time Settings.....	73
Figure 15: Time Window - Manually Option	74
Figure 16: Settings System Web Window	77
Figure 17: SNMP Agent Settings Window.....	78
Figure 18: SNMP Agent Settings - Status Enabled Window	79
Figure 19: Trap Settings Window	83
Figure 20: LED Window.....	86
Figure 21: Hardware Window	87
Figure 22: Web Window	90
Figure 23: User Window	92
Figure 24: Language Window.....	94
Figure 25: Basic Radio Settings Window	96
Figure 26: Advanced Radio Settings Window	100
Figure 27: Radio Status Window	104
Figure 28: Virtual Access Point Tab	111
Figure 29: View QR Code Button	115
Figure 30: Captive Portal - Click-Through	118
Figure 31: Example of HTTP URLs of Approved Web Sites for the Walled Garden	120
Figure 32: Captive Portal - Using a Proxy Server.....	121
Figure 33: Captive Portal - External RADIUS	123
Figure 34: Captive Portal - External RADIUS.....	126
Figure 35: Captive Portal - External Page Redirect Window.....	127
Figure 36: Captive Portal - Terms of Service Page Sample.....	128
Figure 37: Captive Portal - Login Page Sample	129
Figure 38: None Selection in the VAP Security Tab.....	130
Figure 39: WPA Personal Security Tab.....	131
Figure 40: WPA Enterprise Tab.....	134
Figure 41: MAC Address Control Menu.....	138
Figure 42: External RADIUS Selection.....	143
Figure 43: External RADIUS Fields	143
Figure 44: User-Password Format Password.....	145
Figure 45: Fast Roaming Window	146

Figure 46: Advanced VAP Settings Window	148
Figure 47: MAC Address List Window	150
Figure 48: Statistics Window	152
Figure 49: QoS Window	157
Figure 50: LAN Settings Window	166
Figure 51: LAN1 Window	168
Figure 52: WDS Bridge	172
Figure 53: Example of Radio and Channel Assignments in a WDS Bridge	173
Figure 54: System Window	180
Figure 55: Neighbor AP Window	183
Figure 56: Associated Client Window	184
Figure 57: Log Window for Event Messages	189
Figure 58: Log Window for Syslog Client	190
Figure 59: Configuration Window	194
Figure 60: Upgrade Window	199
Figure 61: Reboot Window	200
Figure 62: Support Window	201

List of Tables

Table 1. AWC Smart Cluster Default Settings	31
Table 2. Radio1 (2.4GHz) Basic Default Settings	31
Table 3. Radio2 (5GHz) Basic Default Settings	32
Table 4. Wired Settings in the Easy Setup Window	37
Table 5. Radio1 Settings in the Easy Setup Window	40
Table 6. Radio2 Settings in the Easy Setup Window	44
Table 7. Administrator Settings in the Easy Setup Window	47
Table 8. AWC Smart Cluster Worksheet	52
Table 9. AWC-SCL Status Window	57
Table 10. AWC-SCL Settings Window	59
Table 11. Network DHCP Window	67
Table 12. Network Static IP Selection Window	70
Table 13. Time Window - NTP Option	72
Table 14. Time Window - Manually Option	75
Table 15. Web Window Options	77
Table 16. SNMP Agent Settings Window	80
Table 17. SNMP Trap Settings Window	84
Table 18. Web Window	91
Table 19. Basic Radio Settings Window	97
Table 20. Advanced Radio Settings Window	100
Table 21. Radio Status Window	105
Table 22. Virtual Access Point Tab	112
Table 23. Captive Portal	118
Table 24. Captive Portal - External RADIUS	123
Table 25. WPA Personal Security Tab	132
Table 26. WPA Enterprise Tab	135
Table 27. MAC Access Control Menu	139
Table 28. External RADIUS Fields	144
Table 29. Fast Roaming Window	147
Table 30. Advanced VAP Settings	148
Table 31. Statistics Window	152
Table 32. QoS Window - Basic Settings	158
Table 33. QoS Window - AP EDCA Parameters	159
Table 34. QoS Window - Station EDCA Parameters	162
Table 35. LAN Settings Window - VLAN Configuration Section	167
Table 36. LAN1 or LAN2 Window	168
Table 37. System Window	180
Table 38. Neighbor AP Window	183
Table 39. Associated Client Window	184
Table 40. Message Severity Levels	188
Table 41. Log Window for Syslog Client	191

Preface

This guide contains instructions on how to manage the features of the TQ1402 series access points with the web browser management interface.

The access point models included in this guide are:

- ❑ TQ1402
- ❑ TQm1402

This preface contains the following sections:

- ❑ “Safety Symbols Used in this Document” on page 14
- ❑ “Contacting Allied Telesis” on page 15

Safety Symbols Used in this Document

This document uses the following conventions.

Note

Notes provide additional information.



Caution

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



Warning

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



Warning

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

Contacting Allied Telesis

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

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

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

Chapter 1

Getting Started

Here are the sections in this chapter:

- ❑ “Features” on page 18
- ❑ “Management Tools” on page 19
- ❑ “Starting the First Management Session” on page 21
- ❑ “Starting a Management Session” on page 24
- ❑ “Management Windows” on page 26
- ❑ “Saving and Applying Your Changes” on page 28
- ❑ “Ending Management Sessions” on page 29
- ❑ “What to Configure First” on page 30
- ❑ “Default Radio1 and Radio2 Settings” on page 31

Features

The TQ1402 series wireless access points have the following features:

- One 2.4GHz radio
- One 5GHz radio
- Eight virtual access points per radio
- WPA Personal and WPA Enterprise with WPA, WPA2, TKIP, and CCMP authentication and encryption
- MAC address filter for wireless clients
- Multicast rate limiting
- AWC Smart Cluster
- Captive portals
- Quick Response (QR) codes for VAPs
- Band steering
- Automatic channel selection
- Adjustable transmission power
- Fast roaming
- Airtime fairness
- Quality of Service
- Wireless Distribution System (WDS) bridges
- DHCP client
- RADIUS accounting with external RADIUS server
- Network Time Protocol client
- HTTP and HTTPS web browser management
- SNMPv1 and v2c management
- Event log
- Syslog client
- LAN port: 10/100/1000Base-T Ethernet port with Power over Ethernet (PoE), Auto-Negotiation, and auto MDI/MDIX
- IEEE 802.3 (10Base-T), IEEE 802.3u (100Base-TX), and IEEE 802.3ab (1000Base-T) compliance on LAN port
- OpenFlow is *not* supported
- LLDP is *not* supported

Management Tools

The access points support the following management tools.

Web Browser

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

Note

The product has been tested with Google Chrome.

Vista Manager EX and AWC Plug-in

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

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

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

Vista Manager mini and AWC Plug-in

Vista Manager mini is useful for smaller wireless networks that may not need the capabilities of Vista Manager EX. It is a simplified version of Vista Manager EX and is standard part of the graphical user interface of selected Allied Telesis switches and routers, with AlliedWare Plus. You can use Vista Manager mini and the AWC plug-in to configure the following features on the TQ1402 series:

- Multi-channel wireless networks
- AWC Channel Blankets
- AWC Smart Connect
- Captive portals
- Hotspot 2.0 and Passpoint
- Emergency mode
- Heat maps

Vista Manager mini is available on selected Allied Telesis products, including SwitchBlade x908 GEN2, x950, x930, x550, and x530 series switches, and AR series of UTM firewalls and VPN routers.

SNMPv1, v2c, and v3

You can use SNMPv1, SNMPv2, or SNMPv3 to view the parameter settings of the devices. The MIB is available from the Allied Telesis web site. For instructions on how to configure the unit for SNMP, refer to “Configuring SNMPv1, SNMPv2 and SNMPv3” on page 78 and “Enabling or Disabling the LEDs” on page 86.

Note

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

Note

The access points do *not* support the UWC Wireless LAN Controller.

Starting the First Management Session

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

The default IP address of the access point: 192.168.1.230

If your network has a DHCP server, use the IP address the server assigns it to it to start the management session. For directions, see “Starting a Management Session” on page 24.

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

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

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

- “Starting the First Management Session with a Direct Connection” on page 22.
- “Starting the First Management Session without a DHCP Server” on page 22

Starting the First Management Session with a Direct Connection

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

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

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

3. Set the subnet mask on your computer to 255.255.255.0.
4. Power on the access point.
5. Start the web browser on your computer.
6. Enter the IP address 192.168.1.230 in the URL field of the browser and press the Enter key.

You should now see the login window, shown in Figure 1 on page 24.

7. Enter the user name and password.

- User name: manager
- Password: friend

Note

The user name and password are case-sensitive.

8. Click the Login button.

Starting the First Management Session without a DHCP Server

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

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

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

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

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

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

4. Set the subnet mask on your computer to 255.255.255.0.
5. Power on the access point by pressing on the Power button.
6. Start the web browser on your computer.
7. Enter the IP address 192.168.1.230 in the URL field of the browser and press the Return key.

You should now see the logon window, shown in Figure 1 on page 24.

8. Enter the user name and password.

- User name: manager
- Password: friend

Note

The user name and password are case-sensitive.

9. Click the Login button.

Starting a Management Session

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

Note

If the access point is using its default address 192.168.1.230, see “Starting the First Management Session” on page 21 for instructions.

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

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

Note

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

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

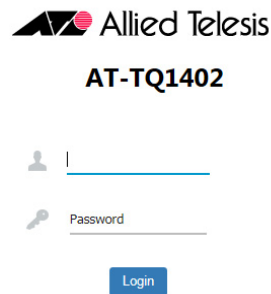


Figure 1. Log On Window

Note

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

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

The default values are:

- User name: manager
- Password: friend

Note

The user name and password are case-sensitive.

4. Click the Login button.

Management Windows

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

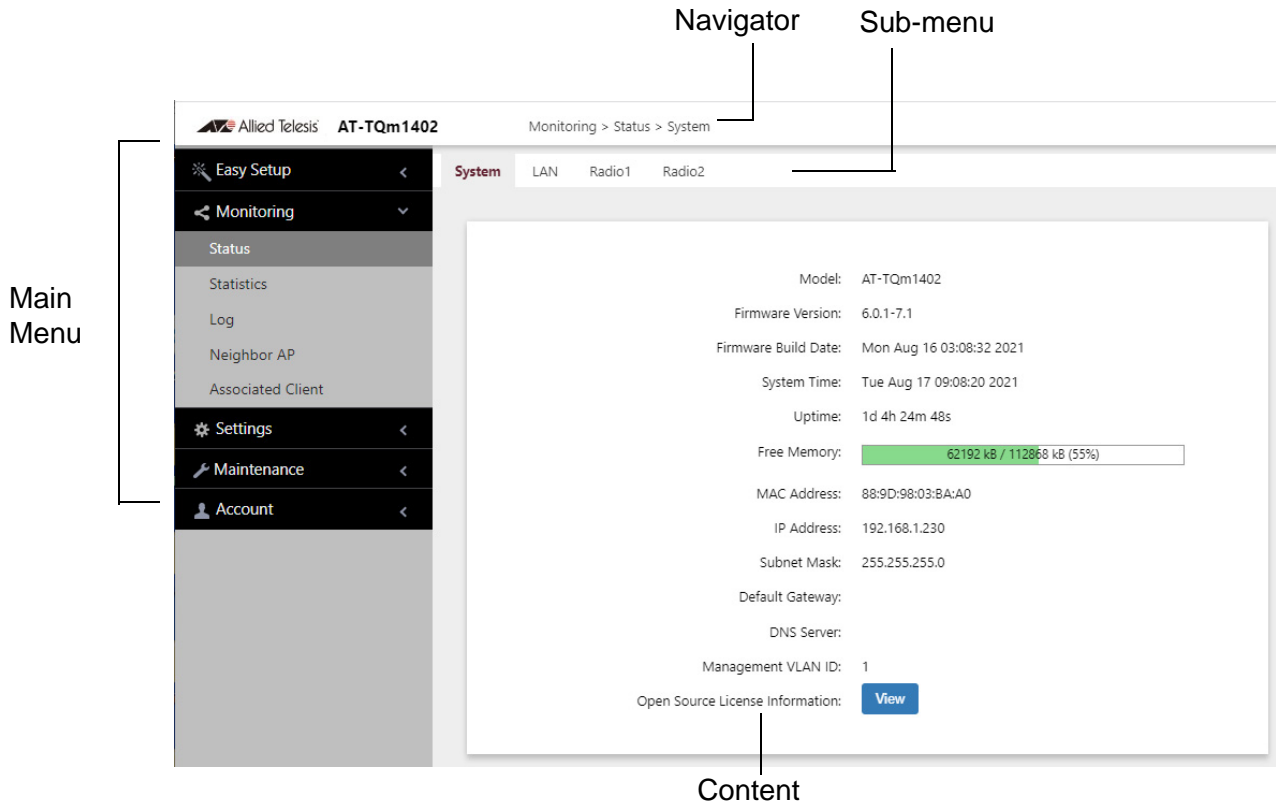


Figure 2. Sample Management Window

Main Menu

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

- Easy Setup
- Monitoring
- Settings
- Maintenance
- Account

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

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

Main Menu Button



Figure 3. Main Menu Button

- Navigation** The Navigator shows the menu path of the current window.
- Sub-menu** Sub-menus are located across the tops of many management windows.
- Content** This is the main body of the windows. It displays parameters for you to configure or status or statistics information.

Saving and Applying Your Changes

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

Ending Management Sessions

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

What to Configure First

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

1. Set the country code. Refer to “Setting the Country Code Setting” on page 108.

Note

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

Note

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

2. Change the manager’s login name and password. Refer to “Changing the Manager’s Login Name and Password” on page 92.
3. If you prefer to use HTTPS management sessions, perform “Configuring the Web Browser Interface” on page 90.
4. Set the language of the management interface to English or Japanese. The default is English. Refer to “Setting the Language of the Web Browser Interface” on page 94.

Default Radio1 and Radio2 Settings

The following tables list the v6.0.1-7.1 default settings for AWC Smart Cluster, Radio1, and Radio2. The tables apply to new units from Allied Telesis or units restored to their default settings. The tables do not apply to units upgraded to v6.0.1-7.1. They retain their previous settings.

Table 1 on page 31 lists default settings for AWC Smart Cluster on the TQ1402 access point. (The TQm1402 access point does not support AWC Smart Cluster.)

Table 1: AWC Smart Cluster Default Settings

Parameter	Setting
Status	Enabled
Cluster Name	default-cluster

For background information, refer to “AWC Smart Cluster (AWC-SCL)” on page 49.

Table 2 lists basic default settings for Radio1 (2.4GHz).

Table 2: Radio1 (2.4GHz) Basic Default Settings

Parameter	Setting
Radio	
Status	Enabled
Operational Mode	IEEE 802.11b/g/n
VAP Mode	Cell Type (not adjustable)
Channel	Auto
Bandwidth	20 MHz
Transmission Power	Max
VAP0	
Status	Enabled
Mode	Access Point
SSID	Allied- <i>nnnnnnnn</i> (Based on access point's MAC address.)
VLAN ID	1

Table 2: Radio1 (2.4GHz) Basic Default Settings (Continued)

Parameter	Setting
Security Mode	WPA Personal
WPA Version	WPA2 and WPA3
Cipher Suite	CCMP
Cipher Suite Key	(Based on access point's MAC address.)
IEEE802.11w (MFP)	Capable
VAP1 to VAP7	
Status	Disabled
Mode	Access Point
SSID	Virtual Access Point #
VLAN ID	1
Security Mode	None

Table 3 lists the basic default settings for Radio2 (5GHz)

Table 3: Radio2 (5GHz) Basic Default Settings

Parameter	Setting
Radio	
Status	Enabled
Operational Mode	IEEE 802.11a/n/ac
VAP Mode - TQ1402	Single Channel Type
VAP Mode - TQm1402	Cell Type (not adjustable)
Channel - TQ1402	36 (5180 MHz)
Channel - TQm1402	Auto
Bandwidth	20 MHz
Transmission Power	Max
VAP0	
Status	Enabled
Mode	Access Point
SSID	Allied- <i>nnnnnnnn</i> (Based on access point's MAC address.)

Table 3: Radio2 (5GHz) Basic Default Settings

Parameter	Setting
VLAN ID	1
Security Mode	WPA Personal
WPA Version	WPA2
Cipher Suite	CCMP
Cipher Suite Key	(Based on access point's MAC address.)
IEEE802.11w (MFP)	Disabled
Broadcast Key Refresh Rate	0
VAP1 to VAP7	
Status	Disabled
Mode	Access Point
SSID	Virtual Access Point #
VLAN ID	1
Security Mode	None

Chapter 2

Easy Setup

This chapter contains the following sections:

- ❑ “Easy Setup Window” on page 36
- ❑ “Wired Settings” on page 37
- ❑ “Radio1 Settings” on page 39
- ❑ “Radio2 Settings” on page 43
- ❑ “Administrator Settings” on page 47
- ❑ “AWC Smart Cluster (AWC-SCL)” on page 49
- ❑ “Planning an AWC Smart Cluster” on page 51
- ❑ “Building a New Cluster or Adding Access Points to an Existing Cluster” on page 53
- ❑ “Disabling AWC Smart Cluster” on page 61
- ❑ “Disabling AWC Smart Cluster” on page 61
- ❑ “Cell Type and Single Channel Type Radio Modes” on page 63

Easy Setup Window

Starting with version 6.0.1-2.1, the TQ1402 and TQm1402 wireless access points have an Easy Setup window for performing these basic functions:

- ❑ Assigning static or dynamic (DHCP) IPv4 addresses to access points.
- ❑ Configuring basic IEEE802.11b/g/n settings on Radio1.
- ❑ Configuring basic IEEE802.11a/n/ac settings on Radio2.
- ❑ Changing the administrator's password.

Note

The Easy Setup window is available in the on-board web browser management interface. It is not available with Vista Manager EX or Vista Manager mini and the Autonomous Wave Controller (AWC) plug-in.

The access points display the Easy Setup window as the first window at the start of your management sessions. You can also display the window by selecting Easy Setup from the main menu. Refer to Figure 4.

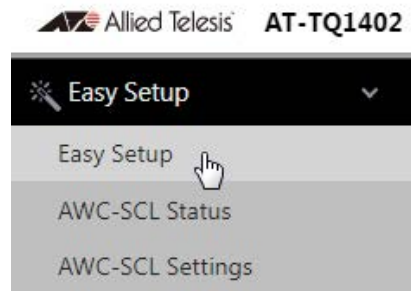


Figure 4. Easy Setup Menu Selection

The window has four sections:

- ❑ Wired Settings
- ❑ Radio1 Settings
- ❑ Radio2 Settings
- ❑ Administrator Settings

Wired Settings

The Wired Settings section is used to assign an IPv4 address to the access point. It can be a static address or a dynamic address from a DHCP server on your network. The example in Figure 5 shows the fields for a static IP address. The default is DHCP. The default address is 198.162.1.230.

Wired Settings

Connection Type	Static IP
Static IP Address	192.168.1.230
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254

Figure 5. Wired Settings in the Easy Setup Window

Note

Changing the IPv4 address of the access point will interrupt your management session. To resume managing the unit, start a new session using the access point's new IP address.

The fields are described in Table 4.

Table 4. Wired Settings in the Easy Setup Window

Field	Description
Connection Type	Select one of the following: <ul style="list-style-type: none"> - DHCP: Select this option to enable the DHCP client. The access point obtains its IPv4 address from a DHCP server on the network. This is the default setting. This selection hides the other fields. - Static IP: Select this option to enter an IPv4 address. Selecting this option displays the other fields in this table.

Table 4. Wired Settings in the Easy Setup Window (Continued)

Field	Description
Static IP Address	Enter an IPv4 address for the access point. The device can have only one address. The default is 192.168.1.230.
Subnet Mask	Enter the subnet mask for the IP address. The default is 255.255.255.0.
Default Gateway	<p>Enter the default gateway address for the unit. The default is 192.168.1.254.</p> <p>The default gateway is an IP address of an interface on a router or other Layer 3 routing device. It specifies the first hop to reaching the subnets or networks where your management devices, such as management workstations and syslog servers, reside. The access point can have only one default gateway and the network portion of the address must be the same as its IP address.</p> <p>The access point must have a default gateway address. 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 access point's IP address.</p>

Radio1 Settings

This section of the Easy Setup window is used to configure basic IEEE802.11b/g/n and WPA Personal settings on the 2.4GHz Radio1. Refer to Figure 6. You can use this section to configure Radio1 and VAP0 at the following default settings:

- Radio1 mode: IEEE802.11b/g/n
- VAP0 Status: Enabled
- VAP0 Mode: Access Point
- VAP0 Security Mode: WPA Personal
- VAP0 Security: WPA2 and WPA3
- VAP0 Cipher: CCMP
- VAP0 IEEE802.11w (MFP): Capable

Note

Configuring Radio1 and VAP0 with the Easy Setup window reverts the above parameters to the listed default settings. To configure Radio1 and VAP0 for other settings, such as IEEE802.11b/g or WPA Enterprise, use the Radio and VAP/Security selections in the main menu instead

The screenshot shows the 'Radio 1 Settings' window with the following configuration:

Setting	Value
Radio Status	Enabled
VAP Mode	Cell Type
SSID	allied-Wvi8zDM7
Key
Channel	auto
Bandwidth	20 MHz
Auto Channel Selection	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 7 <input checked="" type="checkbox"/> 8 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 10 <input checked="" type="checkbox"/> 11
Tx Power	Max

Figure 6. Radio1 Settings in the Easy Setup Window

The fields are described in Table 5 on page 40.

Table 5. Radio1 Settings in the Easy Setup Window

Field	Description
Radio Status	<p>Initial settings are different for each shipping country models. The selections in the pull-down menu are described here:</p> <ul style="list-style-type: none"> - Enabled: RoW model (can change the country). - Disabled: US/TW/JP model (cannot change the country).
VAP Mode	<p>Select the VAP mode. Radio1 has only Cell Type and does not support Single Channel Type. Radio2 has the option Single Channel Type, but it is not supported.</p> <hr/> <p>Note The TQm1402 access point does not support Single Channel Type.</p> <hr/> <p>Refer to “Cell Type and Single Channel Type Radio Modes” on page 63.</p>
SSID	<p>Enter the SSID of VAP0. The default is a unique value based on the MAC address of the access point.</p>
Key	<p>Enter the CCMP key. Here are the guidelines:</p> <ul style="list-style-type: none"> - The key can be from 8 to 63 alphanumeric characters. - It can include special characters. - It is case sensitive. - The default key is based on the MAC address of the access point. - The small double-arrow symbol next to the field toggles the key between alphanumeric characters and asterisks.

Table 5. Radio1 Settings in the Easy Setup Window (Continued)

Field	Description
Channel	<p>Select the channel for the radio from the pull-down menu. Here are the guidelines:</p> <ul style="list-style-type: none"> - You can select only one channel. - The channels vary by radio, bandwidth, and country. - Select "auto", the default setting, to have the radio select the channel automatically. The access point scans the available channels on the radio and selects the one with the least interference. - If you select Auto, you can use the Auto Channel Selection parameter in this window to restrict the channels from which the access point can choose.
Bandwidth	<p>Select the bandwidth for Radio1 from the pull-down menu. The selections for IEEE802.11b/g/n are listed here:</p> <ul style="list-style-type: none"> - 20 MHz. This is the default setting. - 40 MHz <p>The 40 MHz-wide channel allows for higher data rates, but reduces the number of available channels for other wireless devices.</p> <p>Radio1 also supports IEEE802.11b/g, but that cannot be set through the Easy Setup window. Use the Radio and VAP/Security selections in the main menu instead.</p>
Auto Channel Selection	<p>Select the channels that the radio can chose from when the Channel parameter is set to Auto. Here are the guidelines.</p> <ul style="list-style-type: none"> - A channel is enabled when its check box has a check and disabled when the check box is empty. - The available channels vary by radio, mode, bandwidth, and country. - The default is all available channels are enabled. <p>This parameter is disabled when the channel is selected manually.</p>

Table 5. Radio1 Settings in the Easy Setup Window (Continued)

Field	Description
TX Power	Select the strength of the radio transmitter. The selections are Max (maximum), High, Middle, Low, Min (minimum). The default is Max.

Radio2 Settings

This section in the Easy Setup window is used to configure basic IEEE802.11a/n/ac and WPA Personal settings on the 5GHz Radio2. Refer to Figure 7. You can use the section to configure Radio2 and VAP0 at the following default settings:

- Radio2 mode: IEEE802.11a/n/ac
- VAP0 Status: Enabled
- VAP0 Mode: Access Point
- VAP0 Security Mode: WPA Personal
- VAP0 Security (Single Channel Type): WPA2
- VAP0 Security (Cell Type): WPA2 and WPA3
- VAP0 Cipher: CCMP
- VAP0 IEEE802.11w (MFP): Capable

Note

Configuring Radio2 and VAP0 with the Easy Setup window reverts the above parameters to the listed default settings. To configure Radio2 and VAP0 for other settings, such as IEEE802.11b/g or WPA Enterprise, use the Radio and VAP/Security selections in the main menu instead.

Label	Value	Action
Radio Status	Enabled	▼
VAP Mode	Single Channel Type	▼
SSID	allied-Wvi8z0M7	
Key	🔒
Channel	36 (5180 MHz)	▼
Bandwidth	20 MHz	▼
Tx Power	Max	▼

Figure 7. Radio2 Settings in the Easy Setup Window

The fields are described in Table 6 on page 44.

Table 6. Radio2 Settings in the Easy Setup Window

Field	Description
Radio Status	<p>Initial settings are different for each shipping country models. The selections in the pull-down menu are described here:</p> <ul style="list-style-type: none"> - Enabled: RoW model (able to change the country). - Disabled: Cannot change the country model (for example, JP/US/TW)..
VAP Mode	<p>Select the VAP mode. Options are listed here:</p> <ul style="list-style-type: none"> - Single Channel Type: TQ1402 wireless access points in the AWC Smart Cluster use the same channel on Radio2. This is the default setting when AWC Smart Cluster is enabled. This setting is only available with AWC Smart Cluster. <hr/> <p>Note The TQm1402 access point does not support Single Channel Type.</p> <hr/> <ul style="list-style-type: none"> - Cell Type: TQ1402 wireless access points use different channels on Radio2. This setting is available when AWC Smart Cluster is enabled or disabled. This is the only setting when AWC Smart Cluster is disabled. <p>Refer to “Cell Type and Single Channel Type Radio Modes” on page 63.</p>
SSID	<p>Enter the SSID of VAP0. The default is a unique value based on the MAC address of the access point. If AWC Smart Cluster is enabled, the access points in the cluster all use the same VAP0 BSSID, from the access point with the highest MAC address.</p>

Table 6. Radio2 Settings in the Easy Setup Window (Continued)

Field	Description
Key	<p>Enter the CCMP key. Here are the guidelines:</p> <ul style="list-style-type: none"> - The key can be from 8 to 63 alphanumeric characters. - It can include special characters. - It is case sensitive. - The default key is based on the MAC address of the access point. - The small double-arrow symbol next to the field toggles the key between alphanumeric characters and asterisks.
Channel	<p>Select the channel for the radio from the pull-down menu. Here are the guidelines:</p> <ul style="list-style-type: none"> - You can select only one channel. - The channels vary by radio, bandwidth, and country. - The default for Radio2 for the TQ1402 access point when VAP mode is Single Channel Type is channel 36 (5180 MHz). - The default for Cell Type mode is auto. - The auto option has the radio select the channel automatically. The access point scans the available channels on the radio and selects the one with the least interference. This is the default for the TQm1402. - Do not select auto for AWC Smart Cluster on the TQ1402 access point. AWC Smart Cluster requires a specific channel. It can be any available channel. - If you select Auto, you can use the Auto Channel Selection parameter in this window to restrict the channels from which the access point can choose.

Table 6. Radio2 Settings in the Easy Setup Window (Continued)

Field	Description
Bandwidth	<p>Select the bandwidth for Radio2 from the pull-down menu. The selections for IEEE802.11a/n/ac are listed here:</p> <ul style="list-style-type: none"> - 20 MHz. This is the default setting. - 40 MHz - 80 MHz
Auto Channel Selection	<p>Select the channels that the radio can chose from when the Channel parameter is set to Auto. Here are the guidelines.</p> <ul style="list-style-type: none"> - A channel is enabled when its check box has a check and disabled when the check box is empty. - The available channels vary by radio, mode, bandwidth, and country. - The default is all available channels are enabled. - Do not use auto for AWC Smart Cluster on the TQ1402 access point. AWC Smart Cluster requires a specific channel. Select the channel in the Channel field. It can be any available channel. <p>This parameter is disabled when the channel is selected manually.</p>
TX Power	<p>Select the strength of the radio transmitter. The selections are Max (maximum), High, Middle, Low, Min (minimum). The default is Max.</p>

Note

The Easy Setup window requires that the bandwidths of the two radios be set to the default value 20MHz.

Administrator Settings

You use the bottom section of the Easy Setup window to change the password to the on-board manager account. Refer to Figure 8. The fields are described in Table 7.

Note

Do not change the default administrator name “manager”.

The screenshot shows the 'Administrator Settings' section of the Easy Setup window. It contains four input fields:

- Administrator Name:** A text field containing the word 'manager'.
- Current Password:** A password field with a green eye icon to its right.
- New Password:** A password field with a green eye icon to its right.
- Confirm New Password:** A password field with a green eye icon to its right.

Figure 8. Administrator Settings in the Easy Setup Window

Table 7. Administrator Settings in the Easy Setup Window

Field	Description
Administrator Name	Displays the current login manager name. To change the name, enter the new name. Here are the guidelines: <ul style="list-style-type: none"> - The name can be up to 12 alphanumeric characters. - The first character must be a letter. It cannot be a number or special character. - It cannot contain spaces. - The name is case-sensitive. - The default name is “manager”.
Current Password	Enter the current login password.

Table 7. Administrator Settings in the Easy Setup Window (Continued)

Field	Description
New Password	Enter the new password. Here are the guidelines: <ul style="list-style-type: none">- The password can be up to 32 alphanumeric characters.- It cannot contain spaces or special characters.- It is case-sensitive.
Confirm New Password	Reenter the new password.

