TQ5403 Wireless Access Point Series
Versions 6.0.1-5.2 and 6.0.1-6.1 Software Release Notes

Please read this document before using the management software. The document has the following sections:

Supported Platforms

The releases are supported on the following wireless access points:

- TQ5403
- TQm5403
- TQ5403e

For instructions on how to upgrade the management software on wireless access points, refer to the *TQ5403 Wireless Access Points Management Software User’s Guide*, available on the Allied Telesis Inc. web site at **www.alliedtelesis.com/support.**

The v6.0.1-5.2 firmware filenames are listed here:

- AT-TQ5403-6.0.1-5.2.img.zip
- AT-TQm5403-6.0.1-5.2.img.zip
- AT-TQ5403e-6.0.1-5.2.img.zip

The v6.0.1-6.1 firmware filenames are listed here:

- AT-TQ5403-6.0.1-6.1.img.zip
- AT-TQm5403-6.0.1-6.1.img.zip
- AT-TQ5403e-6.0.1-6.1.img.zip

Approved Countries

The TQ5403, TQm5403, and TQ5403e wireless access points are approved for use in the countries listed in Table 1. The table includes the initial firmware versions to support the countries.

Table 1: Approved Countries for the TQ5403, TQm5403, and TQ5403e Wireless Access Points

Country	TQ5403	TQm5403	TQ5403e
Australia	v5.0.0	v5.1.1	v5.3.0
Canada	v5.3.0	v5.3.0	v5.3.1
China	v5.3.1	N/A[1]	N/A
European Union	v5.0.0	v5.1.1	v5.3.0
Hong Kong	v5.1.0	v5.1.0	v5.3.1
India	v5.1.1	v5.1.1	v5.4.1
Israel	v5.4.1	N/A	N/A
Japan	v5.0.0	v5.1.1	v5.3.0
Korea	v5.2.0	v5.2.0	v5.3.1
Malaysia	v5.1.0	v5.1.0	v5.3.1
New Zealand	v5.0.0	v5.1.1	v5.3.0
Singapore	v5.1.0	v5.1.0	v5.3.1
Taiwan	v5.3.0	v5.3.0	v5.3.1
Thailand	v5.1.0	v5.1.0	v5.3.1
United States	v5.0.0	v5.1.1	v5.3.0
Vietnam	v5.2.0	v5.2.0	v5.3.1

1. Not available.

Note
The wireless access points support Dynamic Frequency Selection (DFS) on 5GHz channels designated by countries or regions as DFS channels.

Restored Features in v6.0.1-5.2

- The following features are restored in v6.0.1-5.2:
  - Channel Blankets (AWC-CB)
  - Smart Connect (AWC-SC)

  The features require Vista Manager EX and the AWC plug-in. Refer to the *Vista Manager EX and AWC Plug-in User Guide* for background information and instructions.

New Features in v6.0.1-5.2

- This release adds the new MAC Address + External RADIUS option to the on-board web browser interface and the AWC plug-in. The new option allows you to authenticate wireless clients by combining the on-board MAC address filter with a RADIUS server on your network. Refer to "MAC Filtering and RADIUS Server Authentication" on page 15 for details.
- This release lets you use the on-board web browser interface to download a CSV file with client MAC addresses to the MAC address filter. This simplifies the task of adding the same MAC addresses to multiple access points as well as restoring lists to replacement devices. Refer to "CSV Files for the MAC Address Filter" on page 23.
- The wireless access point features in Table 2 have been added to Vista Manager EX and the AWC plug-in, and AlliedWare Plus and the Wireless Manager.

Table 2: Features Added to Vista Manager EX and AlliedWare Plus

Feature	Description	Management Version Requirement
Hotspot 2.0 and WiFi Certified Passpoint	"Hotspot 2.0 and WiFi Certified Passpoint on Captive Portals" on page 20	Vista Manager EX v3.5.0 or AlliedWare Plus v5.5.0-2.3.3 or later
LAN1 and LAN2 ports (Static LAG, Cascade, and disabled settings)	*TQ5403 Wireless Access Points Management Software User's Guide*	Vista Manager EX v3.3.4 or AlliedWare Plus v5.5.0-1.3.4 or later
SNMPv3		Vista Manager EX v3.3.4 or AlliedWare Plus v5.5.0-1.3.4 or later
External authentication page redirection on Captive Portals	"External Authentication Page Redirection on Captive Portals" on page 17	Vista Manager EX v3.5.0 or AlliedWare Plus v5.5.0-1.3.5 or later
Virtual IP Address for Captive Portals	"Virtual IP Address for Captive Portals" on page 16	Vista Manager EX v3.5.0 or AlliedWare Plus v5.5.0-1.3.5 or later
RADIUS accounting on Captive Portals	"RADIUS Accounting on Captive Portals" on page 18	Vista Manager EX v3.5.0 or AlliedWare Plus v5.5.0-1.3.5 or later

Table 2: Features Added to Vista Manager EX and AlliedWare Plus (Continued)

Feature	Description	Management Version Requirement
Walled gardens on Captive Portals	"Walled Gardens on Captive Portals" on page 19	Vista Manager EX v3.5.0 or AlliedWare Plus v5.5.0-1.3.5 or later

- Wireless access points that receive duplicate authentication messages from clients that are already authenticated enter this message in their system logs: `kern.info kernel: {305.206692} Received duplicate authentication from STA` *`mac_address`*.