AWC Smart Cluster (AWC-SCL)

AWC Smart Cluster (AWC-SCL) is a new feature in this release. It lets you manage up to five TQ1402 access points as a single unit by logically grouping them together. Configuration changes made to any one of the access points in a cluster are automatically transmitted to the other access points over the wired LAN. This simplifies management by letting you manage multiple access points as a group rather than individually. Here are the guidelines:

- ❑ AWC Smart Cluster is supported on the TQ1402 access point. It is not supported on the TQm1402 access point.
- ❑ The feature is intended for access points that are to have identical configuration settings.
- ❑ AWC Smart Cluster is configured in the Easy Setup window in the on-board web browser interface.
- ❑ The default setting for AWC Smart Cluster is enabled. Unless you disable the feature, TQ1402 access points automatically try to form clusters using their default settings as soon as you install them on your network.
- ❑ Clusters must have names. The names of different clusters in the same network have to be unique.
- ❑ Configuration changes are transmitted over the wired network on the LAN ports of the access points. This requires that the LAN ports on access points in clusters be connected to the wired network.
- ❑ You cannot use AWC Smart Cluster with Vista Manager EX or Vista Manager mini and the AWC plug-in. You have to disable Smart Clusters to use those programs to manage TQ1402 access points. Refer to “Disabling AWC Smart Cluster” on page 61.
- ❑ Clusters can have up to five access points. Clusters of six or more units are not recommended.
- ❑ Access points in a cluster must have their own individual IPv4 addresses. You can assign them manually or with a DHCP server.
- ❑ The IP addresses of access points in a cluster have to be members of the same network.
- ❑ Access points can belong to only one cluster at a time.
- ❑ A cluster's BSSID is based on the MAC address of the access point with the highest MAC address. (The web browser management interface does not display the cluster's BSSID.)

- ❑ The System LED functions are follows when AWC Smart Cluster is enabled:
 - Slow green blinking (500 ms intervals) when the access point is searching for a cluster.
 - Fast green blinking (100 ms intervals) when the access point is synchronizing its configuration with other access points in a cluster.

AWC Smart Cluster requires that Radio2 be set to the following default values:

- ❑ Mode: IEEE802.11a/n/ac
- ❑ VAP0 Status: Enabled
- ❑ VAP0 Mode: Access Point
- ❑ VAP0 Security Mode: WPA Personal
- ❑ VAP0 Security: WPA2
- ❑ VAP0 Cipher: CCMP
- ❑ VAP0 IEEE802.11w (MFP): Capable

When AWC Smart Cluster is enabled, you should only use the Easy Setup window to configure Radio1 and Radio2.

TQ1402 access points in an AWC Smart Cluster share the same configuration settings, except for these settings:

- ❑ Host names
- ❑ MAC addresses
- ❑ IP addresses
- ❑ SNMP system names, system contacts, and system locations
- ❑ Channel and transmission powers when the VAP operating mode of Radio2 is Cell Type
- ❑ Transmission powers when the VAP operating mode of Radio2 is Single Channel Type

Planning an AWC Smart Cluster

Here are factors to consider when planning the AWC Smart Cluster of TQ1402 access points:

- ❑ How many access points will be in the cluster? The recommended maximum is five access points.
- ❑ What will be the cluster's name? The name has to be the same on all the access points. The default name is "default-cluster". The name is case-sensitive. Different clusters on the same network must have unique names.
- ❑ What will be the IPv4 addresses of the TQ1402 access points? Each access point has to have a unique IP address and the addresses have to be part of the same network. The addresses can be assigned manually or from a DHCP server.
- ❑ What will be the Administrator password? The password has to be the same on all access points. The default is "friend". The password is case-sensitive.
- ❑ Will the VAP mode on Radio2 on the access points be Cell Type or Single Channel Type? The default is Single Channel Type. Refer to "Cell Type and Single Channel Type Radio Modes" on page 63.

Here are additional factors to consider if the VAP operating mode on Radio2 will be Single Channel Type:

- ❑ What will be the common Radio2 channel of the access points in the AWC Smart Cluster? The default is channel 36 (5180 MHz).
- ❑ Is your wireless network already using channel 36? If so, you need to change its channel or the channel on Radio2 on the TQ1402 access points.
- ❑ Which TQ1402 access point in the cluster has the highest MAC address? The BSSID of the common 5GHz wireless network of the cluster will be based on its MAC address. The MAC addresses of the access points are on labels on the side rear panels. They can also be viewed in the Status -> System window in the on-board web browser management interface.

The worksheet in Table 8 on page 52 is provided to assist you in planning and managing AWC Smart Clusters. You should copy and fill it out for each cluster.

Table 8: AWC Smart Cluster Worksheet

Variable	Value
Smart Cluster Name	
VAP Mode on 5GHz Radio2: Cell Type or Single Channel Type (Default: single Channel Type)	
Common Radio2 Channel for Single Channel Type (Default: channel 36 (5180 MHz))	
#1 TQm1402 Access Point	
Location	
Static or DHCP IP Address	
MAC Address	
#2 TQm1402 Access Point	
Location	
Static or DHCP IP Address	
MAC Address	
#3 TQm1402 Access Point	
Location	
Static or DHCP IP Address	
MAC Address	
#4 TQm1402 Access Point	
Location	
Static or DHCP IP Address	
MAC Address	
#5 TQm1402 Access Point	
Location	
Static or DHCP IP Address	
MAC Address	

Building a New Cluster or Adding Access Points to an Existing Cluster

Check the following on new access points before building a new cluster or adding access points to an existing cluster:

- Do they have firmware version 6.0.1-7.1 or later? (menu selections: Monitoring > Status > System)
- Do they have the same firmware version? The access points of a cluster must have the same firmware version.
- Are their parameters at the default settings? (menu selections: Maintenance > Configuration > Factory Default)
- Is there an existing wireless network that is already using channel 36 (5180 MHz)? If so, you will need to change the channel on that network or on Radio2 on the TQ1402 access points.

Adding new access points to an existing cluster does not change the configuration settings of the cluster. The only exception is possibly the BSSID. If the cluster is set to Single Channel Type, the BSSID will change if the MAC address of the new access point is higher than the addresses of the other access points.

To build a new AWC Smart Cluster or add access points to an existing cluster, do the following:

1. Connect the LAN port on the new access point to your wired LAN.
2. Start a management session on the access point.

Note

To restore the default settings, perform steps 3 and 4. Otherwise, go to step 5.

3. Select **Maintenance > Configuration > Factory Default** to restore the factory default settings.
4. Wait one minute and then start a new management session.
5. Select **Easy Setup** from the main menu. This is the default selection.
6. In the Wired Settings section of the window, assign an IP address to the access point. The IP address has to be part of the same network as the other access points in the cluster. You can assign the address manually or from a DHCP server. The default is DHCP.
7. In the Radio2 Settings section, select **Single Channel Type** or **Cell Type** from the VAP Mode pull-down menu. The default is Single

Channel Type. Refer to “Cell Type and Single Channel Type Radio Modes” on page 63.

8. In the Administrator Settings section at the bottom of the Easy Setup window, change the Administrator password. Refer to “Administrator Settings” on page 47. The access points in the cluster should all have the same password. The password is case-sensitive. The default is “friend”.
9. Select **Easy Setup > AWC-SCL Settings** from the main menu. Refer to Figure 9.

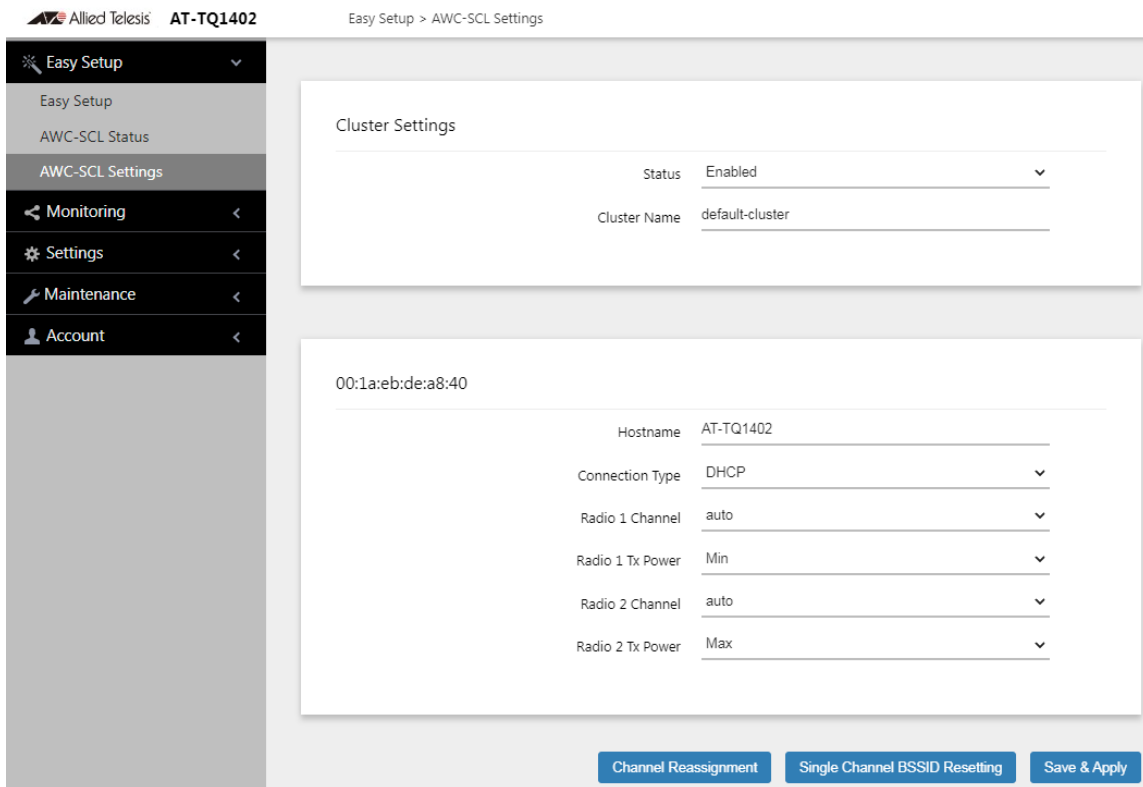


Figure 9. AWC-SCL Settings Window

10. In the Cluster Settings section, enter the **Cluster Name**. If you are adding an access point to a cluster, enter the name of the existing cluster. The name is case-sensitive.
11. In the Cluster Settings section, set the **Status** of Smart Cluster to **Enabled**. This is the default setting.
12. Click the **Save and Apply** button.

The access point searches for other access points on the wired network with the same Cluster Name and, if found, becomes a member by adopting their settings. If there is no cluster yet, it continues searching.

13. If Radio2 VAP0 mode is set to Single Channel Type, click the **Single Channel BSSID Resetting** button In the AWC-SCL Settings window. This step ensures that the BSSID of the cluster is based on the access point with the largest MAC address.
14. Select **Account > Logout** to end the management session.
15. Repeat this procedure to add more access points to the cluster.

Viewing the Members of Clusters

Viewing the Members of Clusters

To view the members of a cluster, go to **Easy Setup > AWC-SCL Status**. Refer to Figure 10.

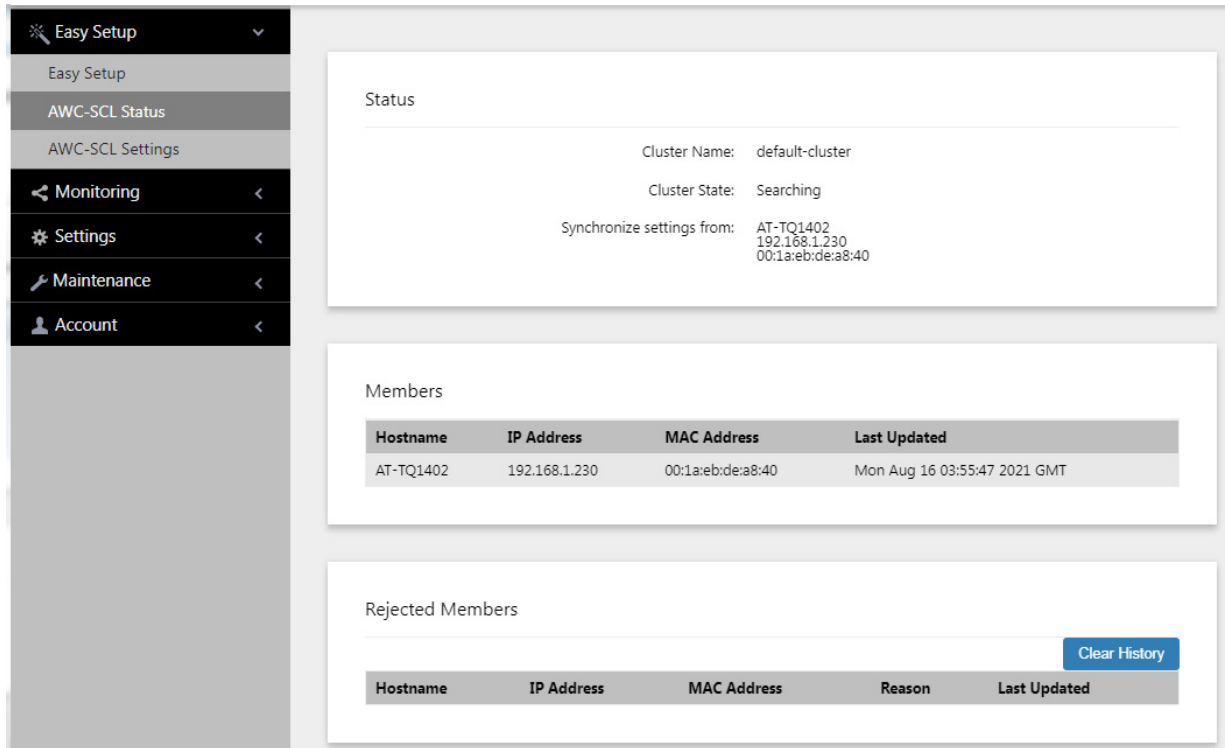


Figure 10. AWC-SCL Status Window

The sections in the window are described in Table 9.

Table 9. AWC-SCL Status Window

Section	Description
Status	Displays the following information: <ul style="list-style-type: none"> - Cluster name - Cluster State: This can be Searching, indicating the access point has not yet joined a cluster, or Constructed, meaning it has joined a cluster. - Synchronize Settings from: Displays the hostname, IP address, and MAC address of the access point in the cluster to which this access point is synchronizing its settings.
Members	Lists the access points of the cluster.
Rejected Members	Lists access points that tried to join the cluster but were rejected. Possible reasons include: <ul style="list-style-type: none"> - The cluster has already reached its maximum number of five access points. - The new access point has a different firmware version. - The new access point has a different country code.

Managing AWC Smart Clusters

To view or configure the settings of the TQ1402 access points in an AWC Smart Cluster, do the following:

1. Using your web browser, log on to any TQ1402 access point in the cluster.
2. Make the desired configuration changes to the access point. Your changes are transmitted to the other access points in the cluster over the wired LAN when you click the **Save & Apply** buttons.
3. When you are finished, log out from the access point by selecting **Account > Logout**.

Configuring the Radios in AWC Smart Clusters

You can change basic Radio1 and Radio2 settings of the access points in a cluster from the AWC-SCL Settings window. To display the window, select **Easy Setup > AWC-SCL Settings**. Refer to Figure 9 on page 54. The fields are described in Table 10.

Table 10. AWC-SCL Settings Window

Field	Description
Hostname	Use this field to change the hostname of the access point where you started the management session on the cluster.
Connection Type	Use this field to change the IPv4 address of the access point where you started the management session. The options are: <ul style="list-style-type: none"> - DHCP: Assign the IP address from a DHCP server on your network. This is the default. - Static: Assign a static address to the access point. For instructions, refer to Table 4 on page 37.
Radio1 Channel	Use this field to change the Radio1 channel. Options are listed here: <ul style="list-style-type: none"> - Option 1: Changes the Radio1 channel only on the access point where you started the management session. From the pull-down menu, select either a static channel or Auto to have the access point search for an unused channel, and click the Save & Apply button. - Option 2: Changes the Radio1 channels on all the access points in the cluster. From the pull-down menu, select Auto and click the Channel Reassignment button. (Do not select a static channel.) Access points that detect interference on their Radio1 channels search for unused channels.

Table 10. AWC-SCL Settings Window

Field	Description
Radio2 Channel	<p>Use this field to change the Radio2 channel when VAP0 mode is Cell Type. It changes the Radio2 channel only on the access point where you started the management session. From the pull-down menu, select a static channel or Auto to have the access point search for an unused channel. Then click the Save & Apply button.</p> <p>To change the Radio2 channels on the access points in a cluster when VAP0 mode is Single Channel Type, use the Easy Setup window. A cluster requires a static channel. Do not select Auto. Assign the same static Radio2 channel to all the access points in the cluster.</p>

Disabling AWC Smart Cluster

The default setting for AWC Smart Cluster on the TQ1402 access point is enabled. You can disable the feature if you do not want to use it or to remove access points from clusters. Afterwards, you can manage access points with the on-board web browser interface or Vista Manager EX or Vista Manager mini and the AWC plug-in.

1. Start a management session on the access point with your web browser.
2. Select **AWC-SCL Settings** from the main menu. The AWC-SCL Settings window is shown in Figure 9 on page 54.
3. In the Clusters Settings section of the window, select **Disabled** from the Status pull-down menu.
4. Click the **Save & Apply** button.

The access point displays the prompt in Figure 11 if Radio2 is set to Single Channel Type. As explained in “Cell Type and Single Channel Type Radio Modes” on page 63, Single Channel Type is only supported with AWC Smart Cluster. The prompt is alerting you that disabling AWC Smart Cluster also disables Single Channel Type on Radio2 and changes the radio's mode to Cell Type.

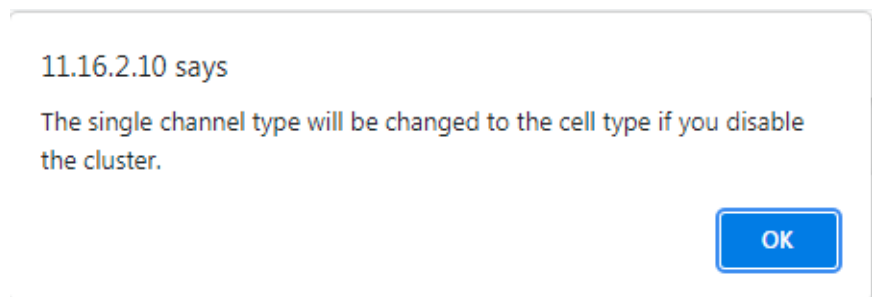


Figure 11. Disabling AWC Smart Cluster Prompt

5. Click the **OK** button.

The access point disables AWC Smart Cluster on Radio2. The access point is no longer a member of a cluster.

Note

Continue with the next step if the cluster is using Single Channel Type and you removed an access point from the cluster.

6. Start a management session on one of the remaining access points in the cluster.
7. Select **Easy Setup > AWC-SCL Settings** from the main menu.
8. Click the **Single Channel BSSID Resetting** button. This step ensures that the cluster's BSSID is from the access point with the largest MAC address.
9. Click the **Save & Apply** button.

Cell Type and Single Channel Type Radio Modes

The standard practice when building wireless networks is to assign radios in access points to different channels when their signals overlap. This is to avoid radio interference. Overlapping signals from access points using different channels are often needed in network environments to ensure that wireless networks adequately cover all physical work areas. Wireless networks that use multiple channels work best for stationary clients who remain connected to the same wireless access points at all times. This mode of operation is called Cell Type on Radio1 and Radio2 on the TQ1402 and TQm1402 access points.

Wireless networks of multiple channels, however, can pose problems for roaming clients. Packets can be lost as clients change channels as they transition between access points. Roaming clients may also experience slow traffic if, instead of transitioning, they remain connected to their original access points after moving a distance away.

The 5GHz Radio2 radio on the TQ1402 access point has a second mode called Single Channel Type. This mode is available when access points are in an AWC Smart Cluster. The mode allows access points in clusters to use the same 5GHz channel even when their signals overlap. This avoids the need for roaming clients to change channels when they transition between access points, thereby reducing the chance of lost packets. Single Channel Type can also reduce the need for complex channel planning.

Here are the Single Channel Type guidelines:

- ❑ Single Channel Type is supported on Radio2 on the TQ1402 access point. It is the default setting. The default channel is 36 (5180 MHz).
- ❑ Radio1 does not support Single Channel Type. It supports Cell Type only.
- ❑ Single Channel Type requires AWC Smart Cluster.
- ❑ The TQm1402 access point does not support Smart Cluster or Single Channel Type. Its radios support Cell Type only.
- ❑ You set the Radio2 VAP mode in the Easy Setup window.
- ❑ When using Single Channel Type, you must use the Easy Setup window to make changes to Radio2 and VAP0 settings.

Refer to “AWC Smart Cluster (AWC-SCL)” on page 49 for information and instructions on how to build clusters of TQ1402 access points with the Cell Type or Single Channel Type VAP mode.

Chapter 3

Basic Settings

This chapter contains the following procedures:

- ❑ “Assigning a Dynamic IP Address from a DHCP Server” on page 66
- ❑ “Assigning a Static IP Address to the Access Point” on page 69
- ❑ “Setting the Date and Time with the Network Time Protocol (NTP)” on page 71
- ❑ “Manually Setting the Date and Time” on page 74
- ❑ “Configuring the Web Browser Interface” on page 76
- ❑ “Configuring SNMPv1, SNMPv2 and SNMPv3” on page 78
- ❑ “Configuring SNMP Traps” on page 83
- ❑ “Displaying the System Log” on page 85
- ❑ “Enabling or Disabling the LEDs” on page 86
- ❑ “Enabling or Disabling the Reset Button” on page 87

Assigning a Dynamic IP Address from a DHCP Server

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

If your network does not have a DHCP server or you prefer to manually assign it an IP address, refer to “Assigning a Static IP Address to the Access Point” on page 69.

Note

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

Note

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

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

1. Select **Settings** > **System** from the main menu.
2. Select **Network** from the sub-menu.
3. Select **DHCP** from the Connection Type pull-down menu. The options in the window change. Refer to Figure 12 on page 66.

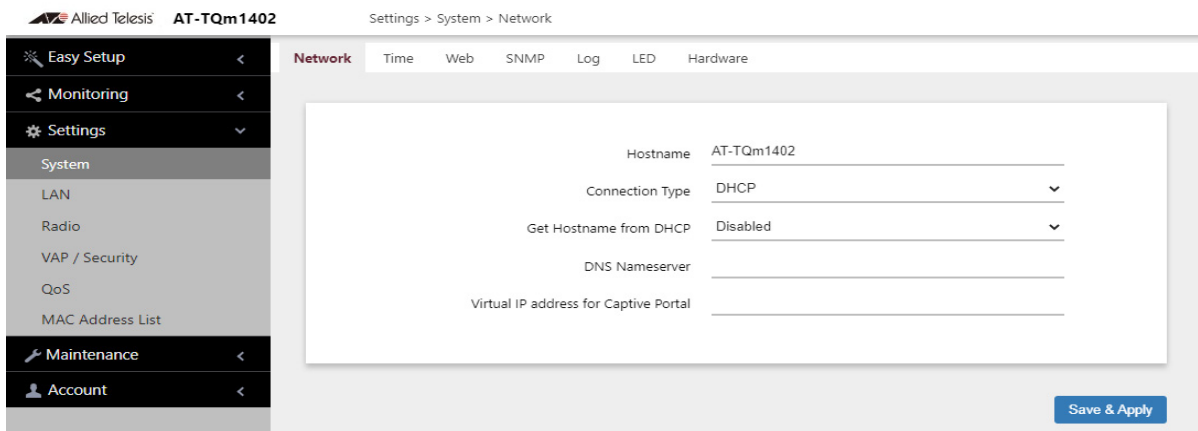


Figure 12. Network DHCP Window

4. Configure the fields by referring to Table 11.

Table 11. Network DHCP Window

Parameter	Description
Hostname	<p>Enter a hostname for the access point. Here are the guidelines:</p> <ul style="list-style-type: none"> - The hostname can be from 1 to 63 alphanumeric characters. - The hostname cannot contain spaces or any special characters, except hyphens. - The first or last character cannot be a hyphen. - The access point can have only one hostname. - The default is AT-TQ1402 or AT-TQm1402. - If you want the DHCP server to supply the hostname, enable the Get Hostname from DHCP Server option in this window.
Connection Type	<p>Select DHCP. This is the default. The Static IP selection is explained in "Assigning a Static IP Address to the Access Point" on page 69.</p>
Get hostname from DHCP	<p>Select one of the following options:</p> <ul style="list-style-type: none"> - Enabled: When the DHCP server assigns an IP address to the access point, the server assigns a host name as well. - Disabled: The DHCP server does not change the hostname of the access point. This is the default setting.
DNS Nameserver	<p>Enter the IP address of the DNS server. If this field is left blank, the access point tries to obtain the address from the DHCP server. The default is no name.</p>

Table 11. Network DHCP Window (Continued)

Parameter	Description
Virtual IP Address for Captive Portal	<hr/> <p>Note Not supported on TQ1402 v6.0.1-7.1.</p> <hr/> <p>Assigns a virtual IP address to the wireless access point. Wireless clients use the virtual address instead of the device’s actual IP address to log on to captive portals. This increases the security of your wireless network by hiding the device’s IP address. The device supports one virtual IP address.</p> <hr/> <p>Note This option is not supported with Wireless Distribution System (WDS) bridges.</p> <hr/> <p>This field is optional. The default is no name.</p>

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

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

Assigning a Static IP Address to the Access Point

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

If you prefer the access point obtain its IP configuration from a DHCP server on your network, refer to “Assigning a Dynamic IP Address from a DHCP Server” on page 66.

Note

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

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

1. Select **Settings** > **System** from the main menu.
2. Select **Network** from the sub-menu.
3. Select **Static IP** from the Connection Type pull-down menu. The options in the window change. Refer to Figure 13.

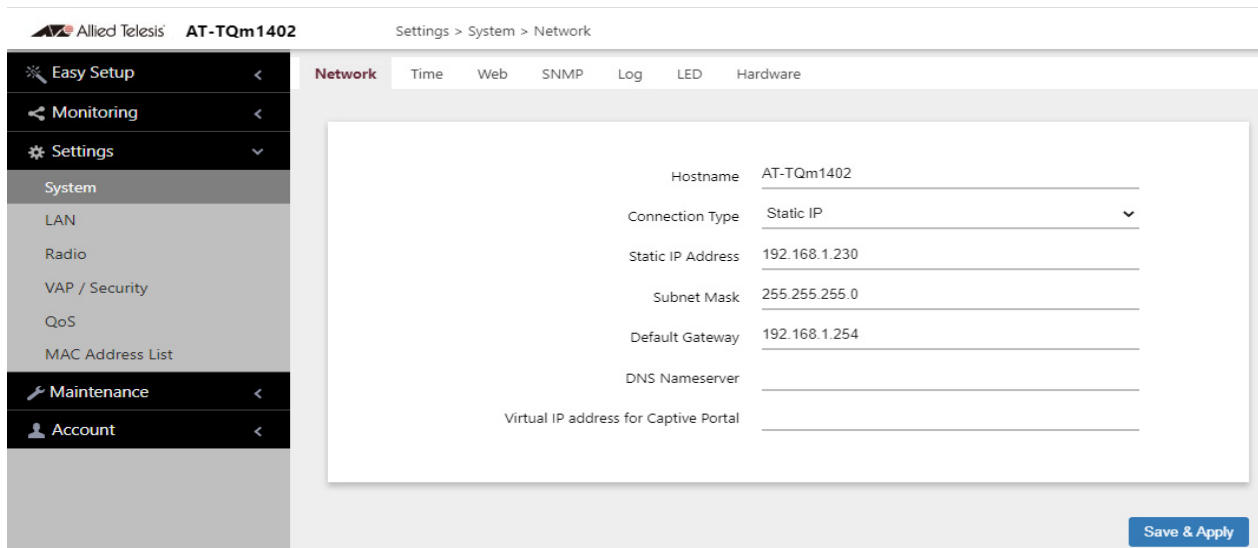


Figure 13. Network Static IP Address Window

4. Configure the field values by referring to Table 12.

Table 12. Network Static IP Selection Window

Item Name	Description
Host Name	Enter a host name for the access point. Here are the guidelines: <ul style="list-style-type: none"> - The host name can be from 1 to 63 alphanumeric characters. - The hostname cannot contain spaces or any special characters, except hyphens. - The first or last character cannot be a hyphen. - The access point can have only one hostname. - The default is AT-TQ1402 or AT-TQm1402.
Connection Type	Select Static IP .
Static IP Address	Enter the new IP address for the access point. The device can have only one IP address. The default is 192.168.1.230.
Subnet Mask	Enter the subnet mask for the IP address. The default is 255.255.255.0.
Default Gateway	Enter the default gateway address for the unit. The default value is 192.168.1.254.
DNS Nameserver	Specify the Domain Name Service (DNS) server address. This field is optional. The default is no name.
Virtual IP Address for Captive Portal	Not supported on TQ1402 v6.0.1-7.1.

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

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

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

Here are the guidelines to using the client:

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

To configure the NTP client, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **Time** from the sub-menu. Refer to Figure 16 on page 74.
3. From the Set System Time pull-down menu, select **Using Network Time Protocol (NTP)**. The window is updated with new options. Refer to Figure 14.