New Features in v6.0.1-6.1

- The Associated Clients window in the on-board web browser interface (Monitoring > Associated Clients) has changed. It now includes the total number of associated clients as well as their IPv4 addresses and NetBIOS names. Refer to "Associated Clients Window" on page 10 and the *TQ5403 Wireless Access Points Management Software User's Guide*.
- Access points now support the AMF Application Proxy in the AWC plug-in and AMF-SEC. The Application Proxy lets you authenticate wireless clients using AMF-SEC and assign them to dynamic or Quarantine VLANs. The option is controlled on the individual VAPs with the MAC Access Control tab in the VAP/Security window in the on-board web browser window. Refer to "MAC Access Control Selection" on page 11.
- The root and satellite access points in a Smart Connect network will now attempt to recover if there is a loss of wireless communications between them, or send an alert message to a Syslog server.
- Channel Blankets now support proxy ARP. The proxy ARP has to be configured with Vista Manager EX v3.5.0 or later and the AWC plug-in.
- Access points now support multiple authentication requests from clients in Channel Blankets. This prevents access points from blocking authenticated clients that send duplicate authentication requests.
- Access points no longer enter the "daemon debug atkkcpd[12576]" message in the System Log when Captive Portal is disabled.
- The MAC Filtering option in the web browser interface has been moved. In previous versions it was in the Virtual Access Point tab. It is now a separate tab in the VAP/Security window and renamed MAC Access Control. Refer to "MAC Access Control Selection" on page 11.
- The Captive Portal menu selection in the web browser interface has been moved. In previous versions it was an option in the Virtual Access Point tab. It is now a separate tab in the VAP/Security window. Refer to "Captive Portal Menu Selection" on page 12.

Resolved Issues in Version 6.0.1-5.2

General

- Access points stopped forwarding traffic after receiving their configurations from Smart Connect.
- Access points delayed transmission of the Bridge MIB for SNMP.
- Access points did not recover from incomplete firmware updates.
- ARP requests from access points to clients failed.
- During firmware updates, access points updated the bootloader even when it was unnecessary.
- The MAC address filter was unpredictable when the table was empty.
- Access points with IEEE802.111r fast roaming and dynamic VLANs assigned roaming clients to the wrong VLANs.
- Radios failed after access points with the OpenFlow protocol were upgraded from v5.x.x to v6.x.x.
- LLDP for PoE negotiation failed after access points were upgraded from v5.x.x to v6.x.x.
- Access points lost communications with the AWC plug-in after receiving calculation results.
- Access points failed to generate dump files after freezing or booting.
- Access points entered non-specific event messages in the system log for DHCP lease timing events.
- Access points did not initialize the on-board web browser management interface after booting,
- Access points added incorrect timestamps to dump files and the Technical Support output.
- SNMP could not be configured with both the on-board web browser interface and AWC plug-in.
- NTP synchronization failed after boot or power on.
- Access points did not validate the format of their static IPv4 addresses.
- Access points added unnecessary folders to memory for the Technical Support feature.
- The kernel log buffer was configured incorrectly.
- Client Isolation failed.

Channel Blankets

- Clients that sent RTS frames before connecting to Channel Blankets VAPs could not connect to VAPs.
- Channel Blankets that had large numbers of entering and exiting clients had traffic delays.
- Channel Blankets that had large volumes of broadcast packets on the management VLAN had traffic delays.
- Roaming clients lost connections to Channel Blankets.
- Access points that had both Smart Connect and Channel Blankets dropped clients.

- Access points booted or froze after receiving RTS frames from clients that had not connected to Channel Blankets VAPs.
- Access points that received large volumes of traffic from associated or unassociated clients on Channel Blankets stopped responding to management commands.
- Access points dropped authentication requests from clients.
- Access points dropped probe responses to roaming clients.
- Access points stopped responding to AWC.
- Access points froze because of roaming clients.
- LLDP together with link aggregation did not work correctly.

Smart Connect

- Radios managed with the AWC plug-in could not reestablish Smart Connect links.
- Radios managed with the AWC plug-in would unexpectedly restart and reload their Smart Connect configurations.

Resolved Issues in Version 6.0.1-6.1

General

- The windows in the on-board web browser interface displayed the copyright label incorrectly.
- You could not enable the Neighbor AP Detection feature on access points that were configured with DHCP Option 43 and that were not using the AWC plug-in.
- The Rx errors statistic in the Technical Support Information feature was incorrect.
- Previously, the QoS map of the Passpoint function in Vista Manager EX supported only two DSCP exceptions. Access points now support 0-21 DSCP exceptions.
- Fixed security issues.
- The on-board web browser interface and the AWC plug-in did not validate Passpoint settings.
- The Dynamic VLAN feature in WPA Enterprise security had memory issues.
- Satellite access points in Smart Connect networks had incorrect lists of candidate access points.
- Access points listed CCMP as a valid cipher suit for WPA3 Enterprise. This is changed to GCMP.
- Enabling LLDP added extraneous entries in the system log.
- Requesting the Bridge MIB caused SNMP to freeze.
- Access points stopped communicating with the AWC plug-in after firmware upgrades.
- Access points did not transmit Radio3 link traps from the LAN port.

Channel Blankets

- Channel Blankets that had large numbers of entering and exiting clients had traffic delays.
- Channel Blankets that had large volumes of broadcast packets on the management VLAN had traffic delays.

- Previously, floor maps in Channel Blankets displayed only connected clients. They now display both connected and unconnected clients.
- Access points stopped transmitting broadcast and multicast packets because of inconsistencies with the Group Temporal Key.
- Access points did not release distant clients to nearer access points.
- Access points froze after detecting inconsistent station information.
- Channel Blankets caused access points to freeze or boot.

Known Issues

General

- Access points do not synchronize Hostname and SNMP System Name.
- Access points might not save changes to the Secondary RADIUS Server Key.
- Access points might disconnect inactive clients several seconds before the Inactivity Timer expires.
- Do not disconnect clients on WDS children with the Associated Client window in the web browser interface.
- Access points might boot if there are inconsistencies in the hardware and software tables. These events are entered in the System Log as “kernel: Rebooting due to DMA error recovery.”
- Wireless clients might not be able to immediately reconnect after disconnecting when IEEE802.11w Management Frame Protection is enabled.
- IEEE802.11WW (MFP) in WPA Personal Security may cause delays in the handling of roaming clients.
- Do not set the Maximum Clients parameter in the web browser interface to more than 200 clients for the TQ5403 or TQ5403e access point, or 127 clients for the TQm5403 access point.
- Channels 12 and 13 are not activated in Auto Channel Selection when the Channel parameter is set to Auto.
- Access points that receive their IP addresses from DHCP servers might initially use their default IP address in SNMP traps and NTP requests when booted. This can occur when access points send SNMP and NTP packets before receiving their IP addresses from DHCP servers.
- Access points might increment the VAP Received Counter when there are no clients.
- Access points might fail to operate properly as AMF Guest nodes, affecting these features:
  - Recognition as an AMF guest node
  - Backup as an AMF Guest node
  - Recover as an AMF Guest node

  The issue can be resolved by linking down and linking up the connection between the access point and AMF member.
- Access points might transmit unnecessary packets from their radios when initializing the management software during boots.

- When booted, access points transmit two DHCP discover packets (untagged and tagged VID 1) if the Management VLAN tag setting is disabled.
- Management VLAN cannot use tagged VID 1. When VID for a VAP is set to other than 1, dynamic VLAN assignment cannot use VID 1 for RADIUS packets.
- Changing the Duplicate AUTH Received parameter in the Advanced Settings Tab from Ignore to Disconnect requires booting the access point to activate the change. You do not need to boot the access point after changing the setting from Disconnect to Ignore.
- Access points managed with the AWC plug-in might take one to two minutes to save their configurations.
- In rare cases, access points managed with the AWC plug-in might not be able to save their configurations, in which case Vista Manager displays an error message. Saving the configuration again is usually successful.
- Access points might prompt wireless clients to disconnect their wireless connections when saving and applying wireless settings. Clients that disconnect will have to reconnect again.
- You cannot set channels 10-13 on the 40MHz bandwidth on the 2.4GHz Radio1.
- Access points might boot if the radios or LAN ports freeze and stop transmitting.
- The Link up/down trap OID is invalid.
- SSIDs containing the “/” character are displayed incorrectly by the AWC plug-in.

Smart Connect (AWC-SC)

- The IP address 172.31.0.0/24 is reserved for the auto-discovery feature in Smart Connect.
- You cannot configure VAPs on radios reserved for Smart Connect.
- Smart Connect requires that all root and satellite access points have the same VID settings.
- Smart Connect cannot forward AMF Guest nodes. Thus, do not use Smart Connect on access points that are connected to AMF Guest nodes.
- Smart Connect and DHCP snooping should not be used on the same network. The results may be unpredictable.