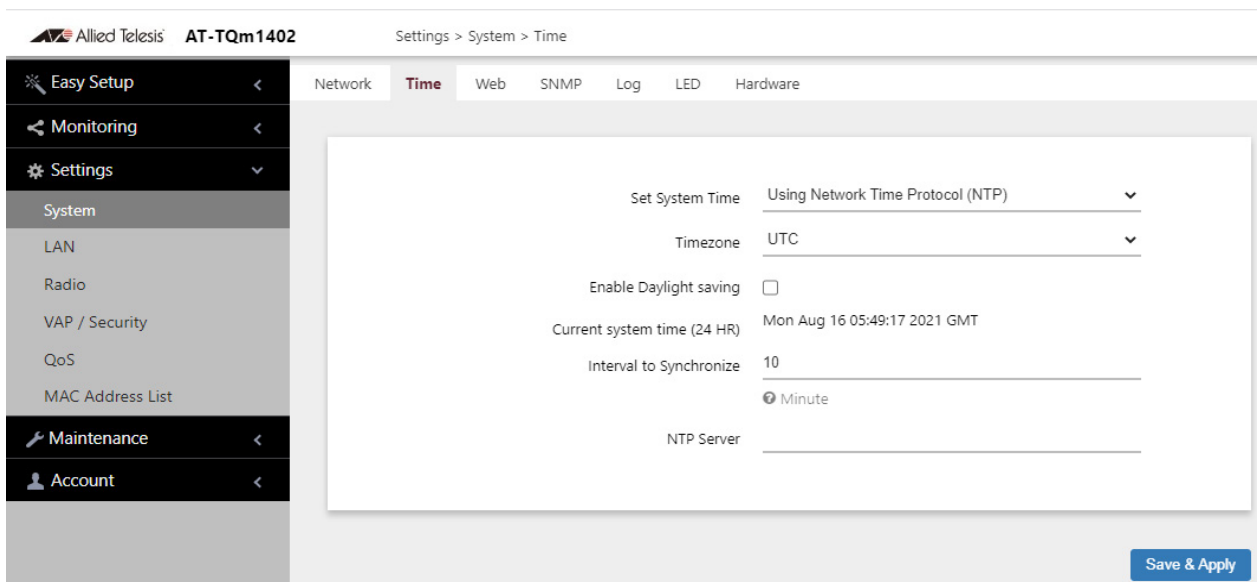


Figure 14. Time Window - NTP Option

4. Configure the fields by referring to Table 13.

Table 13. Time Window - NTP Option

Item Name	Description
Set System Time	Select Using Network Time Protocol (NTP) to synchronize the date and time of the product with the NTP server. The factory default is Manually.
Timezone	Use this pull-down menu to set the time zone of the location of the access point. If the SNTP server is providing Coordinated Universal Time (UTC), the access point uses the time zone parameter to determine its UTC offset, which is the number of hours its location is ahead or behind UTC. It adjusts the time accordingly.
Enable Daylight Saving	If the location of the access point observes daylight savings time, click the check box for this option. The window displays the fields in Figure 15 on page 73. If the area does not observe Daylight Savings time, leave the check box empty.
Start (Daylight Saving)	Use the pull-down menus to set the date and time for the start of Daylight Savings Time.
End (Daylight Saving)	Use the pull-down menus to set the date and time for the end of Daylight Savings Time.
Offset (Daylight Saving)	Use the pull-down menu to select the number of minutes to adjust the time at the start and end Daylight Saving Time. The default is 60 minutes.
Current System Time (24 HR)	Displays the date and time of the access point.
Interval to Synchronize	Enter the interval in minutes at which the access point synchronizes its time with the SNTP server. The range is 1 to 9999 minutes. The default is 10 minutes.

Table 13. Time Window - NTP Option (Continued)

Item Name	Description
NTP Server	<p>Specify the SNTP server using one of the following methods:</p> <ul style="list-style-type: none"> - IP address (example, 12.34.56.78) - Fully qualified domain name (FQDN) (example, ntp.mydomain.com) <p>Here are the guidelines:</p> <ul style="list-style-type: none"> - You can specify only one server. - The first character must be a letter or number. It cannot be a special character. - The last character cannot be a hyphen or period. - The factory default is no server. <p>Observe these guidelines when using an FQDN to identify the server:</p> <ul style="list-style-type: none"> - It cannot start or end with a hyphen. - Domain labels can have a maximum of 63 characters. - An FQDN can have up to 253 characters.

Figure 15 contains the settings for Daylight Savings Time.

Enable Daylight saving

	Month	Week		Hour	Minute
Start	3 ▼	2s ▼	Sunday ▼	2 ▼	0 ▼
	Month	Week		Hour	Minute
End	11 ▼	1s ▼	Sunday ▼	2 ▼	0 ▼
Offset [min]	60				▼

Figure 15. Daylight Savings Time Settings

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

Manually Setting the Date and Time

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

Note

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

Note

Allied Telesis recommends using a NTP server to set the date and time. For instructions, refer to “Setting the Date and Time with the Network Time Protocol (NTP)” on page 71.

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

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

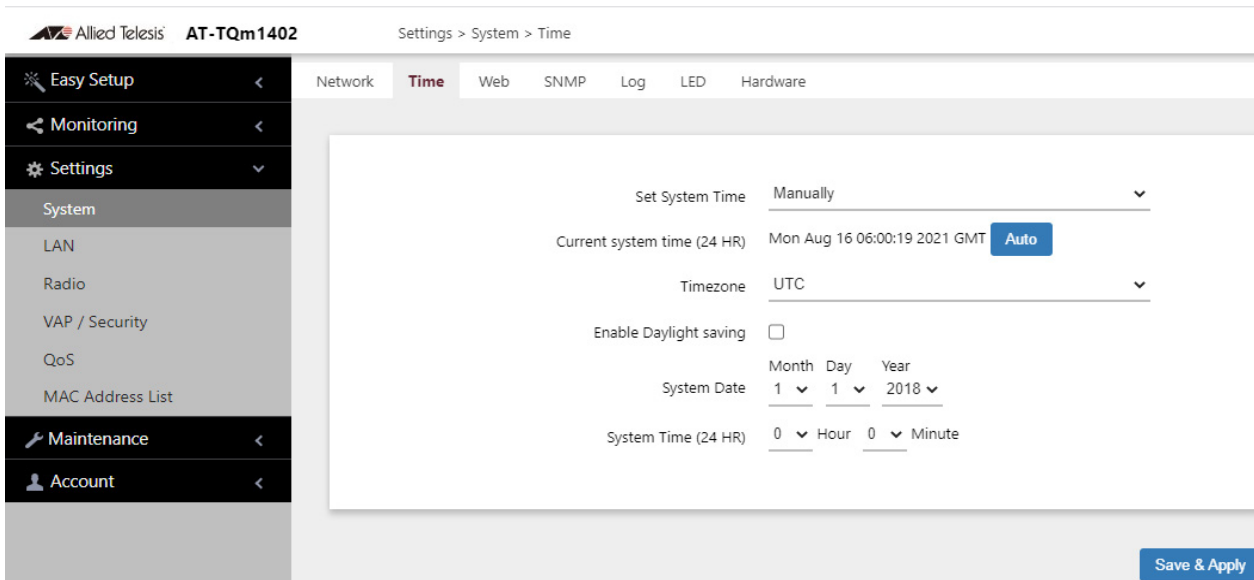


Figure 16. Time Window - Manually Option

3. Configure the parameters by referring to Table 14.

Table 14. Time Window - Manually Option

Field	Description
Set System Time	Select Manually . This is the default.
Current System Time (24 HR)	Displays the current date and time settings. Click the AUTO button to set the date and time on the access point according to your management workstation.
Timezone	Select the Time Zone of the access point from the pull-down menu.
Enable Daylight Savings	If the location of the access point observes daylight savings time, click the dialog box for the Adjust Time for Daylight Savings parameter. The window displays the fields in Figure 15 on page 73 If the area does not observe Daylight Savings time, leave the check box empty.
Start (Daylight Saving)	Use the pull-down menus to set the date and time for the start of Daylight Savings Time.
End (Daylight Saving)	Use the pull-down menus to set the date and time for the end of Daylight Savings Time.
Offset (Daylight Saving)	Use the pull-down menu to select the number of minutes to adjust the time at the start and end Daylight Saving Time. The default is 60 minutes.
System Date	Use the pull-down menus to set the current month, day, and year.
System Time (24 HR)	Use the pull-down menus to set the current hours and minutes. The hours are in 24 hours. For example, 14 represent 2:00 p.m.

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

Configuring the Web Browser Interface

This section has the following management functions:

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

Note

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

Note

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

To configure the above functions, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **Web** from the sub-menu. This is the default tab. Refer to Figure 17.

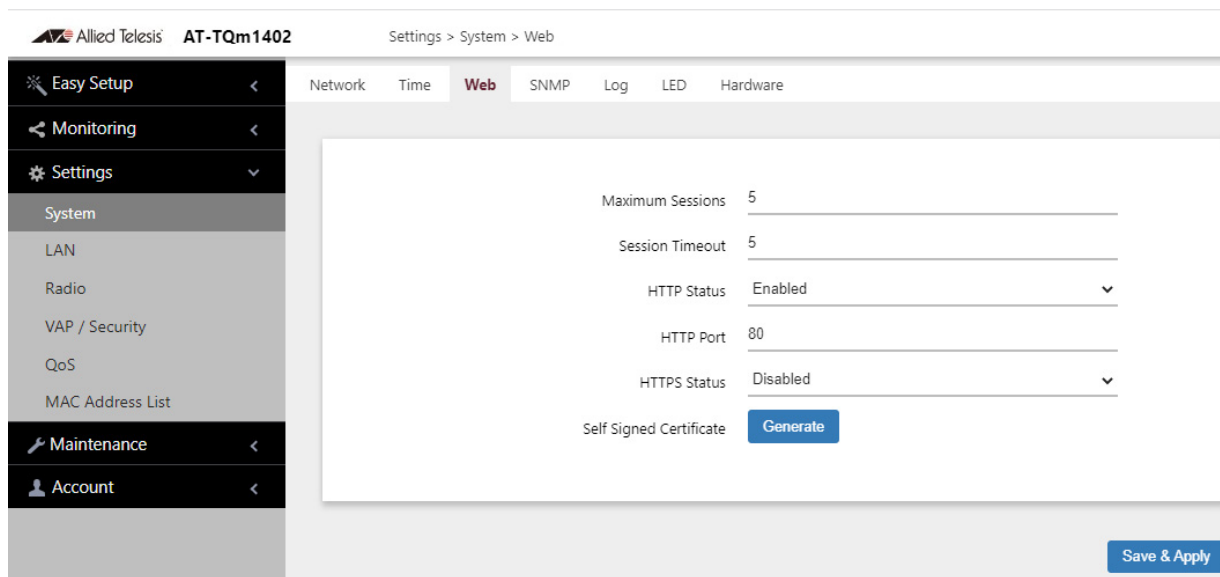


Figure 17. Settings System Web Window

- Configure the parameters by referring to Table 15.

Table 15. Web Window Options

Field	Description
Maximum Session	Specify the maximum number of active management sessions the access point will support at one time. Here are the guidelines: <ul style="list-style-type: none"> - The range is 1 to 10 sessions. - The number of sessions is the sum of HTTP and HTTPS connections. - The default is five sessions. - The access point blocks new management session after reaching the maximum number of sessions.
Session Timeout	Specify the time interval in minutes after which the access point automatically ends inactive sessions. The range is 1 to 1440 minutes (1440 minutes = 1 day). The default is 5 minutes.
HTTP Status	Enable or disable HTTP management the default is enabled.
HTTP Port	Specify the port number of the HTTP server. The range is 0 to 65535. The default is 80.
HTTPS Status	Enable or disable HTTPS management. The default is disabled. The HTTPS server uses port 443. It cannot be changed.
Self Signed Certificate	Generate a self-signed certificate for HTTPS management. The access point comes with a certificate, but you can generate a new one with the option. The new certificated automatically replaces to old certificate.

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

Configuring SNMPv1, SNMPv2 and SNMPv3

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

- ❑ You cannot use SNMP to change the settings on the access point.
- ❑ SNMPv3 requires firmware version 6.0.1-1.1 or later.
- ❑ The access point has one read-only community string.
- ❑ The unit must have an IP address for SNMP management. For instructions, refer to “Assigning a Static IP Address to the Access Point” on page 69 or “Assigning a Dynamic IP Address from a DHCP Server” on page 66.

To enable or disable SNMP, perform the following procedure:

1. Select **Settings** > **System** from the main menu.
2. Select **SNMP** from the sub-menu.
3. Click the **Agent Settings** tab. This is the default tab. Refer to Figure 18.

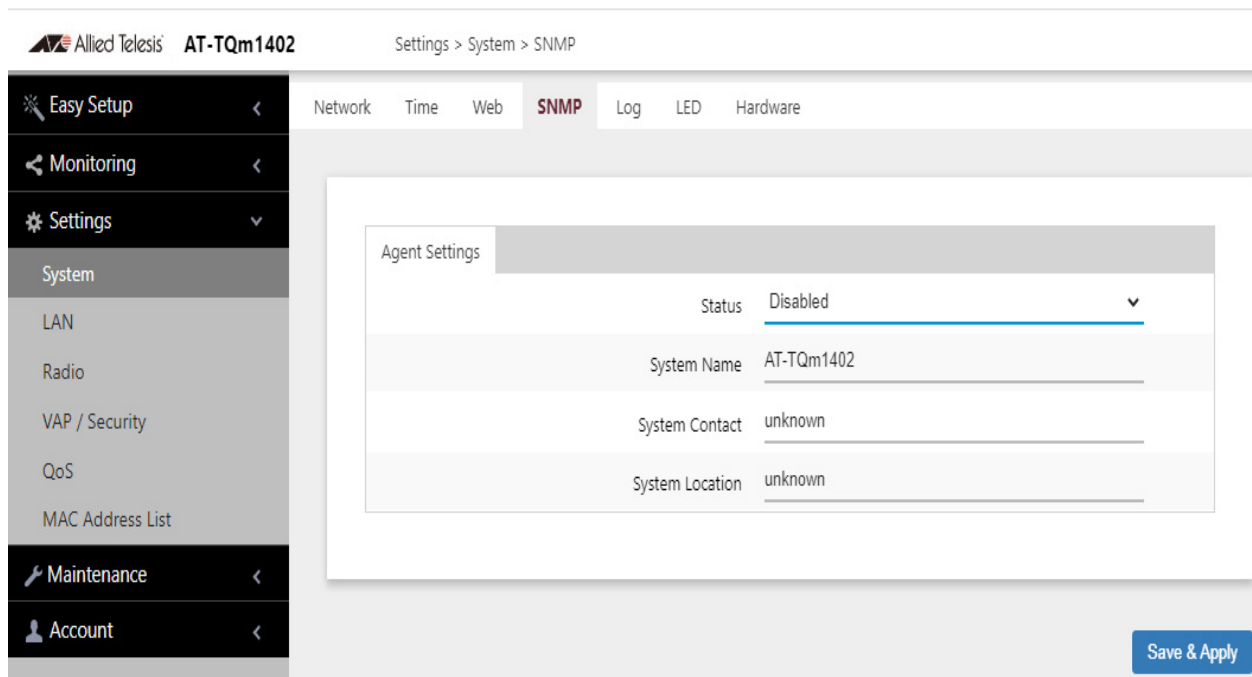


Figure 18. SNMP Agent Settings Window

4. Configure the fields by referring to Table 16 on page 80.

Note

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

Settings > System > SNMP

Network Time Web **SNMP** Log LED Hardware

Agent Settings Trap Settings

Status	Enabled
Version	v1/v2c
Read-only Community Name	public
Port	161
Restrict the source of SNMP requests	Disabled
System Name	AT-TQm1402
System Contact	unknown
System Location	unknown

Save & Apply

Figure 19. SNMP Agent Settings - Status Enabled Window

- Configure the fields by referring to Table 16 on page 80.

Table 16. SNMP Agent Settings Window

Field	Description
Status	<p>Use this option to activate or deactivate the SNMP agent on the access point. The options are explained here:</p> <ul style="list-style-type: none"> - Enabled: Select this option to activate the SNMP agent and trap settings. This allows you to use SNMP to view the parameter settings on the access point. It also allows the access point to send traps. You have to enable SNMP to configure the settings in this window and the Trap Settings window. - Disabled: Select this option to disable SNMP and the trap settings. This is the default setting.
Version	<p>Use this option to select the SNMP version.</p> <ul style="list-style-type: none"> - v1/v2c: SNMPv1,v2c - v3: SNMPv3
Read-only Community Name	<p>Use this option to specify the read-only community string for the access point. The community string is used to view the MIB settings of the device. Here are the guidelines:</p> <ul style="list-style-type: none"> - The community string can be from 1 to 256 alphanumeric characters. - The community string cannot contain any spaces. - The community string is case sensitive. - You can specify only one read-only community string. - You can not leave the field empty. - The default read-only community string is "public". - The community string cannot contain any of the following symbols: "" (Double quote), quote),
Port	<p>Use this parameter to specify the port number for SNMP. The range is 1 to 65535. The default is 161.</p>

Table 16. SNMP Agent Settings Window (Continued)

Field	Description
Restrict the Source of SNMP Requests	<p>Use this option to increase the security of the access point by restricting the use of SNMP to specific subnets or individual workstations. The options are described here:</p> <ul style="list-style-type: none"> - Enabled: Check this option to restrict the use of SNMP on the access point to only those management stations specified in the next field in the window. - Disabled: Check this option to disable this feature and permit any workstation to use the community string to view the unit. This is the default setting.
Only allow from the designated hosts or subnets	<p>Use this field to identify the management workstations permitted to use SNMP to view the device. This field only applies if you select the Enabled option in the previous field. Here are the guidelines:</p> <ul style="list-style-type: none"> - You can specify only one value in the field. - You can specify a specific workstation by its IP address (for example, 149.23.45.102). - You can specify a subnet by including the subnet mask (for example, 67.101.4.0/24). - You can specify a workstation by its FQDN. - The default is blank. <p>Observe these guidelines when using an FQDN to identify the workstation:</p> <ul style="list-style-type: none"> - It cannot start or end with a hyphen. - Domain labels can have a maximum of 63 characters. - An FQDN can have up to 253 characters.
System Name	Specify the SNMP system name of the access point. The default is TQ1402 or TQm1402.
System Contact	Specify the system administrator name. The system contact can be up to 64 alphanumeric characters. The default is unknown.

Table 16. SNMP Agent Settings Window (Continued)

Field	Description
System Location	Enter the location of the device. It can be up to 64 alphanumeric characters. The default is unknown.

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

Configuring SNMP Traps

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

1. Select **Settings > System** from the main menu.
2. Select **SNMP** from the sub-menu.
3. Click the **Trap Settings** tab. Refer to Figure 20.

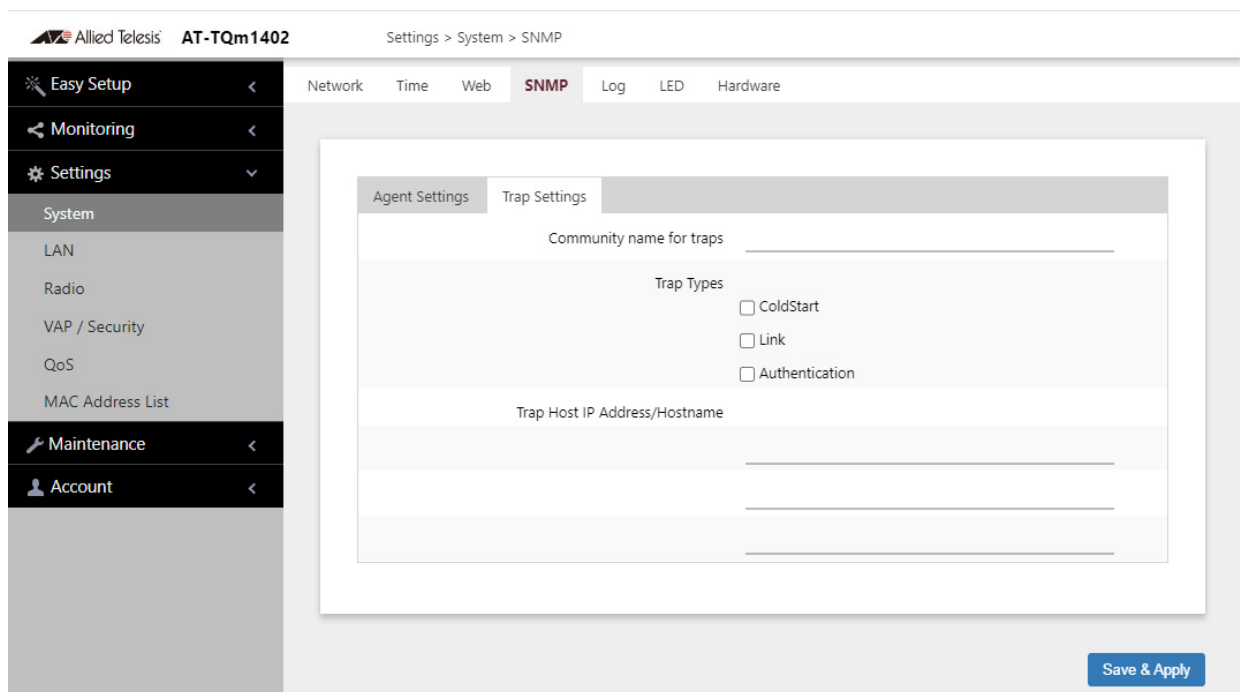


Figure 20. Trap Settings Window

Note

The Status parameter has to be set to Enabled in the Agent Settings tab before the Trap Settings tab is available and you can configure the parameters in this window. SRefer to “Configuring SNMPv1, SNMPv2 and SNMPv3” on page 78.

4. Configure the fields by referring to Table 17 on page 84.

Table 17. SNMP Trap Settings Window

Parameter	Description
Community Name for Traps	<p>Use this field to specify the community name the access point is to use to transmit traps. Here are the guidelines:</p> <ul style="list-style-type: none"> - The community name can be from 1 to 256 alphanumeric characters. - The default is blank. - The name cannot contain any of the following characters: "" (Double quote),
Trap Types	<p>Select radio button for the trap type you want to generate:</p> <ul style="list-style-type: none"> - Cold Start: This trap is sent when the SNMP agent started. - Link: This trap is sent when a radio enabled or disabled. - Authentication: This trap is sent when an SNMP authentication fails
Trap Host IP Address / Hostname	<p>Specify the SNMP hosts to receive the traps. Here are the guidelines:</p> <ul style="list-style-type: none"> - You can specify up to three hosts. - The hosts can be identified by IP addresses or hostnames. - The default is blank. <p>Observe these guidelines when using an FQDN to identify a host:</p> <ul style="list-style-type: none"> - It cannot start or end with a hyphen. - Domain labels can have a maximum of 63 characters. - An FQDN can have up to 253 characters.

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

Displaying the System Log

See Chapter 11, "System Log" on page 187.

Enabling or Disabling the LEDs

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

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

1. Select **Settings > System** in the main menu.
2. Select **LED** in the sub-menu. Refer to Figure 21.

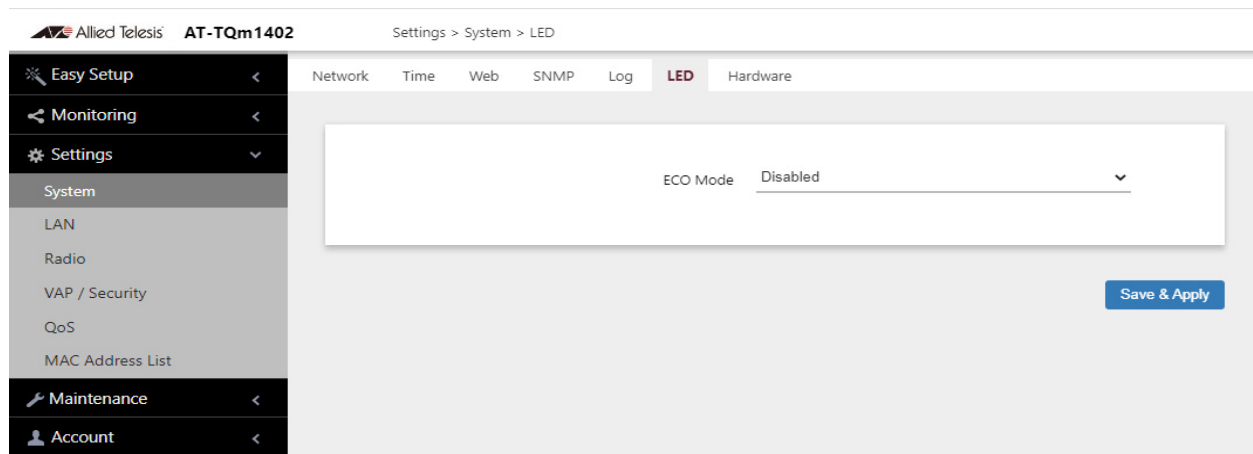


Figure 21. LED Window

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

Enabling or Disabling the Reset Button

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

By default, the reset 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, be sure not to forget the manager account password. Otherwise, you will not be able to manage the unit with the web browser interface.

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

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

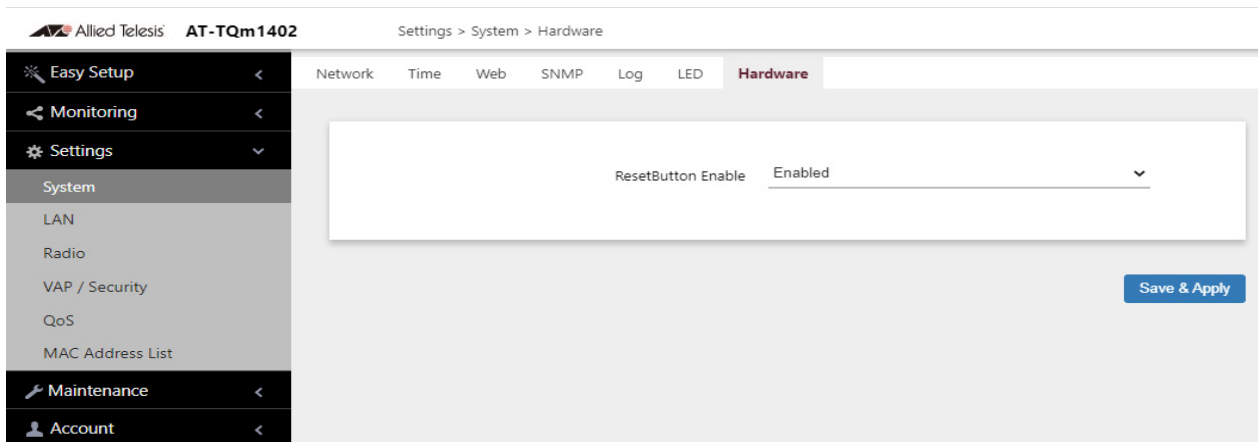


Figure 22. Hardware Window

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

Chapter 4

Web Browser Interface

This chapter contains the following procedures:

- ❑ “Configuring the Web Browser Interface” on page 90
- ❑ “Changing the Manager’s Login Name and Password” on page 92
- ❑ “Setting the Language of the Web Browser Interface” on page 94

Configuring the Web Browser Interface

This section has the following management functions:

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

Note

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

Note

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

To configure the above functions, perform the following procedure:

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

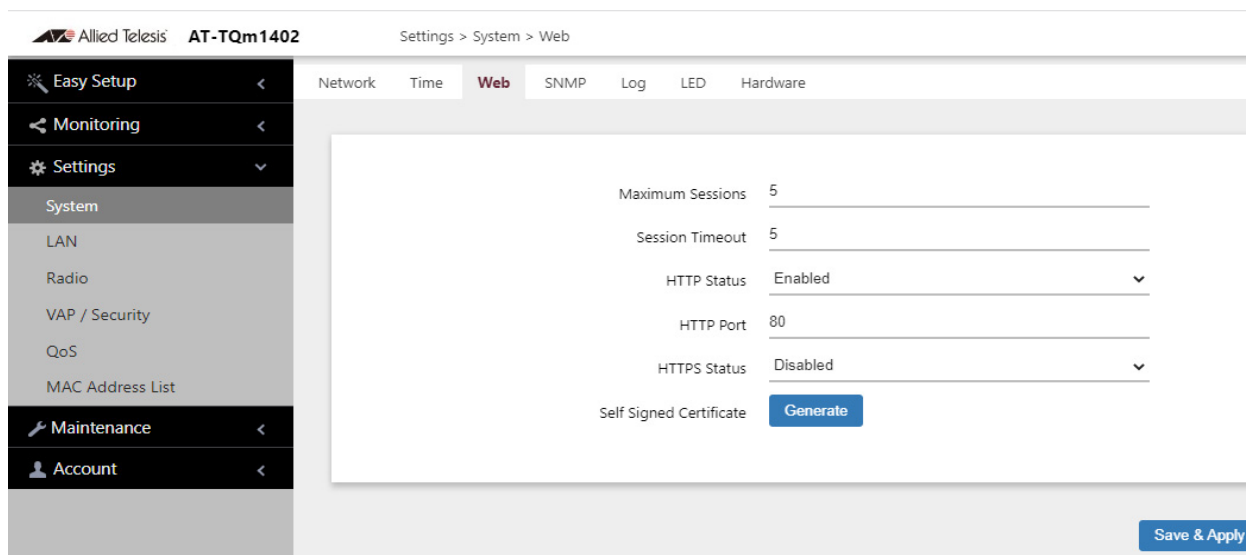


Figure 23. Web Window

3. Configure the fields by referring to Table 18.

Table 18. Web Window

Field	Description
Maximum Sessions	Specify the maximum number of active management sessions the access point will support at one time. Here are the guidelines: <ul style="list-style-type: none"> - The range is 1 to 10 sessions. - The number of sessions is the sum of HTTP and HTTPS connections. - The default is five sessions. - The access point blocks new management session after reaching the maximum number of sessions.
Session Timeout	Specify the time interval in minutes after which the access point automatically ends inactive sessions. The range is 1 to 1440 minutes (1440 minutes = 1 day). The default is five minutes.
HTTP Status	Enable or disable HTTP management. The default is enabled.
HTTP Port	Specify the port number of the HTTP server. The range is 0 to 65535. The default is 80.
HTTPS Status	Enable or disable HTTPS management. The default is disabled. The HTTPS server uses port 443. It cannot be changed.
Self Signed Certificate	Generate a self-signed certificate for HTTPS management. The access point comes with a certificate, but you can generate a new one with this option. The new certificate automatically replaces the old certificate.

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

Note

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

Changing the Manager's Login Name and Password

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

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

Note

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

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

1. Select **Account > User** from the main menu. Refer to Figure 24.

The screenshot shows the web interface for an Allied Telesis AT-TQm1402 device. The breadcrumb navigation at the top indicates 'Account > User'. On the left, a dark sidebar menu contains options: Easy Setup, Monitoring, Settings, Maintenance, and Account (which is expanded to show 'User', 'Language', and 'Logout'). The main content area is a light gray box containing a form with four input fields: 'Administrator Name' (with 'manager' entered), 'Current Password', 'New Password', and 'Confirm New Password'. Each password field has a green eye icon to its right. A blue 'Save & Apply' button is located at the bottom right of the form area.

Figure 24. User Window

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

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

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

4. Select the **New Password** field and enter a new password. The new password. Here are the guidelines:
 - The password can be up to 32 alphanumeric characters.
 - It can not contain spaces or any of these special characters: " , \$, : , < , > , ' , & , * .
 - It is case-sensitive.
5. Select the **Confirm New Password** field and enter the new password again.
6. Click the **SAVE & APPLY** button to save and update the configuration. You must use the new manager name and password in all future management sessions.

Setting the Language of the Web Browser Interface

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

1. Select **Account > Language** from the main menu. Refer to Figure 25.

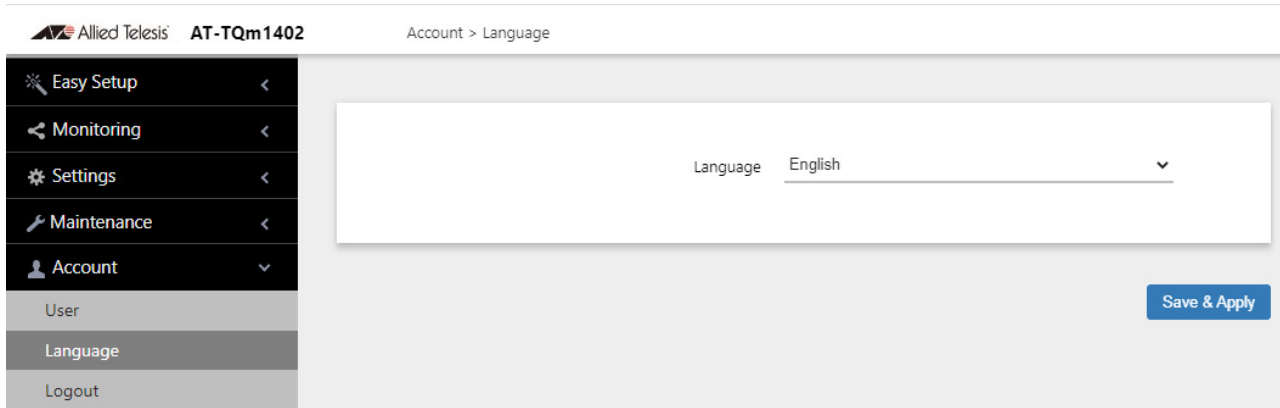


Figure 25. Language Window

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

Chapter 5

2.4GHz and 5GHz Radios

This chapter has the following procedures:

- ❑ “Configuring the Radios” on page 96
- ❑ “Displaying Radio Status” on page 104
- ❑ “Dynamic Frequency Selection” on page 107
- ❑ “Setting the Country Code Setting” on page 108

Configuring the Radios

The radio settings are divided into two groups:

- ❑ “Configuring Basic Radio Settings” next
- ❑ “Configuring Advanced Radio Settings” on page 100

Configuring Basic Radio Settings

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

1. Select **Settings > Radio**.
2. Select **Radio1** or **Radio2** from the sub-menu. You can configure only one radio at a time.
3. Click the **Basic Settings** tab shown in Figure 26. This is the default tab.

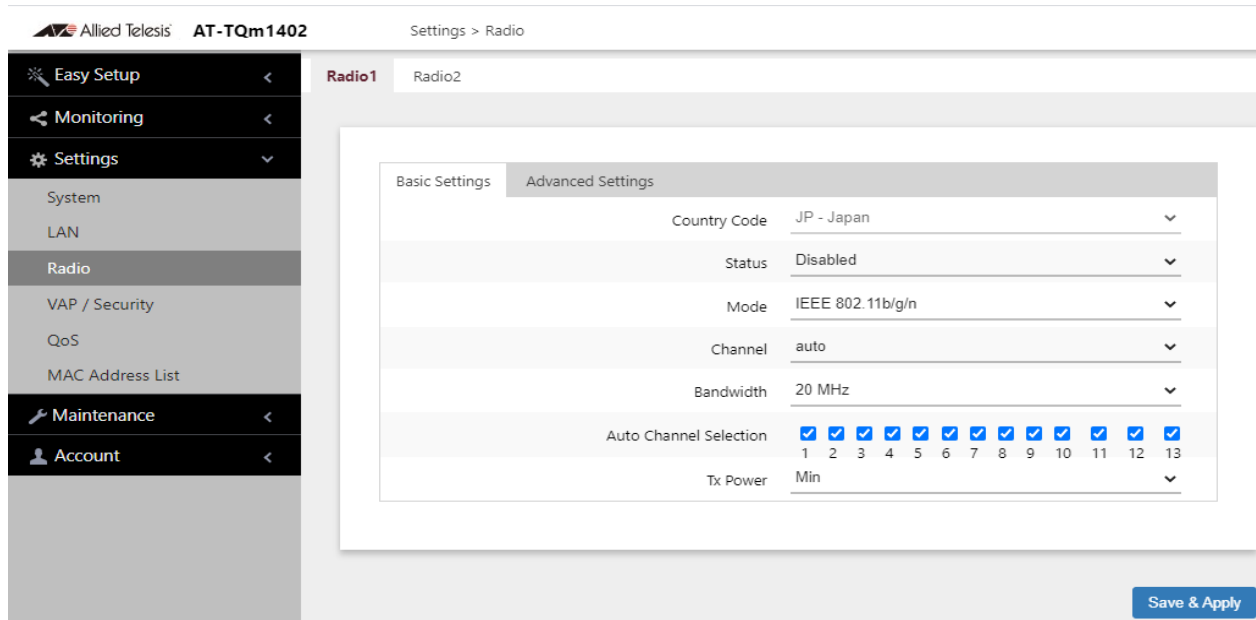


Figure 26. Basic Radio Settings Window

4. Configure the settings by referring to Table 19 on page 97.

Table 19. Basic Radio Settings Window

Field	Description
Country Code	<p>Select the country code that applies to your country or region. The country code ensures that the device operates in compliance with the codes and regulations of your region or country.</p> <hr/> <p>Note You cannot change the country code on units sold in North America, Japan, or Taiwan.</p> <hr/> <p>Here are the guidelines:</p> <ul style="list-style-type: none"> - You can select only one country. - The Country Code parameter is shown in the Basic Settings windows of all three radios but it can only be set from Radio1. - The same country code applies to all three radios. - Changing the country code disables the radios. - You have to reconfigure the radio settings if you change the country code.
Status	<p>Activate or deactivate the radio. The selections in the pull-down menu are described here:</p> <ul style="list-style-type: none"> - Enabled: Activates the radio. This is the default setting. - Disabled: Deactivates the radio.
Mode (Radio1)	<p>Select the communications protocol for Radio1 from the pull-down menu. The selections are listed here:</p> <ul style="list-style-type: none"> - IEEE 802.11b/g: The access point accepts only 802.11b or 802.11g clients. - IEEE 802.11b/g/n: The access point accepts 802.11b, 802.11g, or 802.11n clients operating at 2.4GHz. This is the default for Radio1.

Table 19. Basic Radio Settings Window (Continued)

Field	Description
Mode (Radio2)	<p>Select the communications protocol for Radio2 from the pull-down menu. The selections are listed here:</p> <ul style="list-style-type: none"> - IEEE 802.11a: The access point accepts 802.11a clients. - IEEE 802.11a/n/ac: The access point accepts 802.11a, 802.11n, and 802.11ac clients operating. This is the default setting for Radio2. <p>Wi-Fi multimedia (WMM) has to be enabled (default) to use IEEE 802.11n or IEEE 802.11ac. Refer to “Configuring QoS Basic Settings” on page 158.</p>
Channel	<p>Select the channel for the radio from the pull-down menu. Here are the guidelines:</p> <ul style="list-style-type: none"> - You can select only one channel. - The channels vary by radio, bandwidth, and country. - Select "auto", the default setting, to have the radio select the channel automatically. The access point scans the available channels on the radio and selects the one with the least interference. - If you select Auto, you can use the Auto Channel Selection parameter in this window to restrict the channels from which the access point can choose. - You must set the channel manually when using the Wireless Distribution System (WDS) bridge feature. For information, refer to “WDS Bridge Elements” on page 174. - To view the current active channel, refer to “Displaying Radio Status” on page 104.

Table 19. Basic Radio Settings Window (Continued)

Field	Description
Bandwidth (Radio1)	<p>Select the bandwidth for Radio1 from the pull-down menu. The selections for IEEE 802.11n are listed here:</p> <ul style="list-style-type: none"> - 20 MHz. This is the default setting. - 40 MHz <p>For IEEE 802.11n modes, channel width can be 40 MHz-wide or the legacy 20 MHz-wide. The 40 MHz-wide channel allows for higher data rates, but reduces the number of available channels for other wireless devices.</p> <p>The only bandwidth for IEEE 802.11b/g is 20 MHz.</p>
Bandwidth (Radio2)	<p>Select the bandwidth for Radio2 from the pull-down menu. The available bandwidths for IEEE 802.11n/ac are listed here:</p> <ul style="list-style-type: none"> - 20 MHz. This is the default setting. - 40 MHz - 80 MHz <p>The only bandwidth for IEEE 802.11a is 20 MHz.</p>
Auto Channel Selection	<p>Select the channels that the radio can chose from when the Channel parameter is set to Auto. Here are the guidelines.</p> <ul style="list-style-type: none"> - A channel is enabled when its check box has a check and disabled when the check box is empty. - The available channels vary by radio, mode, bandwidth, and country. - The default is all available channels are enabled. - This parameter is disabled when the channel is selected manually.
Tx Power	<p>Select the strength of the radio transmitter. The selections are Max (maximum), High, Middle, Low, Min (minimum). The default is Max.</p>

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

Configuring Advanced Radio Settings

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

1. Select **Settings** > **Radio** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. You can configure only one radio at a time.
3. Click the **Advanced Settings** tab. See Figure 27.

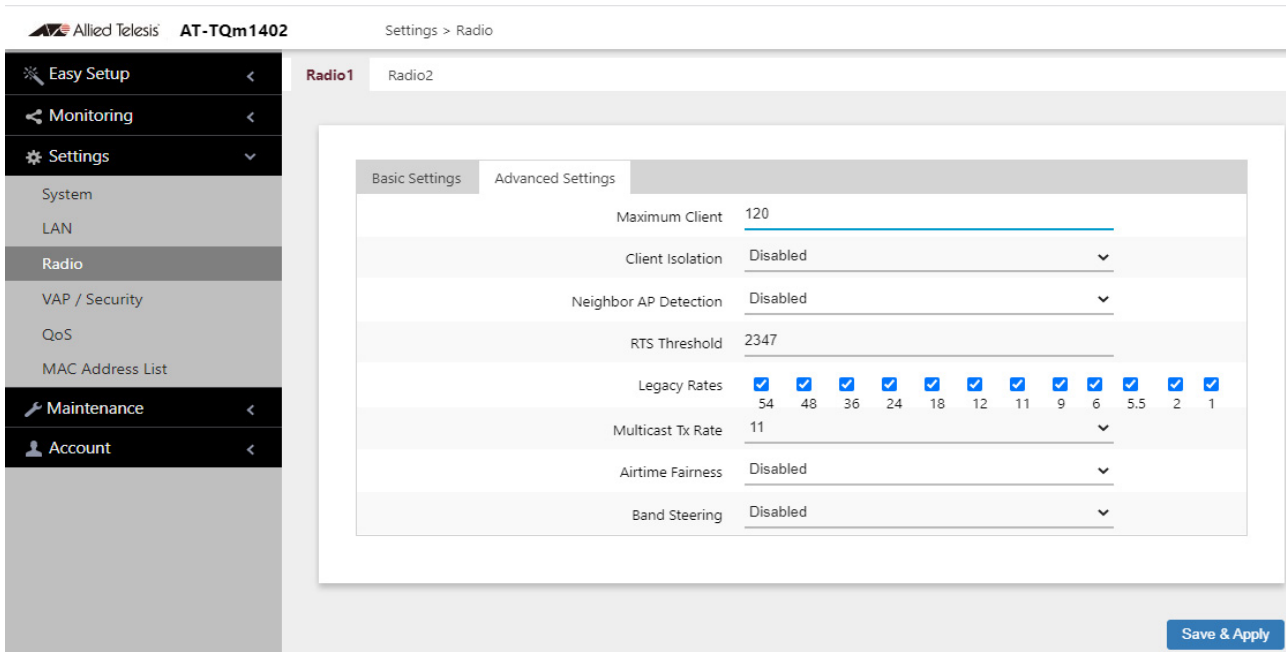


Figure 27. Advanced Radio Settings Window

4. Configure the parameters by referring to Table 20 on page 100.

Table 20. Advanced Radio Settings Window

Field	Description
Maximum Clients	<p>Use this option to specify the maximum number of wireless clients that a radio will support at one time. You might use the option to control the distribution of clients over the radios.</p> <p>A radio rejects all clients when the parameter is set to 0.</p> <p>The maximum numbers of wireless clients that a radio supports at one time are:</p> <ul style="list-style-type: none"> - 2.4GHz Radio1 - 120 clients (default setting) - 5GHz Radio2 - 200 clients (default setting)

Table 20. Advanced Radio Settings Window (Continued)

Field	Description
Client Isolation	<p>Use this option to enable or disable client isolation. When the feature is enabled, the access point does not allow clients in the same VAP to communicate with each other. However, they can communicate with the wired LAN port and with clients in other VAPs.</p> <p>The feature is typically used to enhance wireless security. For instance, by activating this feature on a publicly accessible access point, you enable clients to communicate with the wired LAN port, but not with each other.</p> <p>The options are listed here:</p> <ul style="list-style-type: none"> - Enabled: Activates station isolation. The access point does not allow wireless clients of the same VAP to communicate with each other. - Disabled: Deactivates client isolation. The access point allows wireless clients to communicate with other clients in the same VAP or different VAPs, and with the wired LAN. This is the default setting. <p>This feature does not apply to WDS. Refer to “Introduction to Wireless Distribution System Bridges” on page 172.</p>
Neighbor AP Detection	<p>Use this option to control whether the access point listens for neighboring access points. Here are the options:</p> <ul style="list-style-type: none"> - Enabled: The access point listens for neighboring access points and displays them in the Neighbor AP window. Refer to “Displaying Neighboring Access Points” on page 183. - Disabled: The access point does not listen for neighboring access points. This is the default setting.

Table 20. Advanced Radio Settings Window (Continued)

Field	Description
RTS Threshold	<p>Specifies the size in octets of MPDUs that initiate a Request to Send (RTS) and Clear to Send (CTS) handshake, in IEEE 802.11b/g. The range is 0 to 2347 octets. The default is 2347 octets.</p> <p>You can use this parameter to control the use of RTS/CTS handshakes when the access point transmits MPDUs. The access point uses the handshake before transmitting MPDUs that exceed the defined threshold. If you specify a low value, RTS packets are sent more frequently, which may consume more bandwidth and reduce the throughput. But more RTS packets may help a network recover from interference or collisions, which might occur on a busy network.</p>
Legacy Rates	<p>Select the supported and advertised data transmission rates for IEEE 802.11b/g of the radio. Here are the guidelines:</p> <ul style="list-style-type: none"> - The data rates vary by country. - The default is all data rates are enabled. - Radios are generally more efficient when they advertise subsets of their supported data rates.
Multicast Tx Rate	<p>Select the maximum amount of multicast packets the radio can transmit per second. The default values are listed here:</p> <ul style="list-style-type: none"> - 2.4GHz Radio1: 11Mbps - 5GHz Radio2: 6Mbps
Airtime Fairness	<p>Select Enabled to activate airtime fairness to provide the same communication time (air time) to all connected clients regardless of communication speed. Select Disabled, the default, to turn Airtime Fairness off.</p>

Table 20. Advanced Radio Settings Window (Continued)

Field	Description
Band Steering	<p>Use this option to enable or disable band steering on the radios. Band steering reduces radio congestion by forcing wireless clients that support both 2.4GHz and 5GHz radios to associate with VAPs on a different radio during periods of traffic congestion. Band steering forces clients to associate with VAPs on a 5GHz radio when there is traffic congestion on the 2.4GHz radio. Conversely, clients are forced to associate with VAPs on the 2.4GHz radio when the 5GHz radios are congested. Here are the guidelines:</p> <ul style="list-style-type: none"> - Enabling band steering on one radio activates it on the other radio. Conversely, disabling the feature on one radio disables it on the other radio. - Ideally, the VAP settings on both radios should be identical. This includes SSID names, VLAN IDs, and security settings. - The default setting is disabled.

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

Displaying Radio Status

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

1. Select **Monitoring > Status** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. You can view only one radio at a time. The example in Figure 28 is for Radio1.

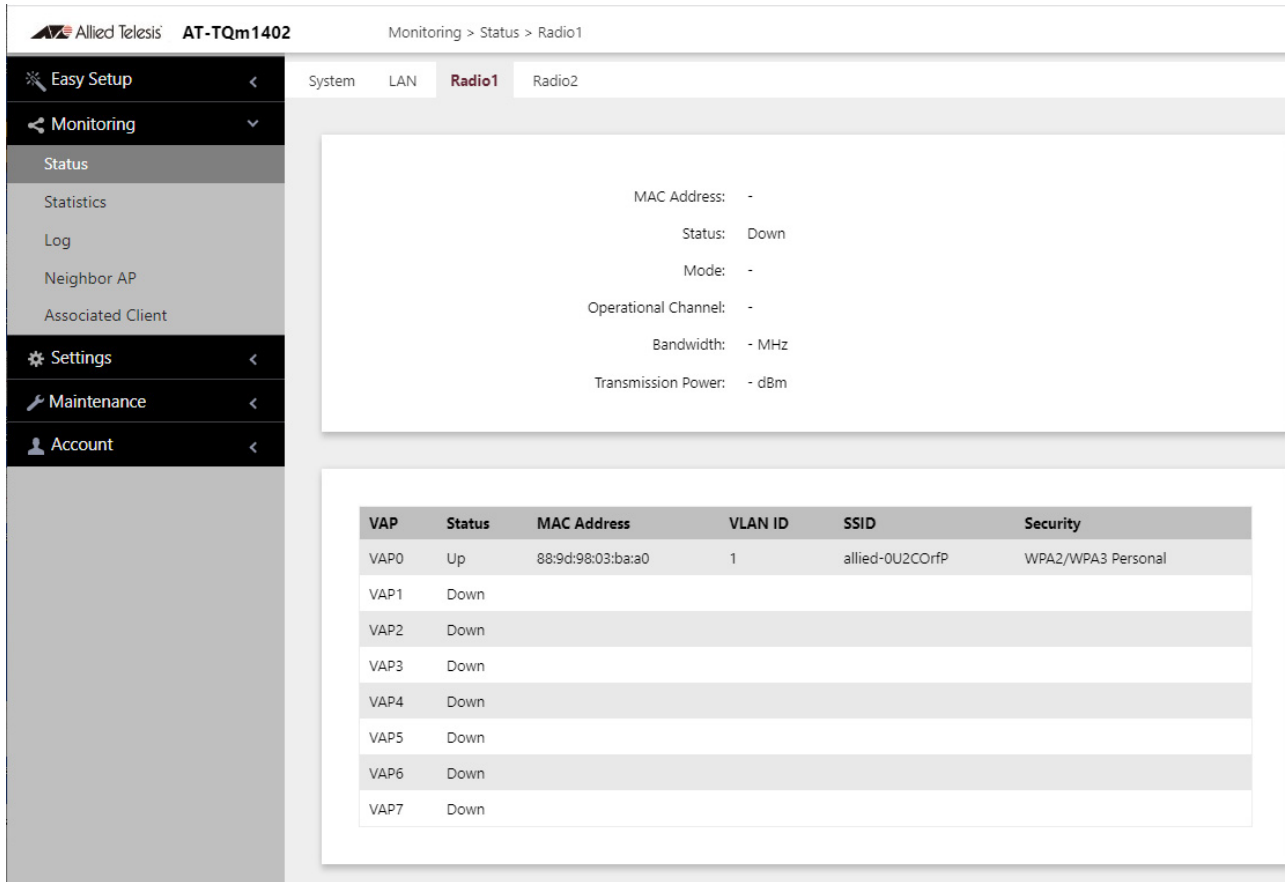


Figure 28. Radio Status Window

Note

The radio status window for Radio2 includes a DFS (Dynamic Frequency Selection) field. For information, see “Dynamic Frequency Selection” on page 107.

The fields are defined in Table 21.

Table 21. Radio Status Window

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

Table 21. Radio Status Window (Continued)

Field	Description
DFS (Radio2 only)	<p>Displays the status of DFS (Dynamic Frequency Selection). For background information, refer to “Dynamic Frequency Selection” on page 107. The possible states are listed here:</p> <ul style="list-style-type: none"> - IDLE: DFS is inactive because the radio is using a W52 or W58 channel. Those channels are not used by DFS. - CAC: Channel Availability Check: The radio has selected a W53 or W56 channel and is performing the DFS radar detection period for one minute before beginning to transmit or receive wireless traffic. If no radar is detected, the radio moves to the ISM status. - ISM: In-Service Monitoring: The radio is using a DFS target channel. If radar is detected, it changes the channel. The DFS status changes to IDLE if the new channel is W52 or W58, or to CAC if the new channel is W53 or W56. - OOC: Out Of Channels: The radio has stopped transmitting and receiving client packets because radar signals are detected on all channel candidates. After 30 minutes, it transitions to CAC.

Dynamic Frequency Selection

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

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

If a wireless access point is using a DFS 5GHz channel for a WDS bridge and it detects radar signals, it randomly selects another channel so as not to interfere with the signals. This action, however, renders the bridge non-functional. For background information, refer to “Introduction to Wireless Distribution System Bridges” on page 172.

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

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

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

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

Note

To determine whether Radio2 is using a DFS channel, refer to “Displaying Radio Status” on page 104.

Setting the Country Code Setting

Note

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

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

Note

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

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

1. Select **Settings > Radio**.
2. Select **Radio1** from the sub-menu. The country code must be set from Radio1.
3. Click the **Basic Settings** tab. This is the default tab. Refer to Figure 26 on page 96.
4. Select the **Country Code** pull-down menu and choose your country or region. Here are the guidelines:
 - You can select only one country.
 - The Country Code parameter is shown in the Basic Settings windows of all three radios, but can only be set from Radio1.
 - The same country code applies to all three radios.
 - Changing the country code disables the radios.
 - You have to reconfigure the radio settings after changing this parameter.
5. Click the **SAVE & APPLY** button to save and update the configuration.

Chapter 6

Virtual Access Points

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

- ❑ “VAP Introduction” on page 110
- ❑ “Configuring Basic VAP Parameters” on page 111
- ❑ “Generating Quick Response (QR) Codes for VAPs” on page 114
- ❑ “Configuring Captive Portal” on page 116
- ❑ “Configuring VAP Security” on page 130
- ❑ “Configuring VAP Fast Roaming” on page 146
- ❑ “Configuring the MAC Address List” on page 150
- ❑ “Displaying VAP and LAN Ports Statistics” on page 152

VAP Introduction

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

VAP parameters are divided into these three groups:

- ❑ “Configuring Basic VAP Parameters” on page 111
- ❑ “Configuring VAP Security” on page 130
- ❑ “Configuring VAP Fast Roaming” on page 146

VAP Guidelines

Here are guidelines to configuring VAP:

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

Configuring Basic VAP Parameters

To configure basic VAP settings, perform the following procedure:

1. Select **Settings > VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Virtual Access Point** tab. This is the default tab. The example in Figure 29 shows the settings for VAP0 on Radio1.

The screenshot displays the web interface for the AT-TQm1402 device. The breadcrumb trail is 'Settings > VAP / Security > Radio1'. The left sidebar shows the navigation menu with 'Settings' expanded to 'VAP / Security'. The main content area shows the configuration for 'Radio1' and 'VAP0'. The 'Virtual Access Point' tab is selected, showing the following settings:

Virtual Access Point	Security	MAC Access Control	Captive Portal	Fast Roaming	Advanced Settings
Status	Enabled				
Mode	Access Point				
SSID	allied-0U2COrfP				
VLAN ID	1				
Hidden SSID	Enabled				

A 'View QR code' button is visible at the bottom right of the configuration area.

Figure 29. Virtual Access Point Tab

5. Configure the parameters by referring to Table 22 on page 112.

Table 22. Virtual Access Point Tab

Field	Description
Status	<p>Enable or disable the VAP. Here are the guidelines.</p> <ul style="list-style-type: none"> - A disabled VAP does not forward any ingress or egress traffic. - The default setting for VAP0 is enabled. - The default setting for VAP1 to VAP7 is disabled. - You cannot disable VAP0. To stop VAP0 from forwarding traffic from wireless clients, you have to disable its radio.
Mode	<p>Select a mode setting from the pull-down menu. This parameter applies only to VAP0. The menu choices are listed here:</p> <ul style="list-style-type: none"> - Access Point: Select this mode to have a VAP function as a normal VAP, without WDS bridging. This is the default setting. - WDS Parent: Select this mode to have VAP0 function as the parent in a WDS bridge. A WDS parent access point has its LAN port connected to the wired network. For background information, refer to “Introduction to Wireless Distribution System Bridges” on page 172. - WDS Child: Select this mode to have VAP0 function as a child in a WDS bridge. A child access point communicates with the wired network through the parent unit. - Single Channel Type: (VAP0 Radio2 only). <hr/> <p>Note The TQm1402 access point does not support Single Channel Type.</p> <hr/> <p>The only mode for VAP1 to VAP7 is Access Point.</p>

Table 22. Virtual Access Point Tab (Continued)

Field	Description
SSID	<p>Enter a name for the VAP. Here are the guidelines:</p> <ul style="list-style-type: none"> - A VAP must have a name. - A name can be from 1 to 32 alphanumeric characters. - Spaces are allowed except the first and last characters of an SSID. - You can assign the same name to more than one VAP. - The default names for VAP0 on Radio1 and Radio2 are based on the MAC address of the access point. - The default names for VAP1 to VAP7 are Virtual Access Points 1 to 7.
VLAN ID	<p>Enter a VID for the VAP. Here are the guidelines:</p> <p>The range is 1 to 4094. The default is VID 1. A VAP can have only one VID. You can assign the same VID to more than one VAP. This VID is ignored for wireless clients that receive their VIDs from a RADIUS server for WPA Enterprise security. VIDs from a RADIUS server override the number in this field.</p>
Hidden SSID	<p>Select whether the access point should advertise the VAP SSID to clients. Here are the options:</p> <p>Disabled: The access point transmits the SSID to advertise the VAP to clients. This is the default setting. Enabled: The access point does not advertise the VAP. Clients who want to connect to a hidden VAP have to know its name.</p>

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

Generating Quick Response (QR) Codes for VAPs

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

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

Here are the guidelines:

- Codes are generated by clicking the View QR Code button in the Virtual Access Point windows.
- QR codes are not supported on VAPs that use RADIUS servers to authenticate wireless clients.
- QR codes require firmware v6.0.1-2.1 or later.

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

1. Select **Settings** > **VAP/Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Configure the VAP settings. Refer to the earlier sections in this chapter.
5. Return to the **Virtual Access Point** tab.
6. Click the **View QR Code** button. Refer to Figure 30 on page 115.

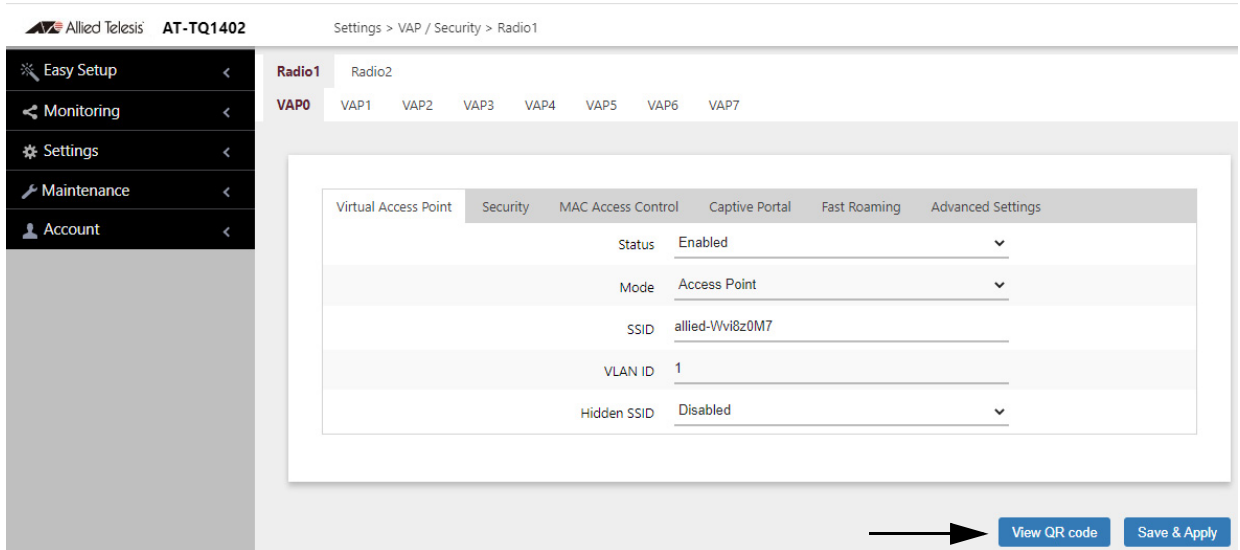


Figure 30. View QR Code Button

Configuring Captive Portal

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

Captive Portal Configurations

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

- ❑ Allowing any wireless clients to access to your networks

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

- ❑ “Requiring Wireless Clients to Click the Agree Button to Access to the Network” on page 117

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

- ❑ “Delegating a Proxy Server to Interact with Wireless Clients” on page 120

Interacting with wireless clients is conducted by the proxy server that you specify. The proxy server hosts web pages so that you can create your own web pages and applications if necessary. See “Creating Pages in HTML for a Proxy Server” on page 127.

- ❑ “Delegating RADIUS Servers and a Proxy Server” on page 122

An authentication process is conducted by a RADIUS server that you specify. You also specify a proxy server to host web pages to interact with wireless clients. You can create your own HTML files on the proxy server. See “Creating Login Pages in HTML When External RADIUS is Selected” on page 128.

- ❑ “Delegating RADIUS Servers to Authenticate Wireless Clients” on page 125

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

Port Numbers

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

- ❑ 8080 for HTTP

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

- ❑ 8443 for HTTPS

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

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

To require wireless clients to click the Agree button to access to the networks, perform the following procedure:

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

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

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

3. Select a VAP to configure from the next sub-menu.

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

4. Select the **Captive Portal** tab. See the example in Figure 29 on page 111.

5. Select **Click-Through** from the Captive Portal pull-down menu. See Figure 31 on page 118.

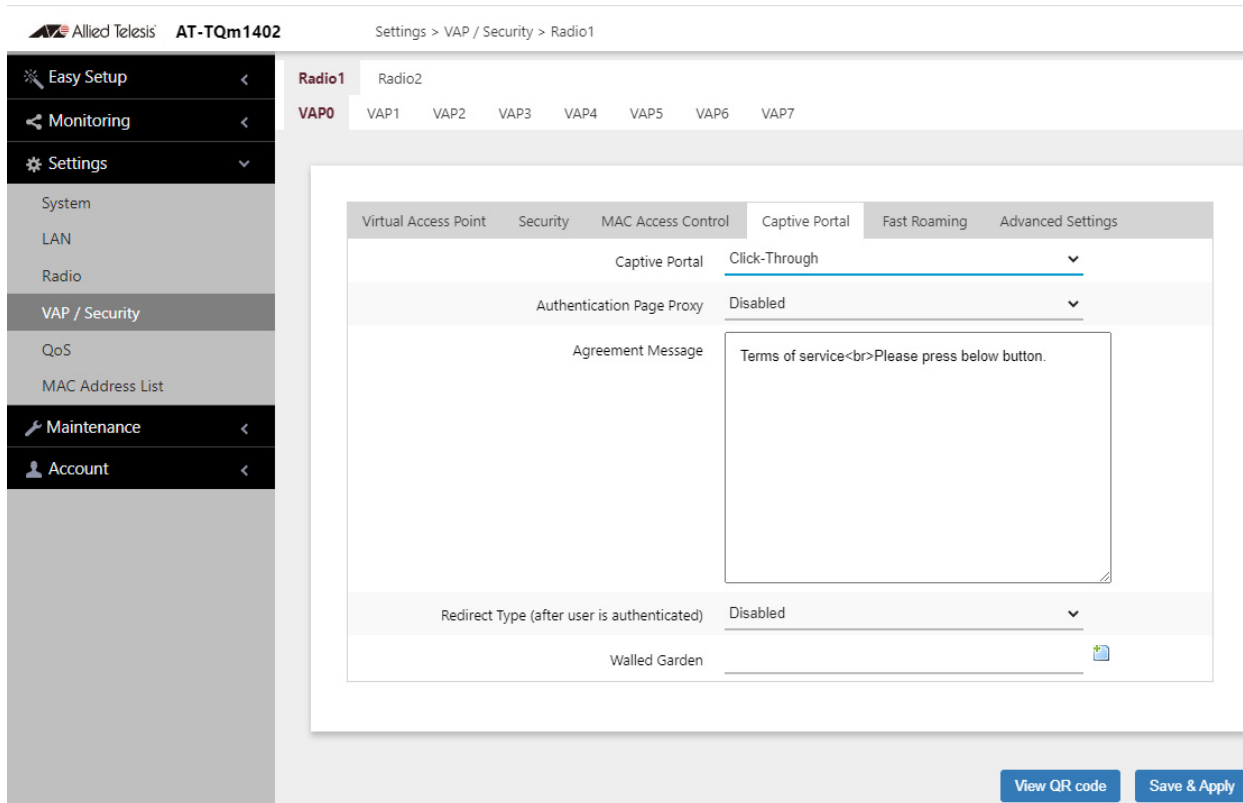


Figure 31. Captive Portal - Click-Through

6. Select **Disabled** from the Authentication Page Proxy pull-down menu. By default, the Authentication Page Proxy is disabled.
7. Configure the parameters by referring to Table 23.

Table 23. Captive Portal

Field	Description
Agreement Message	Enter Conditions of Use or other information in the HTML code format to be displayed in the introductory web page.

Table 23. Captive Portal (Continued)

Field	Description
Authentication Page Proxy	<p>Enable or disable Authentication Page Proxy on the captive portal:</p> <ul style="list-style-type: none"> - Enabled: The access point uses other web server's authentication page via proxy with captive portal. - Disabled: The access point uses its own local authentication page with captive portal. This is the default. <p>Refer to "Delegating a Proxy Server to Interact with Wireless Clients" on page 120</p>
Redirect Type (after user is authenticated)	<p>Select the following options to control a Web page to be displayed to wireless clients after they are allowed to access to the network.</p> <p>The options are:</p> <ul style="list-style-type: none"> - Fixed URL: Allows you to specify a URL to redirect to wireless clients. When this option is selected, the Fixed URL field becomes available. - Session Keep: Displays a web page that wireless clients originally requested. - Disabled: Redirect is disabled. The welcome.html that you prepared is displayed. When the Capital Portal field is Click-Through and the Authentication Proxy Page is Disabled, the welcome page on the access point is displayed. This is the default setting.

Table 23. Captive Portal (Continued)

Field	Description
Walled Garden	<p>Note Walled Garden is not supported on TQ1402 v6.0.1-7.1.</p> <hr/> <p>Enter up to fifty approved HTTP web sites that clients can access through the captive portals on the wireless access point, without having to log on. Clients who access only approved sites are not authenticated. Those who try to access unapproved web sites will see a logon window. The feature is supported on all radios, VAPs, and captive portals.</p> <p>To add the first HTTP web site, enter it in the empty field. You can identify a site by its fully qualified domain name (FQDN), IPv4 address, or IPv4 address and mask (e.g 32.134.45.0/24). When using FQDN, do not include HTTP://. To add more URL addresses, click the green add icon to the right of the last URL field. You can enter up to fifty sites. To delete an entry, click its red delete icon. See Figure 32.</p>

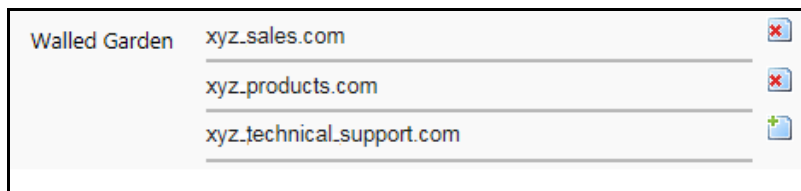


Figure 32. Example of HTTP URLs of Approved Web Sites for the Walled Garden

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

Delegating a Proxy Server to Interact with Wireless Clients

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

To delegate a proxy server to interact with wireless clients, perform the following procedure:

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

3. Select a VAP to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Captive Portal** tab. See the example in Figure 29 on page 111.
5. Select **Click-Through** from the Captive Portal pull-down menu. See Figure 33 on page 121.
6. Select **Enabled** from the Authentication Page Proxy pull-down menu. See Figure 33 on page 121.

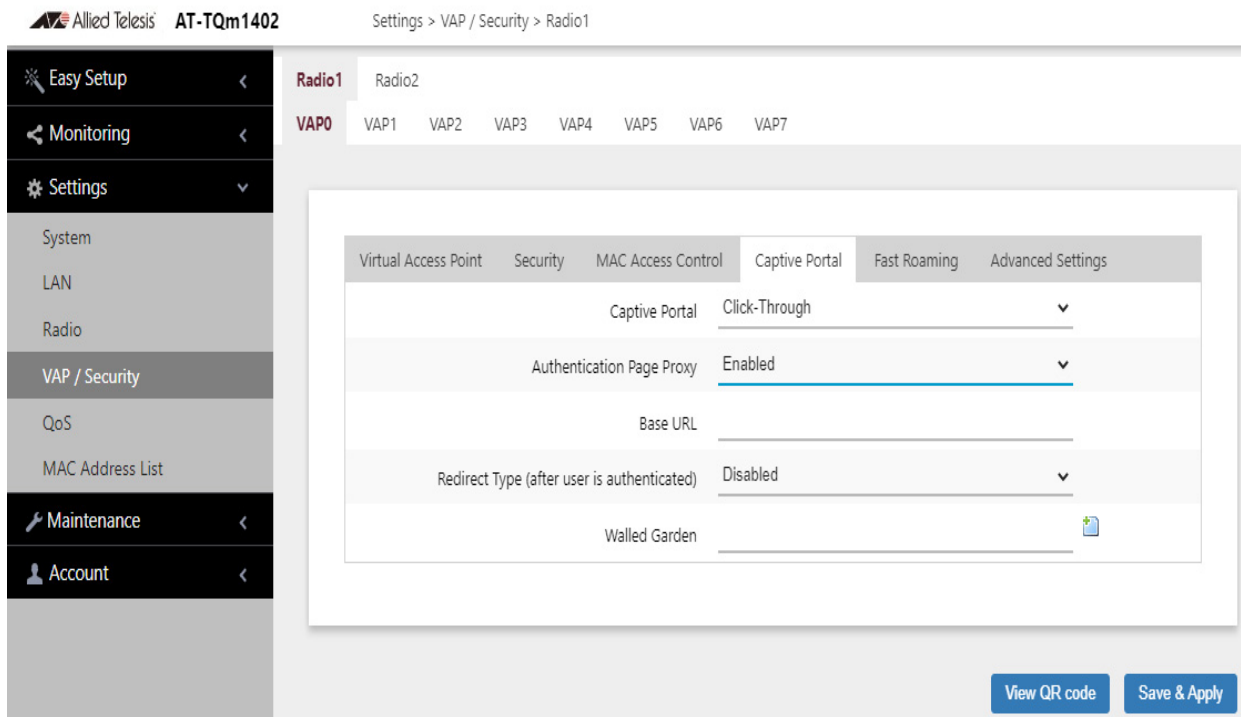


Figure 33. Captive Portal - Using a Proxy Server

7. Specify a URL of your web server in the Base URL field.
8. Specify the Redirect Type field by referring to Table 23 on page 118.
9. Specify the Walled Garden field by referring to Table 23 on page 118.
10. Click the **SAVE & APPLY** button to save and update the configuration.
11. Go to “Creating Pages in HTML for a Proxy Server” on page 127 to create the HTML files.

Delegating RADIUS Servers and a Proxy Server

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

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

To display an authentication page hosted by a RADIUS server when wireless clients access to network resources, perform the following procedure:

1. Select **Settings > VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Captive Portal** tab. See the example in Figure 29 on page 111.
5. Select **External RADIUS** from the Captive Portal pull-down menu. See Figure 34.
6. Select **Enabled** from the Authentication Page Proxy pull-down menu. See Figure 34.

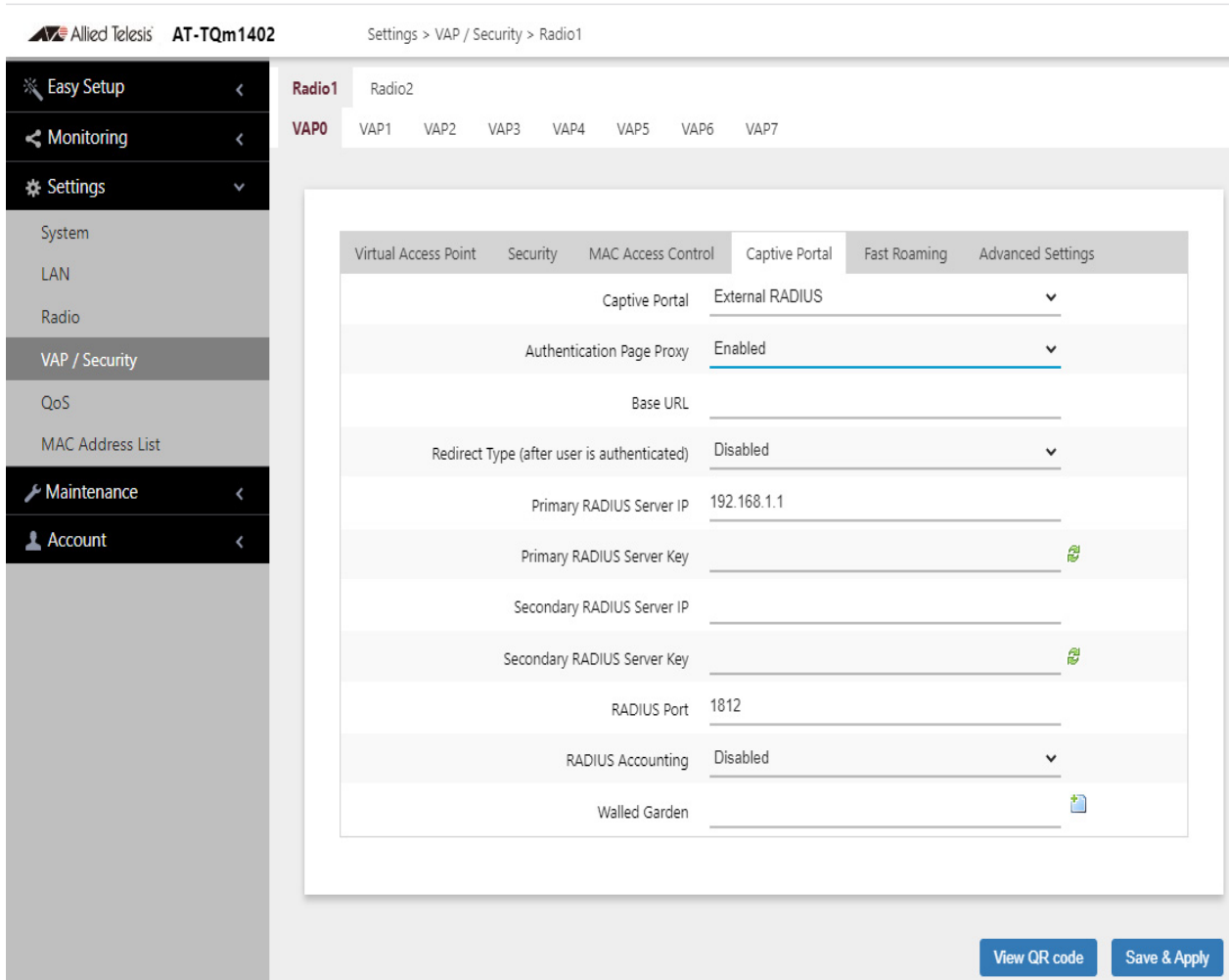


Figure 34. Captive Portal - External RADIUS

7. Configure the parameters by referring to Table 24 on page 123.

Table 24. Captive Portal - External RADIUS

Field	Description
Authentication Page Proxy	Select enabled.
Base URL	Enter the URL of your web server. You can only enter one URL.
Redirect Type (after user is authenticated)	See Table 23 on page 118.
Primary RADIUS Server IP	Enter the IPv4 address of the primary FADIUS server. The default is 192.168.1.1

Table 24. Captive Portal - External RADIUS (Continued)

Field	Description
Primary RADIUS Server Key	<p>Enter the shared secret key for the primary RADIUS server.</p> <p>Here are the guidelines:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The key can be up to 128 alphanumeric characters. <input type="checkbox"/> It is case-sensitive. <input type="checkbox"/> It must be same on the access point and server. <input type="checkbox"/> The default is no key.
Secondary RADIUS Server IP	<p>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.</p>
Secondary RADIUS Server Key	<p>Enter the shared secret key for the secondary RADIUS server.</p>
RADIUS Port	<p>Enter the RADIUS port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must be using the same port number. The range is 0 to 65535. The default is 1812.</p>
RADIUS Accounting	<hr/> <p>Note Captive Portal RADIUS Accounting is not supported on TQ1402 v6.0.1-7.1.</p> <hr/> <p>Controls RADIUS accounting. When accounting is enabled, the access point sends client information, such as usage time, to the RADIUS server. The options are listed here:</p> <ul style="list-style-type: none"> - Enabled: Activate RADIUS accounting. - Disabled: Deactivate RADIUS accounting. This is the default setting.
Walled Garden	<p>See Table 23 on page 118.</p>

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

9. Go to “Creating Login Pages in HTML When External RADIUS is Selected” on page 128 to create the HTML files.

Delegating RADIUS Servers to Authenticate Wireless Clients

Note

Captive Portal External Page Redirect is not supported on TQ1402 v6.0.1-7.1.

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

To delegate RADIUS servers, perform the following procedure:

1. Select **Settings > VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Captive Portal** tab. See the example in Figure 29 on page 111.
5. Select **External RADIUS** from the Captive Portal pull-down menu. See Figure 35.
6. Select **Disabled** from the Authentication Page Proxy pull-down menu. See Figure 35.

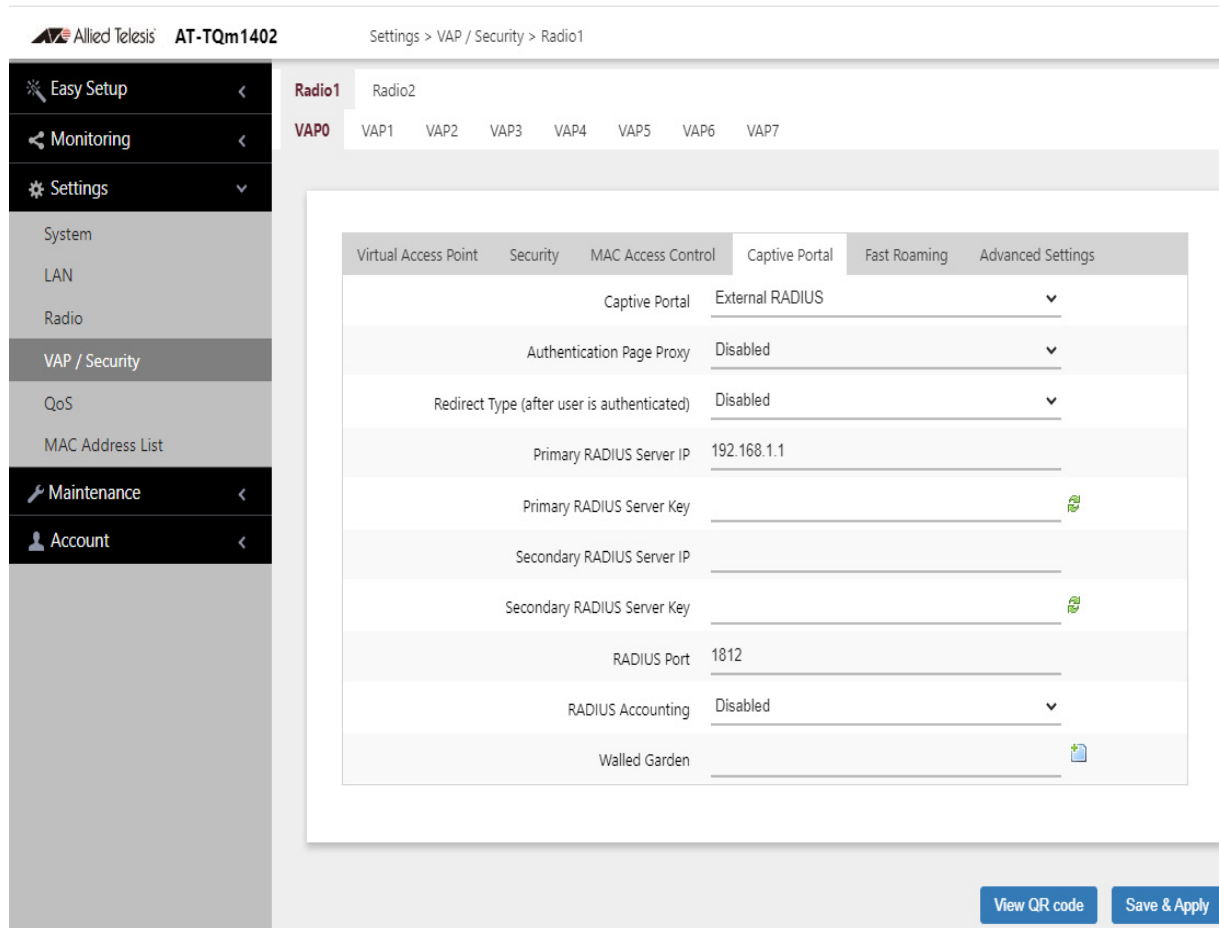


Figure 35. Captive Portal - External RADIUS

7. Configure the parameters by referring to Table 24 on page 123.
8. Click the **SAVE & APPLY** button to save and update the configuration.

Redirecting to an External Authentication Page

The External Page Redirect option allows the wireless access point to redirect clients of captive portals to remote web servers for the logon windows. This feature requires a RADIUS server to authenticate the clients and is supported on all radios and VAPs. When you select this option, the window adds fields for the External Page URL for the URL of the remote web server, and for the IP addresses of the RADIUS servers.

To designate an external authentication page and delegate RADIUS servers, perform the following procedure:

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

3. Select a VAP to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Captive Portal** tab. See Figure 36.
5. Select **External Page Redirect**. See Figure 36.

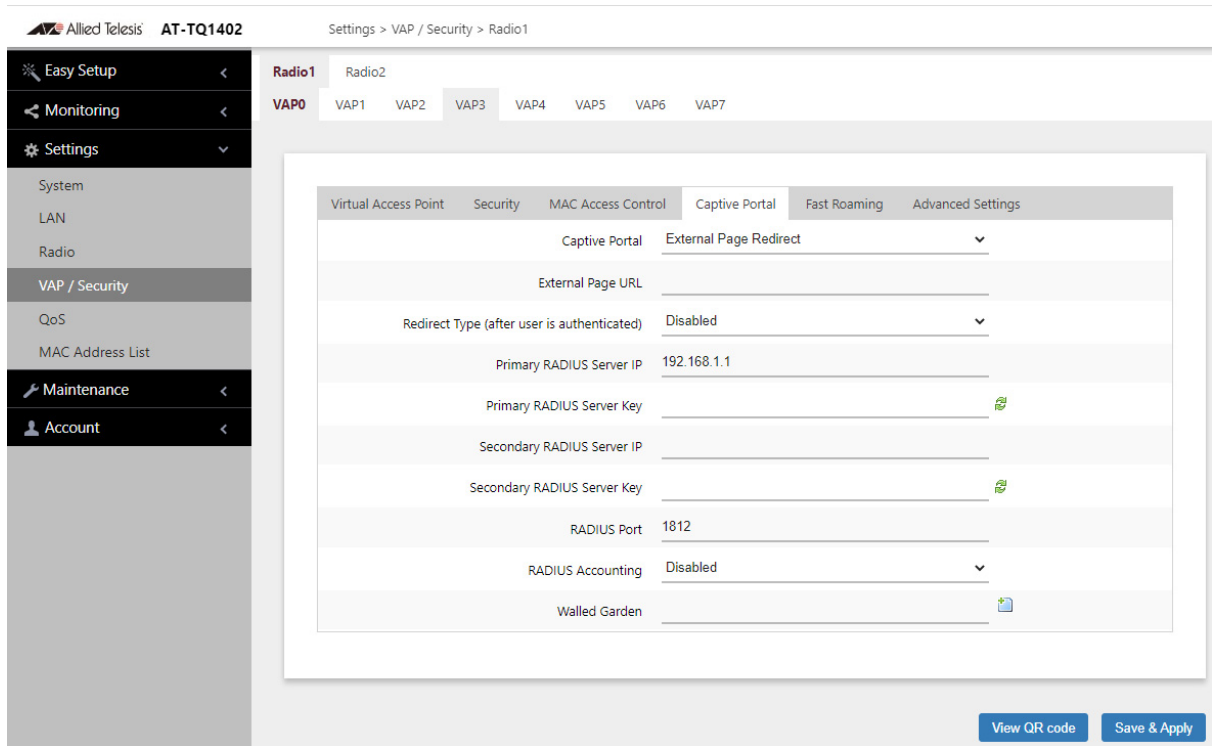


Figure 36. Captive Portal - External Page Redirect Window

6. Click the **Save & Apply** button to save and update the configuration, or click the **View QR code** button to generate a QR code.

Creating Pages in HTML for a Proxy Server

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

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

Requirements for the click_through_login.html and click_through_login_fail.html

Here is a list of requirements:

- You must include a <form> element with the method attribute specified to "post" and no action attribute.
- In the <form> element, you must include a <button> tag or an

<input> tag with the type attribute specified to “submit” for a wireless client to submit the data to the proxy server.

- ❑ No requirement for a welcome.html

HTML Code and Display Examples of Login Page

The following is an example of HTML code:

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

Figure 37 shows its web page displayed in a web browser.

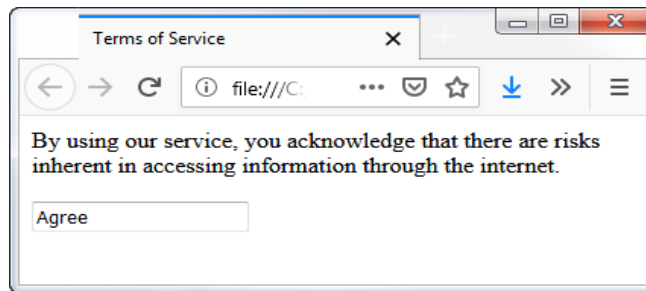


Figure 37. Captive Portal - Terms of Service Page Sample

Creating Login Pages in HTML When External RADIUS is Selected

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

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

Requirements for the radius_login.html and radius_login_fail.html

Here is a list of requirements:

- ❑ You must include a <form> element with the method attribute specified to “post” and no action attribute.

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

HTML Code and Display Examples of Login Page

The following is an example of HTML code:

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

Figure 38 on page 129 shows its web page displayed in a web browser.

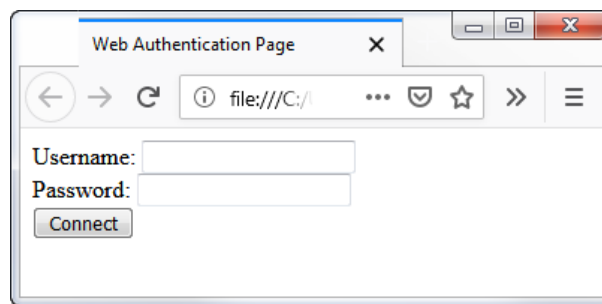


Figure 38. Captive Portal - Login Page Sample

Configuring VAP Security

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

- ❑ “No Security” on page 130
- ❑ “WPA Personal (Pre-Shared Key)” on page 131
- ❑ “WPA Enterprise” on page 133

No Security

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

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

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Security** tab.
5. Select **None** from the Mode pull-down menu. This is the default setting. Refer to Figure 39.

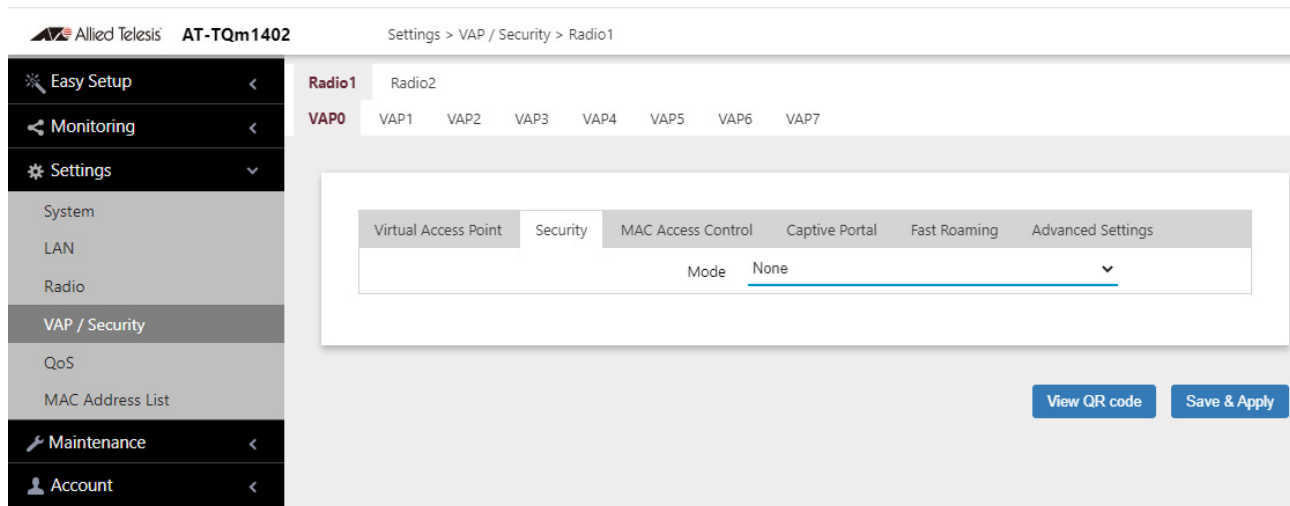


Figure 39. None Selection in the VAP Security Tab

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

WPA Personal (Pre-Shared Key)

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

1. Select **Settings** > **VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Security** tab.
5. Select **WPA Personal** from the Mode pull-down menu. Refer to Figure 40.

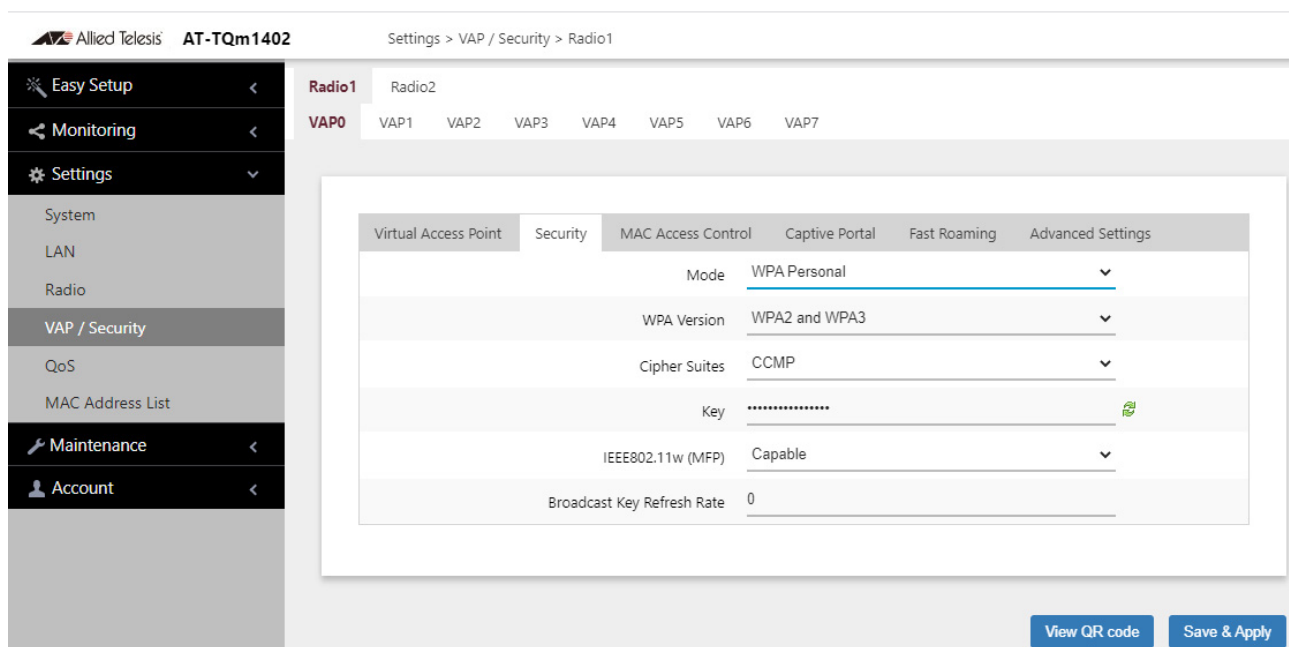


Figure 40. WPA Personal Security Tab

6. Configure the parameters by referring to Table 25 on page 132.

Table 25. WPA Personal Security Tab

Field	Description
Mode	Select WPA Personal .
WPA Version	<p>Select the WPA version. The options are listed here:</p> <ul style="list-style-type: none"> - WPA and WPA2: Select this option if the VAP has both WPA and WPA2 clients. - WPA2: Select this option if clients support WPA2 only. This is the default setting. - WPA2 and WPA3: Select this option if the VAP has both WPA2 and WPA3 clients. - WPA3: Select this option if clients support WPA3 only. This is the default setting.
Cipher Suites	<p>Select the cipher suite for the VAP. The options are listed here:</p> <ul style="list-style-type: none"> - CCMP. This is the default. <hr/> <p>Note When the WPS version is WPA2 and WPA3, or WPA3, CCMP is the only option.</p> <hr/> <ul style="list-style-type: none"> - TKIP and CCMP <p>When both TKIP and CCMP are selected, clients who are using WPA must have one of the following:</p> <ul style="list-style-type: none"> - A valid TKIP key. - A valid CCMP (AES) key.
Key	<p>Enter a shared secret key Here are the guidelines:</p> <ul style="list-style-type: none"> - The key can be from 8 to 63 alphanumeric characters. - It can include special characters. - It is case sensitive. - The default is no key. <p>The small double-arrow symbol next to the field toggles the key between alphanumeric characters and asterisks.</p>

Table 25. WPA Personal Security Tab (Continued)

Field	Description
IEEE802.11w (MFP)	<p>Control IEEE 802.11w management frame protection. This feature is only supported with WPA2 as the WPA Version. It is not supported with WPA and WPA2. The options are listed here:</p> <ul style="list-style-type: none"> - Enabled: Activates management frame protection. This is the default. <hr/> <p>Note When the WPS version is WPA2 and WPA3, or WPA3, Enabled is the only option.</p> <hr/> <ul style="list-style-type: none"> - Disabled: Deactivates management frame protection.
Broadcast Key Refresh Rate	Specify the refresh interval rate for the broadcast (group) key. The range is 0 to 86400 seconds. The key is not refreshed when this parameter is set to 0 seconds, which is the default.

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

WPA Enterprise

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

Note

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

1. Select **Settings > VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Security** tab.
5. Select **WPA Enterprise** from the Mode pull-down menu. See Figure 41 on page 134.

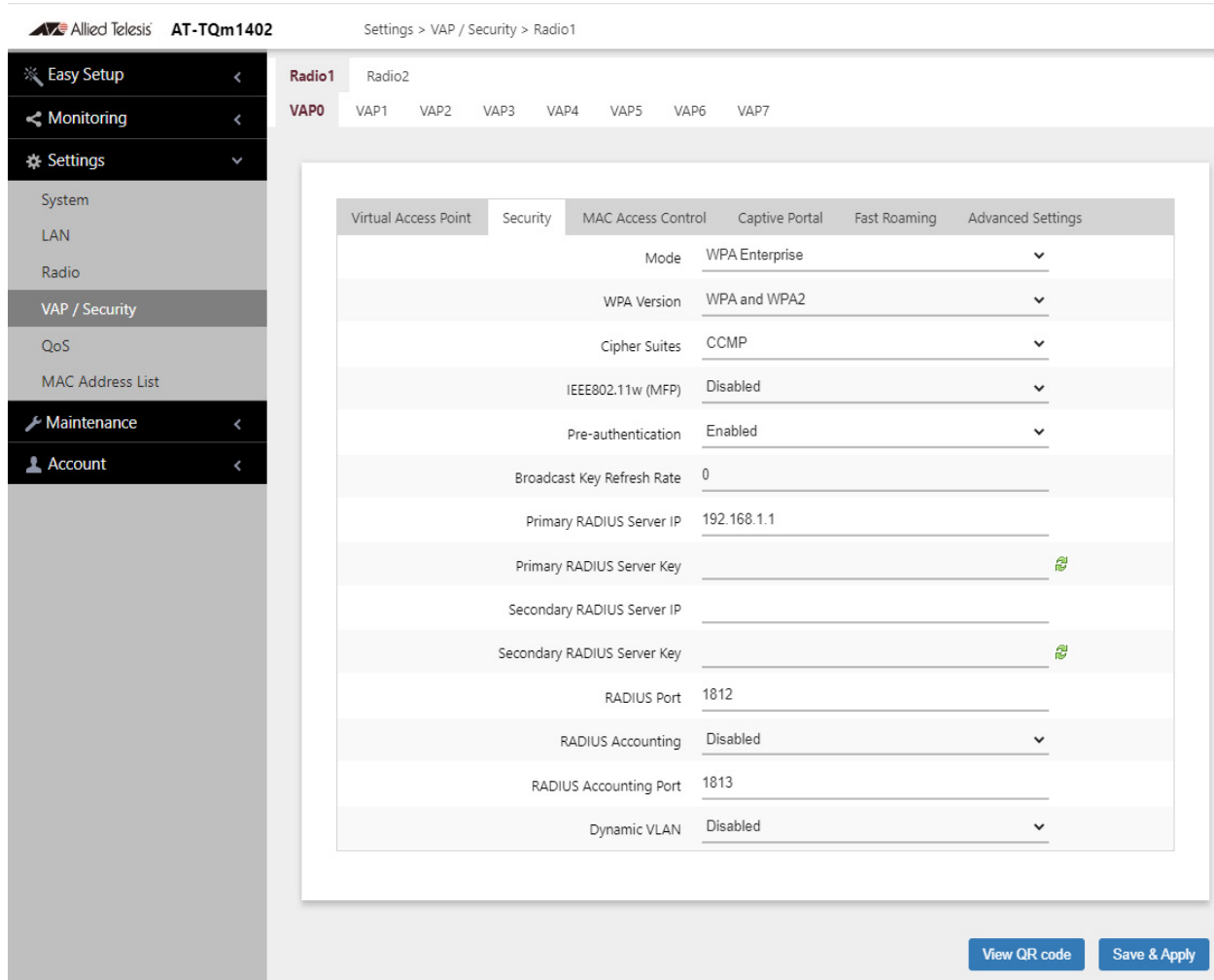


Figure 41. WPA Enterprise Tab

6. Configure the parameters by referring to Table 26 on page 135.

Table 26. WPA Enterprise Tab

Field	Description
Mode	Select WPA Enterprise .
WPA Version	<p>Select the WPA version for the VPA. The options are listed:</p> <ul style="list-style-type: none"> - WPA and WPA2 - Select this option if the VAP has both WPA and WPA2 clients. - WPA2: Select this option if all the clients support WPA2 only. This is the default setting. - WPA3: Select this option if clients support WPA3 only. <hr/> <p>Note WPA3 is supported only on Radio2.</p> <hr/>
Cipher Suites	<p>Select the cipher suite for the VAP, The options are listed here:</p> <ul style="list-style-type: none"> - CCMP. This is the default. <hr/> <p>Note When the WPS version is WPA3, CCMP is the only option.</p> <hr/> <p>- TKIP and CCMP</p> <p>When both TKIP and CCMP are selected, clients configured to use WPA with RADIUS must have one of the following:</p> <ul style="list-style-type: none"> - A valid TKIP RADIUS IP address and RADIUS key. - A valid CCMP IP address and RADIUS key.

Table 26. WPA Enterprise Tab (Continued)

Field	Description
IEEE802.11w (MFP)	<p>Control IEEE 802.11w management frame protection. This feature is only supported with WPA2 as the WPA Version. It is not supported with WPA and WPA2. The options are listed here:</p> <ul style="list-style-type: none"> - Enabled: Activates management frame protection. This is the default. <hr/> <p>Note When the WPS version is WPA3, Enabled is the only option.</p> <hr/> <ul style="list-style-type: none"> - Disabled: Deactivates management frame protection.
Pre-authentication	<p>Set the pre-authentication status for WPA2 clients.</p> <ul style="list-style-type: none"> - Enabled: Enables pre-authentication. The access point forwards pre-authentication information from WPA2 clients to the next access points. This can speed up authentications of roaming clients as they associate with different access points. This is the default. - Disabled: Disables pre-authentication for WPA2 clients.
Broadcast Key Refresh Rate	<p>Enter the interval for updating the key of the broadcast packet to be sent to the wireless clients connected to the VAP. The range is 0 to 86400 seconds. The key is not updated when this parameter is set to 0 (zero). The default is 0.</p>
Primary RADIUS Server IP	<p>Enter the IPv4 address of the primary RADIUS server. The default is 192.168.1.1.</p>
Primary RADIUS Server Key	<p>Enter the shared secret key for the primary RADIUS server. Here are the guidelines:</p> <ul style="list-style-type: none"> - The key can be up to 128 alphanumeric characters. - It is case-sensitive. - It must be same on the access point and server. - The default is no key.

Table 26. WPA Enterprise Tab (Continued)

Field	Description
Secondary RADIUS Server IP	Enter the IPv4 address of a secondary RADIUS server. This field is optional. The access point sends authentication requests to this address if the primary RADIUS server does not respond to requests.
Secondary RADIUS Server Key	Enter the shared secret key for the secondary RADIUS server.
RADIUS Port	Enter the RADIUS port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must be using the same port number. The range is 0 to 65535. The default is 1812.
RADIUS Accounting	Control RADIUS accounting, When accounting is enabled, the access point sends client information, such as usage time, to the RADIUS server. The options are listed here: <ul style="list-style-type: none"> - Enabled: Activate RADIUS accounting. - Disabled: Deactivate RADIUS accounting. This is the default setting.
RADIUS Accounting Port	Enter the RADIUS accounting port number of the RADIUS server. If you entered IP addresses for both primary and secondary servers, the units must use the same accounting port number. The range is 0 to 65535. The default is 1813.
Dynamic VLAN	Control whether the VAP only accepts clients that are assigned VIDs by RADIUS servers. The options are listed here: <ul style="list-style-type: none"> - Enabled: The VAP forwards packets only from clients that are assigned VIDs from RADIUS servers. - Disabled: The VAP forwards packets without regard to how clients are assigned VIDs. This is the default setting.

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

Configuring MAC Access Control Settings

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

To configure MAC Access Control Settings, perform the following procedure:

1. Select **Settings** > **VAP/Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure for the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **MAC Access Control** tab. This is the default tab. Refer to Figure 42 on page 138

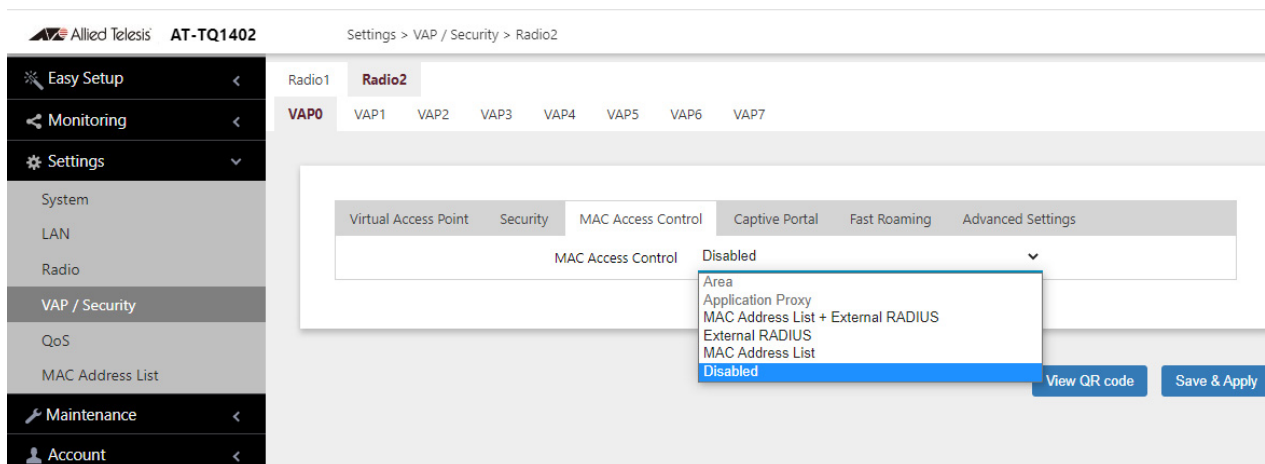


Figure 42. MAC Address Control Menu

5. Configure the parameters by referring to Table 27.

The menu options are described in Table 27.

Table 27: MAC Access Control Menu

Menu Selection	Definition
Area	Authenticates wireless clients based on their MAC addresses and physical locations in Channel Blankets or multi-channel VAPs. Requires Vista Manager EX v3.2.1 or later and the AWC plug-in. See “Configuring Area Authentication” on page 140
Application Proxy	Authenticates clients using the AMF Application Proxy in the AMF Security controller. The application proxy allows you to add security policies that define where and when clients can access your wireless network. It also allows you to designate their network assignments by assigning them VLAN IDs. This feature requires AMF Security mini or the AMF Security Controller (AMF-SEC) v2.2.0 or later, and Vista Manager EX v3.6.0. It also requires the OpenFlow license on the access point. Refer to the <i>AMF Security mini User Guide</i> or <i>AMF Security Controller User Guide</i> for further information. See “Configuring Application Proxy” on page 140.
MAC Address + External RADIUS	<p>Authenticates MAC addresses of wireless clients by combining the on-board MAC address filter with a RADIUS server on your network.</p> <ul style="list-style-type: none"> - Allow: The wireless access point accepts clients whose MAC address are either in the on-board filter or on the RADIUS server. - Deny: The wireless access point accepts clients whose MAC address are not in the on-board filter, but are on the RADIUS server. <p>Refer to “Authenticating Clients with Both the On-board MAC Filter and RADIUS Server” on page 141.</p>

Table 27: MAC Access Control Menu (Continued)

Menu Selection	Definition
External RADIUS	Authenticates MAC addresses of wireless clients with a RADIUS server on your network. See “Authenticating Wireless Clients with an External RADIUS Server” on page 142.
MAC Address List	Authenticates MAC addresses of wireless clients using the MAC address filter in the access point. See “Configuring the MAC Address List” on page 150 for instructions on how to add MAC addresses to the filter. The access point has only one on-board MAC address filter.
Disabled	Disables MAC address authentication on the VAP.

6. Click the **SAVE & APPLY** button to save and update the configuration, or click **VIEW QR CODE** to generate a QR code.

Configuring Area Authentication

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

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

Configuring Application Proxy

Authenticates clients using the AMF Application Proxy in the AMF Security controller. The application proxy allows you to add security policies that define where and when clients can access your wireless network. It also allows you to designate their network assignments by assigning them VLAN IDs. This feature requires AMF Security mini or the AMF Security Controller (AMF-SEC) v2.2.0 or later, and Vista Manager EX v3.6.0. It also requires the OpenFlow license on the access point. Refer to the *AMF Security mini User Guide* or *AMF Security Controller User Guide* for further information.

Authenticating Clients with Both the On-board MAC Filter and RADIUS Server

The access point can use its on-board filter or an external RADIUS server to authenticate the MAC addresses of wireless clients. It can also authenticate addresses by combining both methods. This is performed with the MAC Address + External RADIUS option in the MAC Access Control menu. When clients associate on a VAP where this option is enabled, the access point first compares their MAC addresses against its on-board filter and, if there is no match, sends the addresses to a designated RADIUS server.

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

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

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

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

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

Here are the basic steps to using the MAC Address + External RADIUS option in the MAC Access Control menu:

1. Configure the on-board MAC address filter by adding the MAC addresses of clients the access point is to accept or reject. Refer to "Configuring MAC Access Control Settings" on page 138.
2. Configure the external RADIUS server by adding the MAC address of clients the access point is to accept.
3. Select the MAC Address + External RADIUS option in the MAC Access Control menu.

Authenticating Wireless Clients with an External RADIUS Server

4. Enter the RADIUS server settings. Refer to Table 27 on page 139.

There are several ways that the wireless access point can authenticate wireless clients by their MAC addresses. One method uses the on-board MAC address filter. It allows you to specify the MAC addresses of the wireless clients whose traffic the access points are to either accept or reject. You can apply the filter to the individual VAPs, and so add filtering to those VAPs where it is most needed.

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

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

Note

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

To configure a VAP to use an external RADIUS server to authenticate wireless clients, perform the following procedure:

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

5. Select **External RADIUS** from the MAC Filtering option. Refer to Figure 43 on page 143:

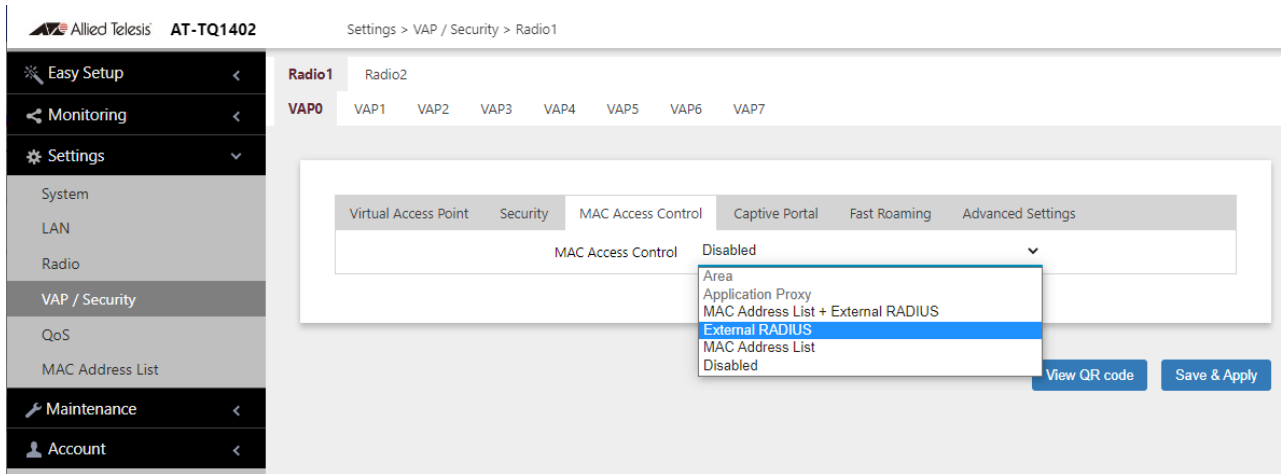


Figure 43. External RADIUS Selection

Selecting External RADIUS displays the additional settings shown in Figure 44.

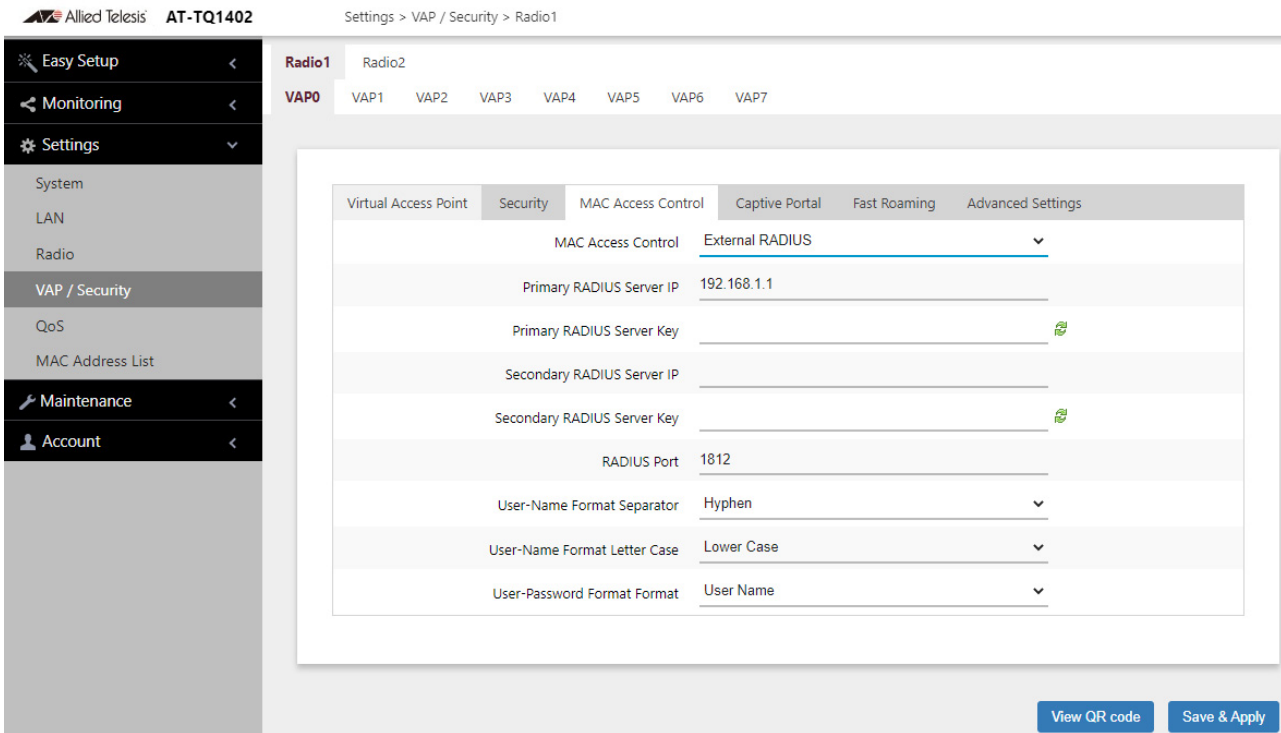


Figure 44. External RADIUS Fields

6. Configure the fields by referring to Table 28.

Table 28: External RADIUS Fields

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

Table 28: External RADIUS Fields (Continued)

Parameter	Description
User-Password Format Format	Specify the password for the MAC addresses. The choices are listed here: <ul style="list-style-type: none"> - User Name: The MAC addresses are used as the password. If you select this option, wireless access points send the MAC addresses as both the user-name and user-password attributes of the clients to the servers. This is the default. - Fixed: A fixed value is used as the password for all MAC addresses. Selecting this option displays the User-Password Format Password field. Refer to Figure 45.
User-Password Format Password	Enter the fixed password for the MAC addresses. This field only applies to the Fixed setting in the User-Password Format Format option. The password is case sensitive.



The screenshot shows a configuration interface. At the top, there is a dropdown menu labeled 'User-Password Format Format' with the option 'Fixed' selected. Below this, a text input field labeled 'User-Password Format Password' is visible, indicating that the 'Fixed' option is active.

Figure 45. User-Password Format Password

7. Click the **SAVE & APPLY** button to save and update the configuration, or click **VIEW QR CODE** to generate a QR Code.

Configuring VAP Fast Roaming

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

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

To configure fast roaming, perform the following procedure:

1. Select **Settings > VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Fast Roaming** tab. Refer to Figure 46.

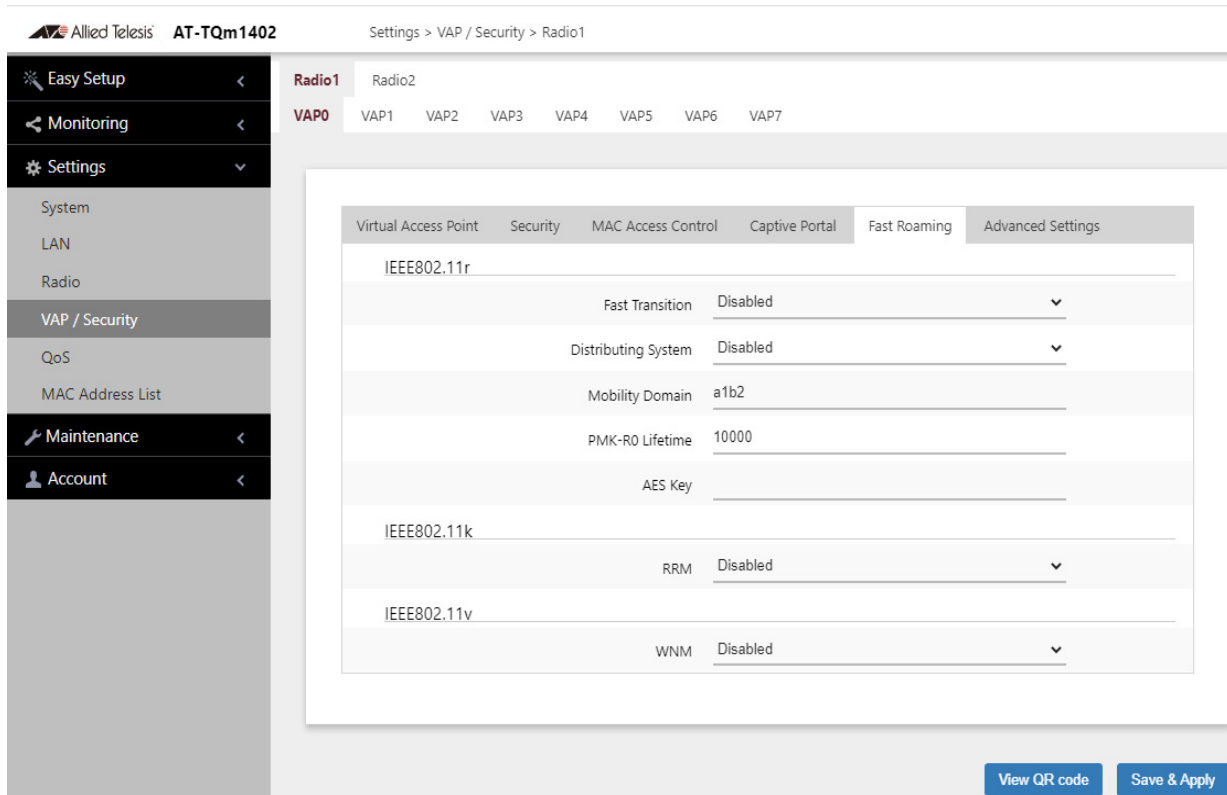


Figure 46. Fast Roaming Window

5. Configure the fields by referring to Table 29.

Table 29. Fast Roaming Window

Field	Description
IEEE802.11r Fast Transition	Refer to the Vista Manager EX and AT-Vista Manager EX AWC documentation for descriptions of these parameters.
802.11k RRM	Select one of the following: <ul style="list-style-type: none"> - Enabled: Activates IEEE 802.11k Radio Resource Measurement (RRM). - Disabled: Deactivate RRM. This is the default.
802.11v WNM	Select one of the following: <ul style="list-style-type: none"> - Enabled: Activates IEEE 802.11v Wireless Network Management (WNM). - Disabled: Deactivates WNM. This is the default.

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

Configuring Advanced VAP Settings

To configure advanced VAP settings, perform the following procedure:

1. Select **Settings > VAP / Security** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. The default is Radio1. You can configure only one radio at a time.
3. Select a VAP to configure from the next sub-menu. The default is VAP0. You can configure only one VAP at a time.
4. Select the **Advanced Settings** tab. See Figure 46.

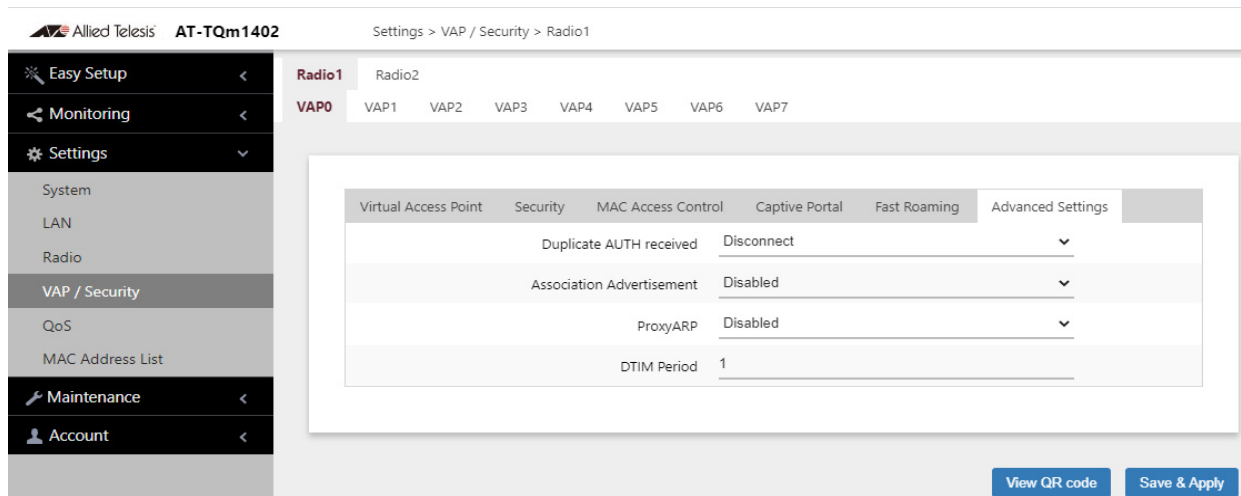


Figure 47. Advanced VAP Settings Window

5. Configure the fields by referring to Table 29.

Table 30. Advanced VAP Settings

Field	Description
Duplicate AUTH received	<p>Controls how the access point responds when it receives authentication requests from wireless clients that have already been authenticated. The options are:</p> <ul style="list-style-type: none"> - Disconnect: The access point responds to duplicate authentication requests by sending deauthentications and disconnecting the clients. This is the default. - Ignore: The access point responds to duplicate authentication requests by authenticating the clients again.

Table 30. Advanced VAP Settings (Continued)

Field	Description
Association Advertisement	<p>Select one of the following:</p> <ul style="list-style-type: none"> - Enabled: The access point notifies wireless clients when they are newly associated. With the association confirmation, wireless clients remove the information from previously associated access points. - Disabled: Deactivate the Association Advertisement feature. This is the default.
ProxyARP	Not available. This feature is disabled.
DTIM Period	<p>Controls the delivery traffic indication map (DTIM) period. This specifies the number of beacons an access point transmits before transmitting any buffered broadcast or multicast packets. This allows wireless clients that are in the Sleep Mode to wake up prior to receiving the packets. The range is 1 to 255 beacons. The default is 1 beacon.</p> <p>Specify the number of DTIM Period from 1 to 5.</p> <ul style="list-style-type: none"> - When the number is higher, the energy saving is more efficacious though the response becomes slow. - When the number is lower, the energy saving is less efficacious though the response becomes quick.

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

Configuring the MAC Address List

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

Here are the guidelines to the MAC address filter:

- ❑ The access point has only one MAC address filter.
- ❑ You can activate or deactivate the filter on individual VAPs.
- ❑ You need to know the MAC addresses of the wireless clients whose association requests the access point is to accept or reject.
- ❑ You need to know the VAPs where you want to activate the filtering. Activating filtering on VAPs is described in “Configuring Basic VAP Parameters” on page 111.

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

1. Select **Settings > MAC Address List**. Refer to Figure 48.

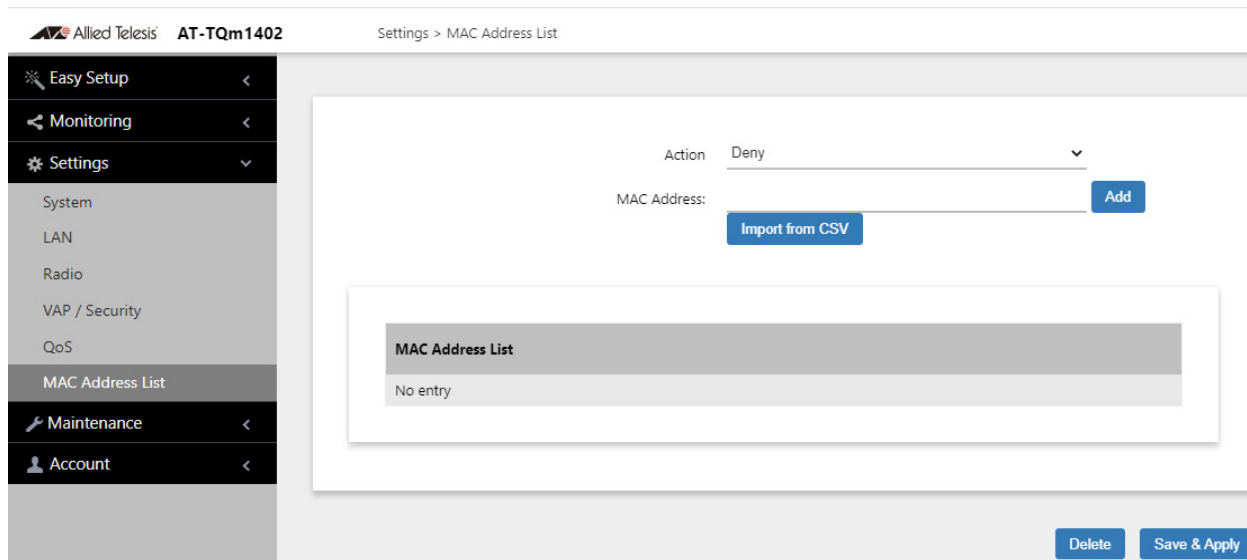


Figure 48. MAC Address List Window

2. From the Action pull-down menu, select one of the following:
 - Deny: Select this option to have the access point reject association requests from wireless clients whose MAC addresses you enter in the filter, and to accept association requests from all other clients. This is the default setting.
 - Allow: Select this option to have the access point accept association requests from the wireless clients whose MAC addresses you enter in the filter, and to reject association requests from all other clients.
3. To enter the MAC address of a wireless client the access point is to deny or accept, click the **MAC Address** field and enter the address, in this format xx:xx:xx:xx:xx:xx.
4. Click the **Add** button. You can enter only one address at a time. You cannot enter broadcast or multicast addresses.
5. To remove addresses, do one of the following:
 - To delete MAC addresses individually, click the check boxes of the addresses in the list and click the Delete button.
 - To delete all the addresses, click the check box to the right of the MAC Address List title and click the Delete button
6. Click the **SAVE & APPLY** button to save and update the configuration.

Displaying VAP and LAN Ports Statistics

To view VAP and LAN ports status and statistics, select **Monitoring > Statistics** window. Refer to Figure 49.

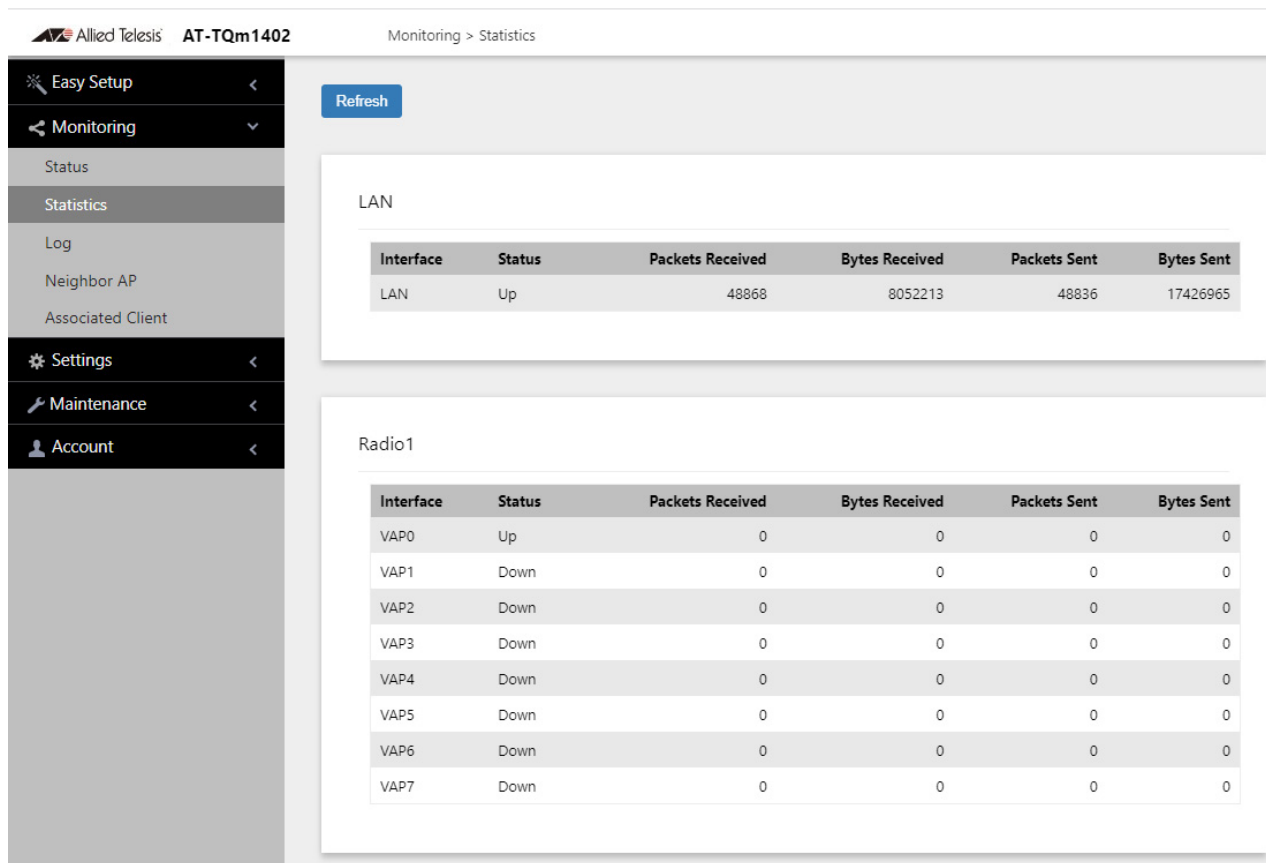


Figure 49. Statistics Window

The columns are defined in Table 31.

Table 31. Statistics Window

Column	Description
Interface	Displays LAN1 and LAN 2 ports, and VAPs 0 to 7).
Status	Displays the status (up or down) of the interface.
Packets Received	Displays the total number of packets received on the interface.
Bytes Received	Displays the total number of bytes received on the interface.

Table 31. Statistics Window (Continued)

Column	Description
Packets Sent	Displays the total number of packets transmitted on the interface.
Bytes Sent	Displays the total number of bytes transmitted on the interface.

Chapter 7

Quality of Service

This chapter describes the following procedures:

- ❑ “Introduction to Quality of Service” on page 156
- ❑ “Configuring QoS Basic Settings” on page 158
- ❑ “Configuring AP EDCA Parameters” on page 159
- ❑ “Configuring Station EDCA Parameters” on page 162

Introduction to Quality of Service

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

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

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

1. Select **Settings** > **QoS** from the main menu.
2. Select **Radio1** or **Radio2** from the sub-menu. You can configure only one radio at a time. Refer to Figure 50 on page 157.
3. Configure the QoS parameters by referring to the following sections:
 - ❑ “Configuring QoS Basic Settings” on page 158
 - ❑ “Configuring AP EDCA Parameters” on page 159
 - ❑ “Configuring Station EDCA Parameters” on page 162
4. Click the **SAVE & APPLY** button to save and update your configuration.

Allied Telesis **AT-TQ1402** Settings > QoS

Monitoring < Settings > System LAN Radio VAP / Security **QoS** MAC Address List Maintenance < Account <

Radio1 Radio2

Basic Settings

WiFi Multimedia(WMM) Enabled

No Acknowledgement Disabled

APSD Disabled

Advanced Settings

AP EDCA Parameters

	AIFS	cwMin	cwMax	Max. Burst
Data 0 (Voice)	1	3	7	1.5
Data 1 (Video)	1	7	15	3
Data 2 (Best Effort)	3	15	63	0
Data 3 (Background)	7	15	1023	0

Station EDCA Parameters

	AIFS	cwMin	cwMax	TXOP Limit
Data 0 (Voice)	2	3	7	47
Data 1 (Video)	2	7	15	94
Data 2 (Best Effort)	3	15	1023	0
Data 3 (Background)	7	15	1023	0

Save & Apply

Figure 50. QoS Window

Configuring QoS Basic Settings

The fields for the Basic Settings section are defined in Table 32.

Table 32. QoS Window - Basic Settings

Parameter	Description
WiFi Multimedia (WMM)	<p>Enable or disable QoS prioritizing and coordination. Here are the settings:</p> <ul style="list-style-type: none"> - Enabled: The access point uses the AP EDCA settings to control the flow of downstream traffic to the wireless clients and the station EDCA parameters to control the flow of upstream traffic from the clients. This is the default setting. - Disabled: QoS control of the upstream traffic from the clients is disabled. You can still configure some of the parameters that control the downstream traffic from the access point to the clients. <p>WMM must be enabled on radios that use IEEE 802.11n or IEEE 802.11ac.</p>
No Acknowledgment	<p>Control whether the access point acknowledges frames that have QoSNoAck for their service class values from wireless clients. Here are the settings:</p> <ul style="list-style-type: none"> - Enabled: The access point does not acknowledge frames that have QoSNoAck for their service class values. - Disabled: The access point acknowledges frames that have QoSNoAck for their service class values. This is the default setting.
APSD	<p>Enable or disable Automatic Power Save Delivery (APSD), which allows wireless clients to enter standby or sleep mode to conserve their battery. The options are:</p> <ul style="list-style-type: none"> - Enabled - Disabled: This is the default setting.

Configuring AP EDCA Parameters

Table 33 defines the AP EDCA parameters in the QoS window in Figure 50 on page 157.

Table 33. QoS Window - AP EDCA Parameters

Parameter	Description
Data Type (Queue)	<p>Lists the four egress queues:</p> <ul style="list-style-type: none"> - Data 0 (Voice): High priority queue, with low latency and guaranteed bandwidth. The queue is used to store time-sensitive data, such as VOIP and streaming media. - Data 1 (Video): High priority queue, with minimum delay. The queue is used to store time-sensitive data, such as video traffic. - Data 2 (best effort): Medium priority queue, with minimum throughput and delay. The queue is used to store most traditional IP data. - Data 3 (Background): Lowest priority queue, with high throughput. This queue is used for bulk data that requires maximum throughput and is not time-sensitive, such as FTP packets.
AIFS (InterFrame Space)	<p>Select the Arbitration Inter-Frame Spacing (AIFS) value to control the amount of time the access point waits after transmitting a frame and before transmitting the next frame. Queues with shorter wait times have higher priorities than queues with longer wait times. Here are the guidelines:</p> <ul style="list-style-type: none"> - The wait time is measured in slots. - The range is 1 to 15 slots. - The defaults are 1 for Data 0 and Data 1, 3 for Data 2, and 7 for Data 3.

Table 33. QoS Window - AP EDCA Parameters (Continued)

Parameter	Description
cwMin (Minimum Contention Window)	<p>Enter a value (in milliseconds) to be the lower limit of the range from which the access point determines the initial random back-off wait time for resending packets during transmission conflicts. Here are the guidelines:</p> <ul style="list-style-type: none"> - The access point generates the first random number between 0 and this number. - If the first random back-off wait time expires before the data frame is sent, a retry counter is increased and the random back-off value (window) is doubled. Doubling continues until the size of the random back-off value reaches the number defined in the maximum contention window. - Valid values for this parameter are: 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. - This parameter must be lower than the cwMax value. - The defaults are 3 for Data 0, 7 for Data 1, and 15 for Data 2 and Data 3.
cwMax (Maximum Contention Window)	<p>Select the maximum contention window, which is the upper limit (in milliseconds) for doubling the random back-off value. The doubling continues until either the data frame is sent or the maximum contention size is reached. Once the maximum contention window is reached, retries continue until a maximum number of retries is reached. Here are the guidelines:</p> <ul style="list-style-type: none"> - This parameter must be greater than or equal to the cwMin value. - Valid values are: 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. - The default values are 7 for Data 0, 15 for Data 1, 63 for Data 2, and 1023 for Data 3.

Table 33. QoS Window - AP EDCA Parameters (Continued)

Parameter	Description
Max. Burst	<p>Specifies the maximum burst length (in seconds) for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. The decreased overhead results in higher throughput and better performance. Here are the guidelines:</p> <ul style="list-style-type: none"> - This is an AP EDCA parameter only and as such applies only to egress traffic from the access point to the wireless clients. - The factory defaults are 1.5 for Data 0, 3.0 for Data 1, and 0 for Data 2 and Data 3. - The range is 0.0 to 8.1 seconds.

Configuring Station EDCA Parameters

Table 34 defines the Station EDCA parameters in the QoS window in Figure 50 on page 157.

Table 34. QoS Window - Station EDCA Parameters

Parameter	Description
Data Type (Queue)	Specifies the four ingress queues: <ul style="list-style-type: none"> - Data 0 (Voice) - High priority queue, with minimum delay. The queue is used to store time-sensitive data, such as VOIP and streaming media. - Data 1 (Video): High priority queue, with minimum delay. The queue is used to store time-sensitive data, such as video traffic. - Data 2 (best effort): Medium priority queue, with minimum throughput and delay. The queue is used to store most traditional IP data. - Data 3 (Background): Lowest priority queue, with high throughput. This queue is used for bulk data that requires maximum throughput and is not time-sensitive, such as FTP packets.
AIFS (InterFrame Space)	Select the Arbitration Inter-Frame Spacing (AIFS) value to control the wait time for data frames. The wait time is measured in slots and has the range 1 to 15 slots. The defaults are listed here: 2 for Data 0 and Data 1, 3 for Data 2, and 7 for Data 3.

Table 34. QoS Window - Station EDCA Parameters (Continued)

Parameter	Description
cwMin (Minimum Contention Window)	<p>Enter a value (in milliseconds) to be the lower limit of the range from which the station determines the initial random back-off wait time for resending packets during transmission conflicts. Here are the guidelines:</p> <ul style="list-style-type: none"> - The first random number the station generates will be between 0 and this number. - If the first random back-off wait time expires before the data frame is sent, a retry counter is increased and the random back-off value (window) is doubled. Doubling continues until the size of the random back-off value reaches the number defined in the maximum contention window. - This parameter must be less than or equal to the cwMax value. - Valid values for this parameter are: 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023 milliseconds. - The defaults are 3 for Data 0, 7 for Data 1, and 15 for Data 2 and Data 3.
cwMax (Maximum Contention Window)	<p>Select the maximum contention window, which is the upper limit (in milliseconds) for doubling the random back-off value. The doubling continues until either the data frame is sent or the maximum contention size is reached. Once the maximum contention window is reached, retries continue until a maximum number of retries is reached. Here are the guidelines:</p> <ul style="list-style-type: none"> - This parameter must be greater than or equal to the cwMin value. - Valid values are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023 milliseconds. - The default values are 7 for Data 0, 15 for Data 1, and 1023 for Data 2 and Data 3.

Table 34. QoS Window - Station EDCA Parameters (Continued)

Parameter	Description
TXOP Limit	<p>Select the Transmission Opportunity (TXOP) limit. It defines the time intervals that a WME client has the right to initiate transmission to the access point. Here are the guidelines:</p> <ul style="list-style-type: none">- The time intervals are in 32 microseconds.- The range is 0 to 256 intervals.- The default intervals are 47 for Data 0, 94 for Data 1, and 0 for Data 2 and Data 3.

Chapter 8

LAN Port

This chapter describes the following procedures:

- ❑ “Configuring the Management VLAN” on page 166
- ❑ “Displaying the Status of LAN Port” on page 168
- ❑ “Displaying the Status of LAN Port” on page 168

Configuring the Management VLAN

Here are the guidelines to setting the management VLAN:

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

Note

Changing the management VLAN might end your management session.

To configure the management VLAN, perform the following procedure:

1. Select **Settings** > **LAN** from the main menu. Refer to Figure 51.

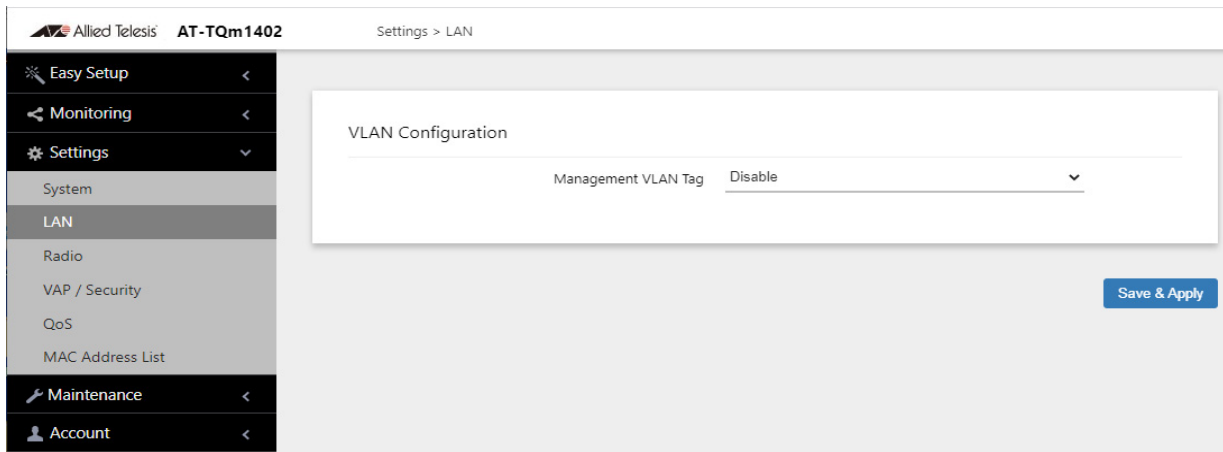


Figure 51. LAN Settings Window

2. Configure the settings by referring to Table 35 on page 167.

Table 35. LAN Settings Window - VLAN Configuration Section

Parameter	Description
Management VLAN Tag	Select one of the following: <ul style="list-style-type: none"><li data-bbox="824 390 1414 422">- Enabled: Activates the management VLAN.<li data-bbox="824 443 1458 474">- Disabled: Deactivates the management VLAN.

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

Displaying the Status of LAN Port

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

1. Select **Monitoring > Status** from the main menu.
2. Select **LAN** from the sub-menu. See Figure 52.

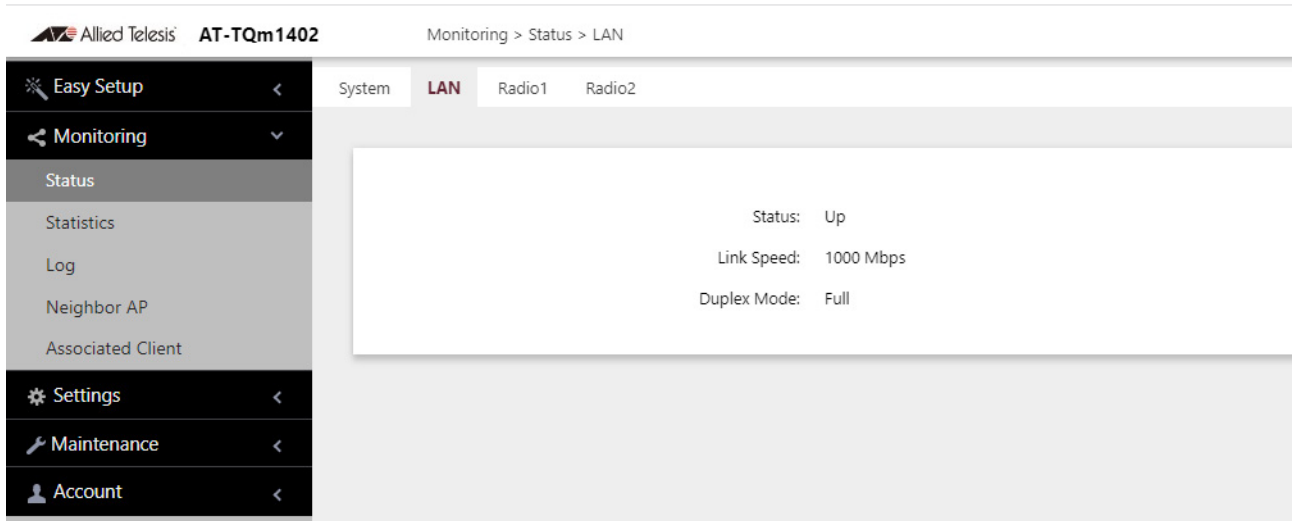


Figure 52. LAN1 Window

The fields are defined in Table 36.

Table 36. LAN1 or LAN2 Window

Item Name	Description
Status	Displays the status of the LAN1 port. The possible states are listed here: <ul style="list-style-type: none"> - Up: The port has established a link with a network devices, such as an Ethernet switch or router. - Down: The port has not established a link with a network device.
Link Speed	Displays the speed of the link (10 Mbps, 100 Mbps, 1000 Mbps).

Table 36. LAN1 or LAN2 Window (Continued)

Item Name	Description
Duplex Mode	Displays the duplex mode of the port, as follows: <ul style="list-style-type: none">- Full: Full-duplex.- Half: Half-duplex.

Chapter 9

Wireless Distribution System Bridges

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

- ❑ “Introduction to Wireless Distribution System Bridges” on page 172
- ❑ “WDS Bridge Elements” on page 174
- ❑ “Guidelines” on page 176
- ❑ “Preparing Access Points for a WDS Bridge” on page 177

Introduction to Wireless Distribution System Bridges

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

A WDS bridge consists of one parent and children. The parent is connected to the wired network through its LAN ports. The children function as wireless clients of the parent, communicating with the wired network over the WDS bridge to the parent.

Note

Allied Telesis supports only one child per parent for a WDS bridge built with the TQ1402 and TQm1402 access points.

An example of a parent and a child is shown in Figure 53.

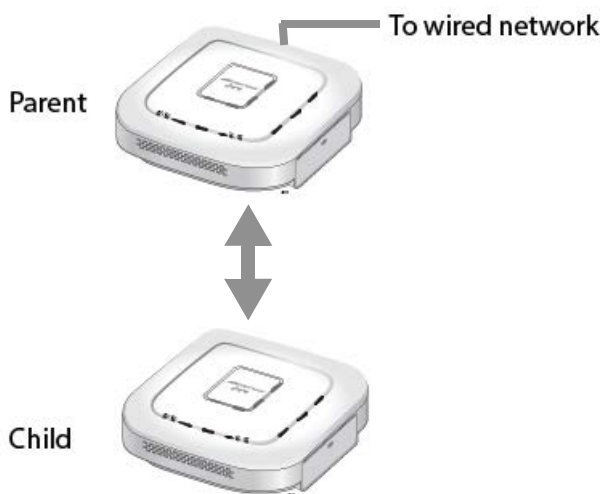


Figure 53. WDS Bridge

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

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

should use other radios to access the network. Additionally, because the access points have to use the same channel, you have to select the channel manually, instead of using the default auto channel setting. In the example in Figure 54, the parent and child are using Radio2 and channel 40 for the WDS bridge. Wireless clients can access the network using Radio1.

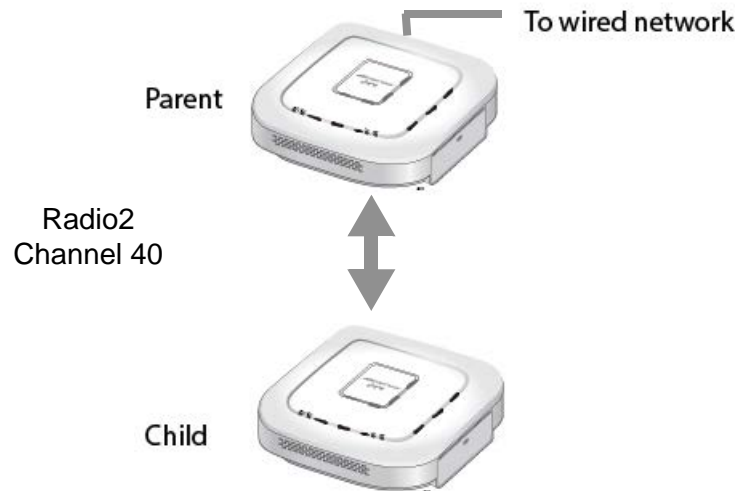


Figure 54. Example of Radio and Channel Assignments in a WDS Bridge

WDS Bridge Elements

This section describes the various elements of a WDS bridge.

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

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

VAP0 The WDS bridge uses VAP0 on the selected radio as the wireless link. The VAP assignment cannot be changed. VAP1 to VAP7 are automatically disabled. Wireless clients should not be allowed to use VAP0 of the designated radio when the devices are arranged in a WDS bridge because the bridge might experience a reduction in performance. Instead, wireless clients should use the other radios and VAPs to access the network.

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

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

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

Parent and Child When configuring an access point for a WDS bridge, you designate it as either parent or child. The parent is usually a unit with its LAN port connected to the wired network. The child is a unit that accesses the wired network through the parent.

Note

Allied Telesis supports only one child per parent for a WDS bridge built with the TQ1402 and TQm1402 access points.

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

- No encryption
- WPA Personal (WPA3 is not supported for a WDS bridge.)

Note

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

**Dynamic
Frequency
Selection**

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

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

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

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

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

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

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

Guidelines

Here are the guidelines for WDS bridges:

- ❑ A WDS bridge can have two wireless access points.
- ❑ One access point is the parent and the other is the child.
- ❑ The LAN port on the parent is connected to the wired network.
- ❑ The TQ1402 or TQm1402 access point cannot be a parent and a child at the same time.
- ❑ The LAN port on a child should not be connected to the wired network.
- ❑ You can use Radio1 or Radio2 for the WDS bridge.
- ❑ You can use no security (none) or WPA Personal security for VAP0 on the selected radio of the bridge. Allied Telesis recommends using WPA Personal security.
- ❑ When WPA Personal is selected as the security mode, WPA3 or WPA2 and WPA3 cannot be selected as the WPA version.
- ❑ A WDS bridge can have both TQ1402 and TQm1402 access points.
- ❑ The radios of the WDS bridge have to be set to the same mode and channel.
- ❑ You must set the channel manually. Do not use the Auto setting.
- ❑ If you use Radio2 for the bridge, Allied Telesis recommends selecting a channel that is not part of dynamic frequency selection. This is to minimize the chance that the access points have to change channels and break the WDS bridge due to radar signals.
- ❑ A WDS bridge uses VAP0 on the selected radio as the communications link. The VAP should not be used by wireless clients. All other VAPs on the radio are disabled.
- ❑ The WDS bridge feature on these access points is not compatible with the same feature on other products from Allied Telesis or other companies.

Preparing Access Points for a WDS Bridge

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

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

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

1. Start a management session.
2. On the selected radio for the bridge, set the mode and channel. Refer to “Configuring Basic Radio Settings” on page 96. Here are the guidelines:
 - You can use any available radio mode for the bridge, but the radios in the different access points must use the same mode.
 - You can use any available channel, but the devices must use the same channel. Do not use the Auto setting.
3. Configure the security setting for VAP0 on the radio. The security setting can be none or WPA Personal. For instructions, refer to “Configuring VAP Security” on page 130.
4. Select **Settings > VAP / Security**.
5. Choose the radio for the WDS bridge by selecting **Radio1** or **Radio2** from the sub-menu.
6. Select **VAP0** from the sub-menu. This is the default VAP.
7. From the Mode pull-down menu, select either **WDS Parent** or **WDS Child**. This can only be set on VAP0.
8. Click the **SAVE & APPLY** button to save and update the configuration.

Note

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

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

When an access point is designated as a child, it automatically begins searching for a parent on the designated radio and channel. If it finds one, it forwards traffic from its wireless clients over the bridge to the parent, as needed, and transmits traffic from the parent to its clients. To view the children of a parent, display the Associated Clients window, as explained in “Displaying Associated Clients” on page 184.

Chapter 10

Monitoring

This chapter has the following procedures:

- ❑ “Displaying Basic System Information” on page 180
- ❑ “Displaying Neighboring Access Points” on page 183
- ❑ “Displaying Associated Clients” on page 184

Displaying Basic System Information

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

1. Select **Monitoring > Status** from the main menu.
2. Select **System** from the sub-menu. This is the default window. Refer to Figure 55.

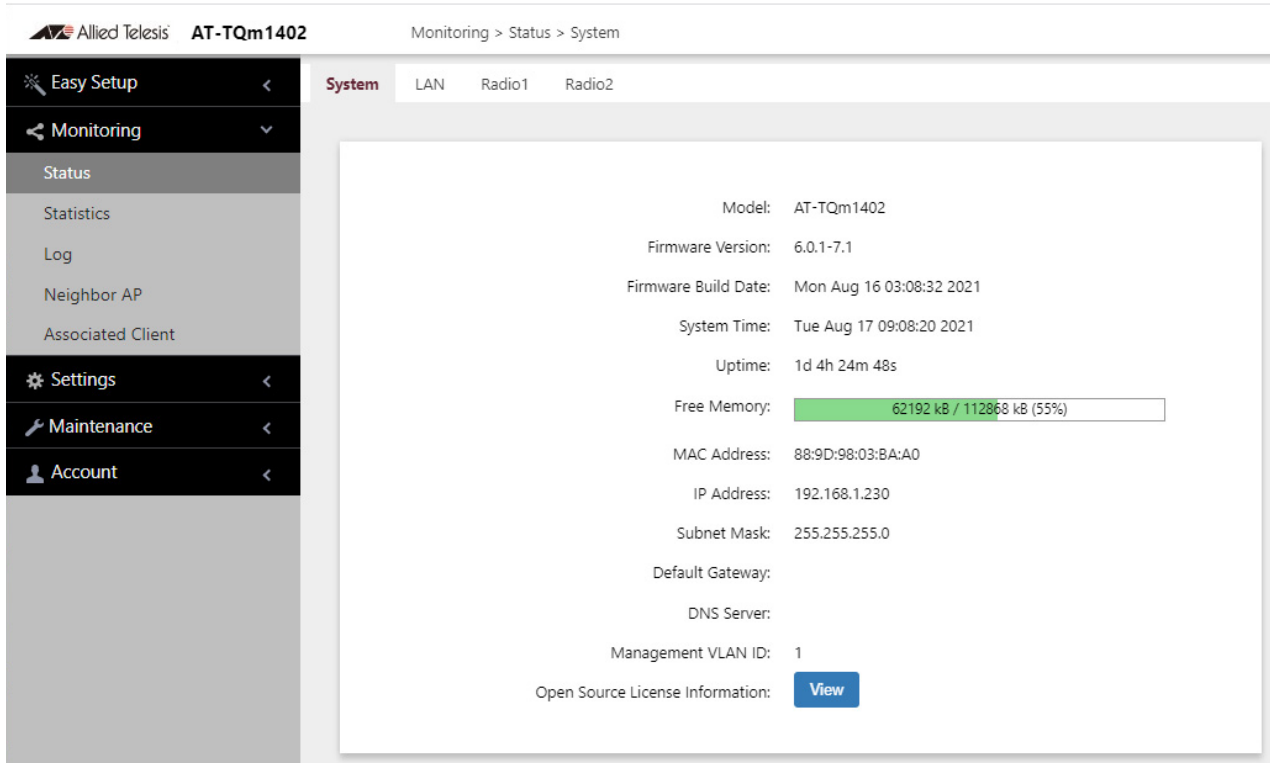


Figure 55. System Window

The fields are defined in Table 37.

Table 37. System Window

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

Table 37. System Window (Continued)

Item Name	Description
System Time	Displays the date and time. To set the date and time, refer to “Manually Setting the Date and Time” on page 74 or “Setting the Date and Time with the Network Time Protocol (NTP)” on page 71.
Uptime	Displays the number of hours, minutes, and seconds that have elapsed since the unit was last reset or powered on.
Free Memory	<p>Displays the amount of free memory in the access point, as follows:</p> <ul style="list-style-type: none"> - The first value is the total amount of unused memory, in KB. - The second value is the total amount of memory, in KB. - The last number in parentheses is the percentage of total memory that is free.
MAC Address	Displays the MAC address of the access point and radio 1. Radios 2 and 3 have different MAC addresses. You cannot change the MAC addresses.
IP Address	Displays the IP address of the access point. To set this value, refer to “Assigning a Dynamic IP Address from a DHCP Server” on page 66 or “Assigning a Static IP Address to the Access Point” on page 69.
Subnet Mask	Displays the subnet mask. To set this value, refer to “Assigning a Dynamic IP Address from a DHCP Server” on page 66 or “Assigning a Static IP Address to the Access Point” on page 69.
Default Gateway	Displays the default gateway address. The default gateway is an IP address of an interface on a router or other Layer 3 routing device. It specifies the first hop to reaching the subnets or networks where your management devices, such as management workstations and syslog servers, reside. The access point can have only one default gateway. To set this value, refer to “Assigning a Dynamic IP Address from a DHCP Server” on page 66 or “Assigning a Static IP Address to the Access Point” on page 69.

Table 37. System Window (Continued)

Item Name	Description
DNS Server	Displays the current DNS server address. Refer to “Assigning a Dynamic IP Address from a DHCP Server” on page 66 or “Assigning a Static IP Address to the Access Point” on page 69.
Management VLAN ID	Displays the management VLAN ID. The default is 1. Refer to “Configuring the Management VLAN” on page 166.
Open Source License Information	When you click the View button, displays open source license information.

Displaying Neighboring Access Points

To view information about other access points that the access point has detected, select **Monitoring > Neighbor AP**, Refer to Figure 56.

Note

This feature requires activating the Neighbor AP Detection option on the radios, as explained in “Configuring Advanced Radio Settings” on page 100.

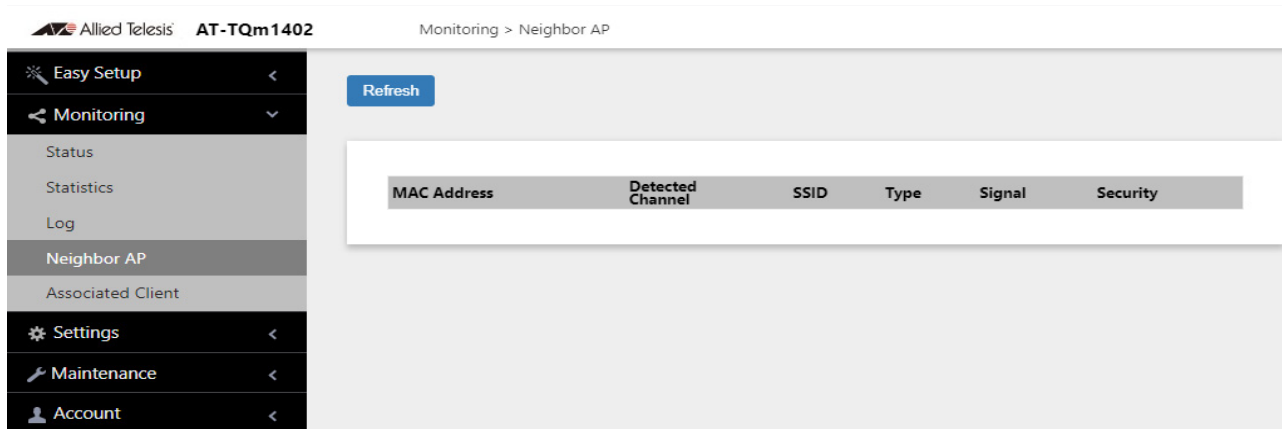


Figure 56. Neighbor AP Window

The columns are described in Table 38.

Table 38. Neighbor AP Window

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

Displaying Associated Clients

To view the active wireless clients on the VAPs of the access point, select **Monitoring > Associated Clients** from the main menu. Refer to Figure 57.

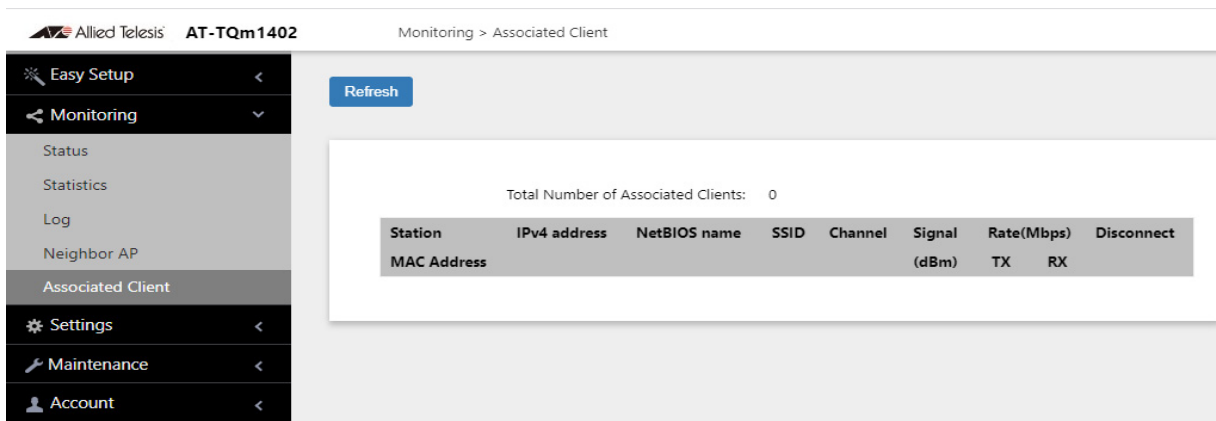


Figure 57. Associated Client Window

The columns are defined in Table 39.

Table 39. Associated Client Window

Column	Description
Station MAC Address	Displays the MAC addresses of associated clients.
IPv4 address	Displays the IPv4 address of associated clients. It will not be displayed when IPv6 is used.
NetBIOS name	Displays the NetBIOS name of associated clients. It will display "n/a" when NetBIOS name is not acquired or during the acquisition.
SSID	Displays the network name (SSIDs) to which the client is connected.
Channel	Displays the radio channel the client is using.
Signal	Displays the strength of the signal from the client.
Rate (Mbps)	Displays the transmission (Tx) and reception (Rx) rates in Mbps.
Disconnect	Displays the Disconnect button. Clicking the button disconnects the client.

Chapter 11

System Log

This chapter describes the system log in the following sections:

- ❑ “Displaying the System Log” on page 188
- ❑ “Sending Log Messages to a Syslog Server” on page 190

Displaying the System Log

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

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

The messages are divided into the eight severity levels listed in Table 40:

Table 40. Message Severity Levels

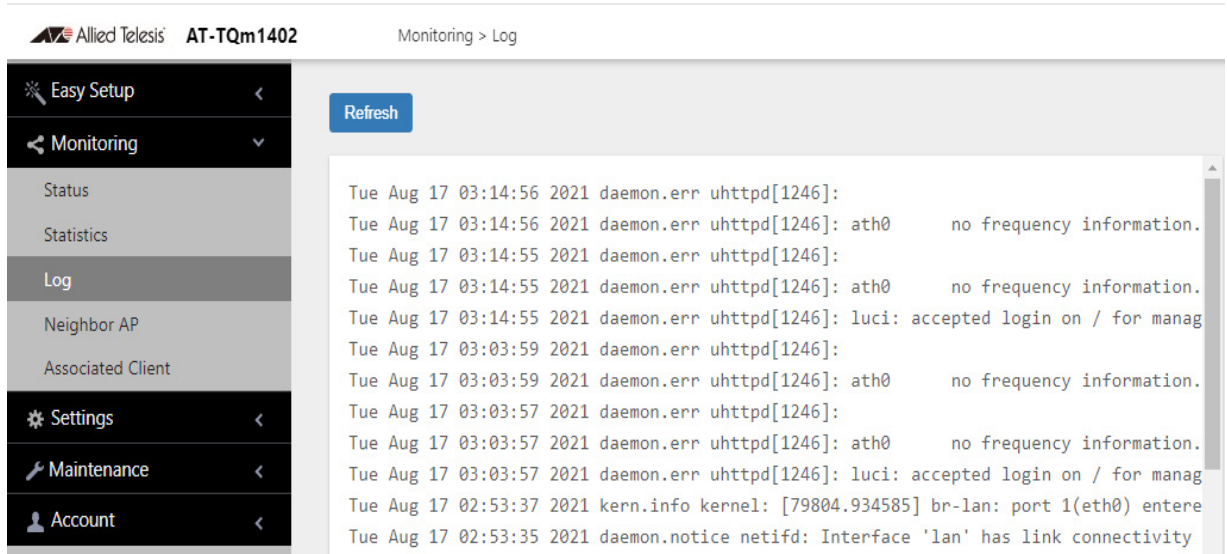
Severity Level	Description
0 - Emergency	System is unusable.
1 - Alert	State that must be dealt with immediately.
2 - Critical	Serious condition.
3 - Error	Error occurred
4 - Warning	Warning conditions exist.
5 - Notice	Normal but needs attention.
6 - Informational	Information message.
7 - Debug	Debug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

At its default setting, the log displays all messages. You can restrict the log to display only certain messages by adjusting the Severity parameter in the syslog client. Refer to “Sending Log Messages to a Syslog Server” on page 190.

Note

All messages are deleted from the log when the access point is reset or powered off. To permanently save the messages, refer to “Sending Log Messages to a Syslog Server” on page 190.

To view the system log, select **Monitoring > Log**, Figure 58 on page 189 is an example.



The screenshot shows the 'Monitoring > Log' page of the AT-TQm1402 device. On the left is a navigation menu with options: Easy Setup, Monitoring (selected), Status, Statistics, Log (highlighted), Neighbor AP, Associated Client, Settings, Maintenance, and Account. A 'Refresh' button is located above the log window. The log window displays a list of system messages with the following text:

```
Tue Aug 17 03:14:56 2021 daemon.err uhttpd[1246]:  
Tue Aug 17 03:14:56 2021 daemon.err uhttpd[1246]: ath0 no frequency information.  
Tue Aug 17 03:14:55 2021 daemon.err uhttpd[1246]:  
Tue Aug 17 03:14:55 2021 daemon.err uhttpd[1246]: ath0 no frequency information.  
Tue Aug 17 03:14:55 2021 daemon.err uhttpd[1246]: luci: accepted login on / for manag  
Tue Aug 17 03:03:59 2021 daemon.err uhttpd[1246]:  
Tue Aug 17 03:03:59 2021 daemon.err uhttpd[1246]: ath0 no frequency information.  
Tue Aug 17 03:03:57 2021 daemon.err uhttpd[1246]:  
Tue Aug 17 03:03:57 2021 daemon.err uhttpd[1246]: ath0 no frequency information.  
Tue Aug 17 03:03:57 2021 daemon.err uhttpd[1246]: luci: accepted login on / for manag  
Tue Aug 17 02:53:37 2021 kern.info kernel: [79804.934585] br-lan: port 1(eth0) entere  
Tue Aug 17 02:53:35 2021 daemon.notice netifd: Interface 'lan' has link connectivity
```

Figure 58. Log Window for Event Messages

Sending Log Messages to a Syslog Server

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

1. Select **Settings** > **System** from the main menu.
2. Select **Log** from the sub-menu. Refer to Figure 59.

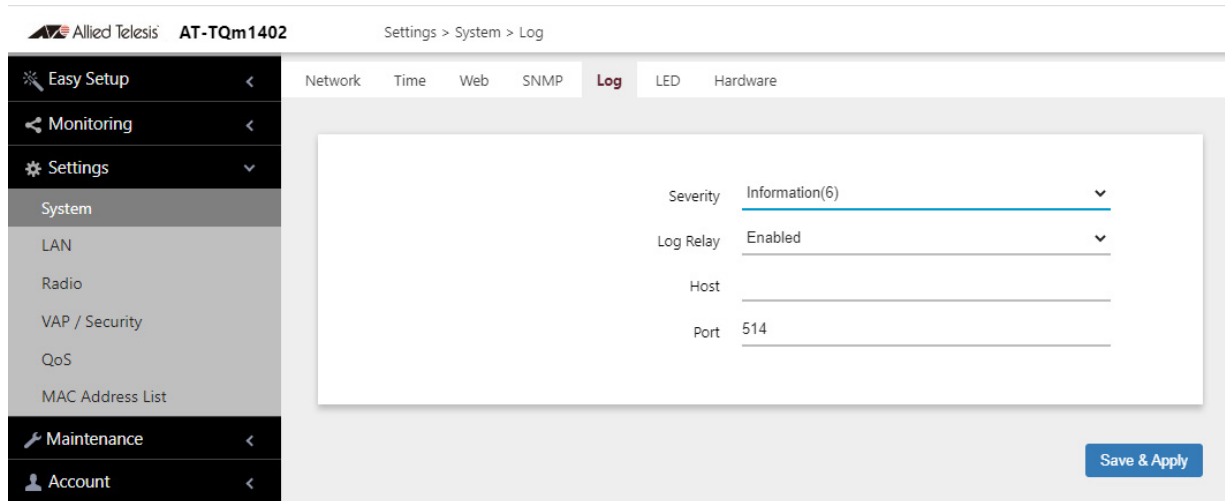


Figure 59. Log Window for Syslog Client

3. Configure the fields by referring to Table 41.

Table 41. Log Window for Syslog Client

Field	Description
Severity	<p>Select the severity of messages the access point is to display in the log file and transmit to the syslog server. The severity levels are listed in Table 40 on page 188. Here are the guidelines:</p> <ul style="list-style-type: none"> - You can specify only one severity level. - The severity level applies to both the messages displayed in the log file and transmitted to a syslog server. - The selected level includes that level and all numerically lower (higher severity) messages. For example, selecting level 3, error, designates system messages levels 0 to 3. - The default is level 7, debug. This is the highest value; it designates all messages.
Log Relay	<p>Select one of the following:</p> <ul style="list-style-type: none"> - Enabled: Activates the syslog client to transmit the event messages to your syslog server. - Disabled: Deactivates the syslog client to stop the access point from transmitting event messages. This is the default.
Host	<p>Enter the IP address (for example, 10.10.1.200) or host name (FQDN) of the syslog server. Here are the guidelines:</p> <ul style="list-style-type: none"> - You can enter only one host. - Do not include a subnet mask with IP address. - The factory default is blank. <p>Observe these guidelines when using an FQDN to identify the host:</p> <ul style="list-style-type: none"> - It cannot start or end with a hyphen. - Domain labels can have a maximum of 63 characters. - An FQDN can have up to 253 characters.
Port	<p>Enter the port number of the syslog server. The range is 1 to 65535. The default is 514.</p>

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

Chapter 12

Maintenance

This chapter has the following procedures:

- ❑ “Downloading the Configuration of the Access Point to Your Computer” on page 194
- ❑ “Restoring a Configuration to the Access Point” on page 196
- ❑ “Restoring the Default Settings to the Access Point” on page 197
- ❑ “Uploading New Management Software to the Access Point” on page 198
- ❑ “Rebooting the Access Point” on page 200
- ❑ “Collecting Technical Support Information to a File” on page 201

Downloading the Configuration of the Access Point to Your Computer

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

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

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

1. Select **Maintenance > Configuration** from the main menu. Refer to Figure 60.

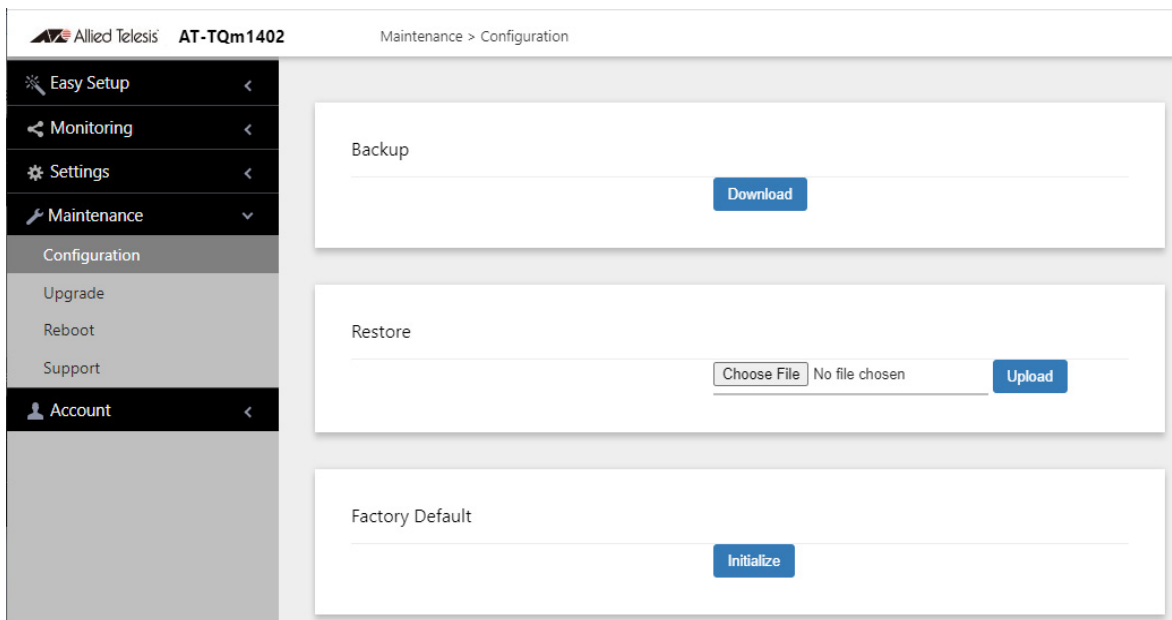


Figure 60. Configuration Window

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

4. If desired, change the filename of the configuration file. The filename suffix must be "txt".
5. Click the **Save** button.

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

Restoring a Configuration to the Access Point

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

- ❑ You can only restore configuration files that are created with “Downloading the Configuration of the Access Point to Your Computer” on page 194.
- ❑ A configuration file must have the “txt” suffix.
- ❑ You can restore a configuration file to multiple access points to give them the same configuration. However, if a configuration file has a static IP address, you should change the IP address of a device immediately after you restore a configuration to prevent an IP address conflict from occurring among the devices.
- ❑ You cannot edit a configuration file with a text editor.

Note

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

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

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

1. Select **Maintenance > Configuration** from the main menu. Refer to Figure 60 on page 194.
2. Click the **Choose File** button in the Restore section of the window and select the configuration file to restore to the access point from your management workstation or network server.
3. Click the **Open** button.
4. Click the **Upload** button.
5. Wait one minute for the access point to upload the file and reboot.
6. To resume managing the unit, establish a new management session.

Restoring the Default Settings to the Access Point

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

- ❑ The manager name and password are reset to “manager” and “friend”, respectively.
- ❑ If the access point currently has a static IP address, the address is deleted and the DHCP client is activated. If the device does not receive a response from a DHCP server on the LAN1 port, it uses the default IP address 192.168.1.230.

Note

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

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

1. Select **Maintenance > Configuration** from the main menu. Refer to Figure 60 on page 194.
2. Click the **Initialize** button in the Factory Default section of the window.
3. At the confirmation prompt, click **OK** to restore the default settings or **Cancel** to cancel the procedure.
4. After clicking OK, wait one minute for the device to reset, and afterwards establish a new management session. For instructions, refer to “Starting the First Management Session” on page 21.

Uploading New Management Software to the Access Point

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

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

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



Caution

Do not power off the access point during the firmware upgrade.



Caution

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

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

1. Select **Maintenance** > **Upgrade** from the main menu. Refer to Figure 61 on page 199.

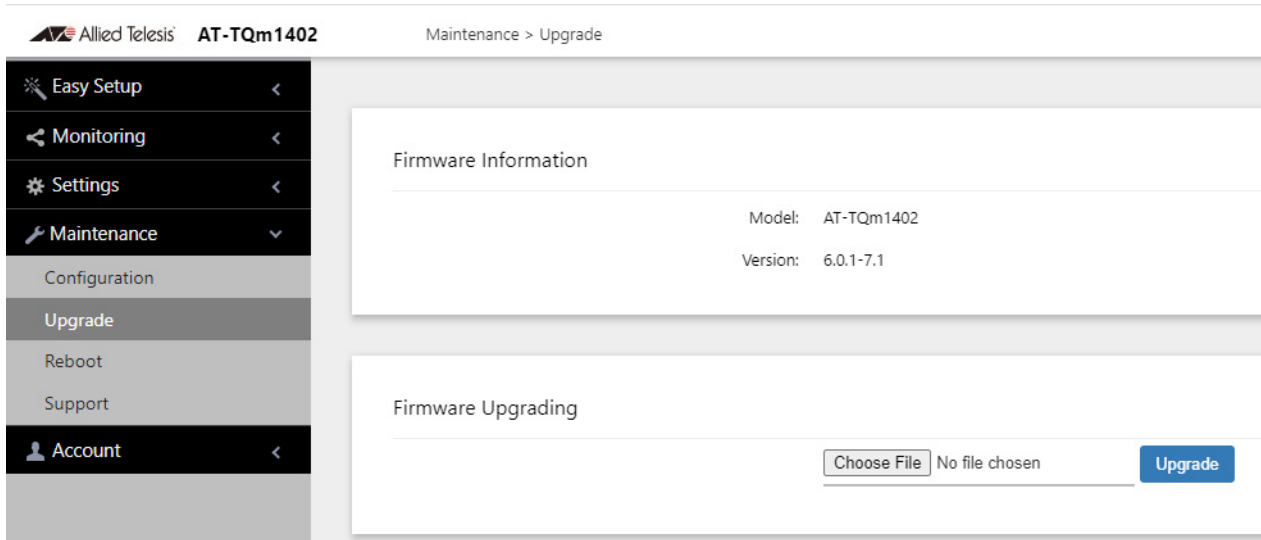


Figure 61. Upgrade Window

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

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

The access point displays a confirmation prompt.

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

Note

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

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

Rebooting the Access Point

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



Caution

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

To reboot the access point, perform the following procedure:

1. Select **Maintenance** > **Reboot** from the main menu. Refer to Figure 62.

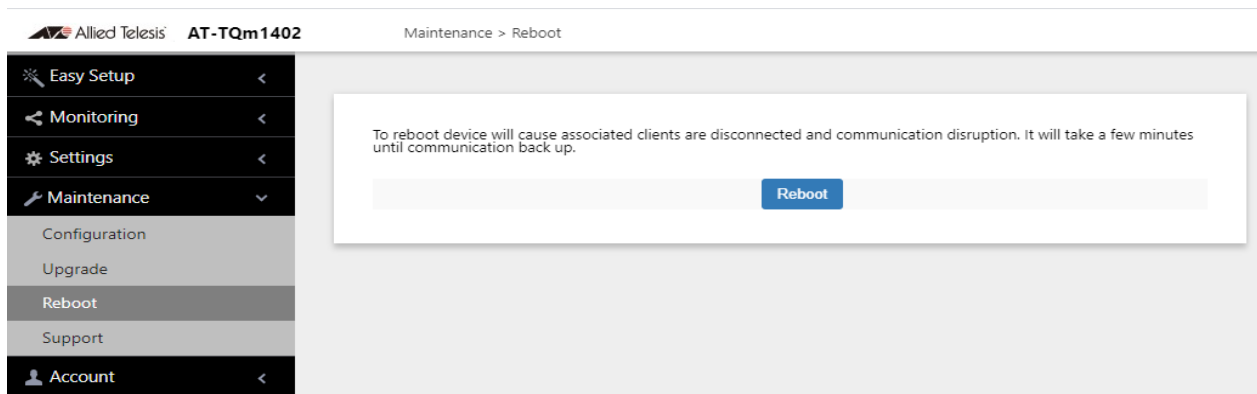


Figure 62. Reboot Window

2. Click the **Reboot** button.
The access point displays a confirmation prompt.
3. Click **OK**.
Your current management session is interrupted.
4. To resume managing the unit, wait one minute for it to complete initializing its management software and then start a new management session.

Collecting Technical Support Information to a File

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

Note

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

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

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

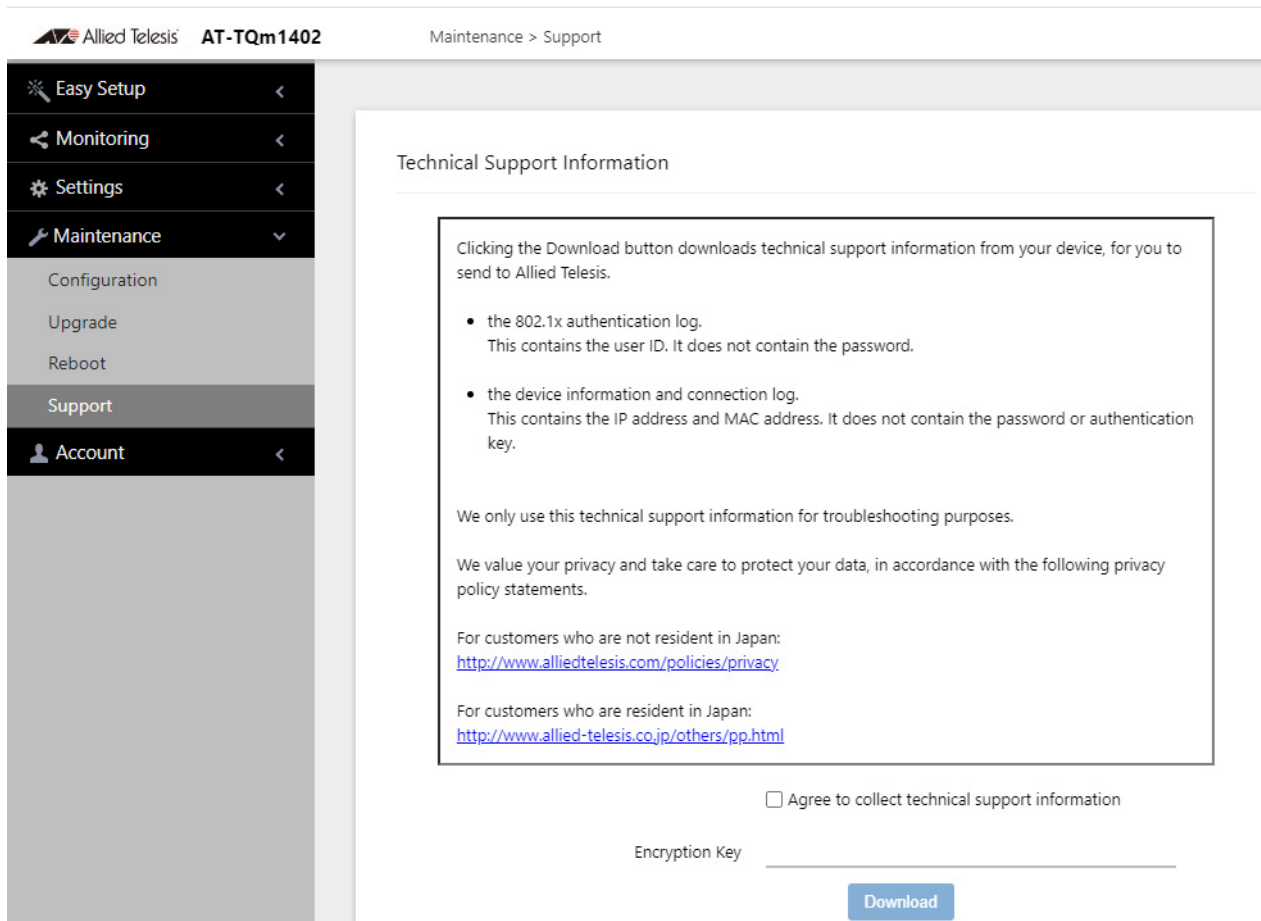


Figure 63. Support Window

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

3. After reading the privacy policy statement, click the check box for **Agree to collect technical support information** to permission to collect the technical support information.
4. If you want to send the file encrypted, enter an encryption key in the Encryption Key field. This step is optional. Here are the guidelines:
 - The key can be up to 32 alphanumeric characters.
 - It is case sensitive.
 - Spaces are not allowed.
 - Be sure to send the key to the technicians at Allied Telesis.
 - The factory default is blank. The file is sent in clear text if you do not enter a key.
5. Click the **Download** button.

Your web browser prompts you to save a zip file.
6. Save the zip file on your system.
7. Send the zip file to your Allied Telesis contact.