OpenFlow Protocol

- This release does not support the OpenFlow protocol.

Channel Blankets (AWC-CB)

Caution
Do not operate Channel Blankets on access points that have different firmware versions. Network operations may be unpredictable. When updating wireless access points in networks where Channel Blankets are employed, Allied Telesis recommends disabling the feature on all access points first, and enabling Channel Blankets again after updating all units.

- Channel Blankets require a minimum of two access points. Channel Blankets of only one access point may operate unpredictably.
- The RADIUS attribute “Session-timeout” must be disabled in VAPs with Channel Blankets.

- Wireless access points in Channel Blankets might freeze if clients rapidly connect and disconnect from VAPs.
- The Technical Support Information feature might not work with Channel Blankets.
- IEEE802.11w (MFP) should be enabled on access points using Channel Blankets.
- Association Advertisements should be enabled on access points using Channel Blankets.
- Channel Blankets might drop broadcast packets during heavy traffic.
- Access points might not send the Clear to Send (CTS) signal when clients send the Ready to Send (RTS) signal, preventing clients from connecting to Channel Blankets.

Channel Blankets (AWC-CB) Settings

Observe the following guidelines when configuring access point radios for Channel Blankets:

- All radios in Channel Blankets have to have the same settings.
- The Management VLAN has to be disabled.
- These radio settings have to be configured as follows:
  - Band Steering - Disabled
  - Neighbor AP Detection - Disabled
  - Airtime Fairness - Disabled
  - RTS Threshold - 2347 octets (default)
- These VAP settings have to be configured as follows:
  - VAP VID - 1
  - Inactivity Timer - 300 seconds
  - Duplicate AUTH Received - Disconnect
  - Proxy ARP - Disabled
  - Captive Portal - Disabled
- When using WPA Personal, configure these settings as follows:
  - Broadcast Key Refresh Rate - 0 (zero, default)
  - Fast Roaming - disabled
- When using WPA Enterprise, configure these settings as follows
  - Broadcast Key Refresh Rate - 0 (zero, default)
  - RADIUS Accounting - disabled
  - Fast Roaming - disabled
  - Pre-authentication - disabled
  - Dynamic VLAN - disabled
  - RADIUS session-timeout - disabled
- IEEE802.11w (MFP) in WPA Personal Security is not supported in Channel Blankets.

Note
When booted or powered on, access points in Channel Blankets may take up to two minutes before forwarding traffic from wireless clients.

Undocumented Features

The following features are not documented in the current *TQ5403 Wireless Access Points Management Software User's Guide (revision D)*:

Associated Clients Window

The Monitoring > Associated Client window now includes the total number of associated clients on the wireless access point as well as the IPv4 addresses and, when possible, NetBIOS names. Refer to Figure 1.

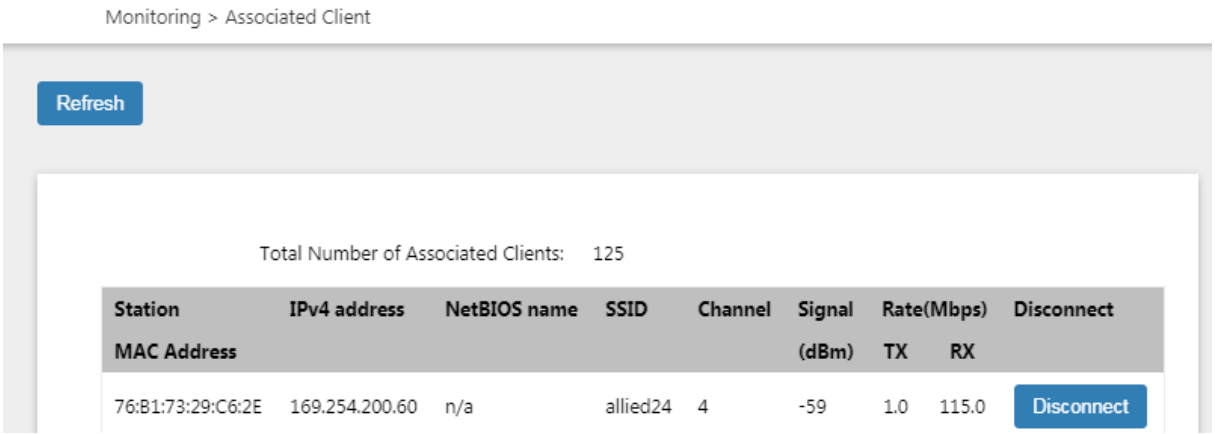

Figure 1. Associated Clients Window

MAC Access Control Selection

- The MAC Filtering menu selection option has moved and been renamed. In previous versions it was in the Virtual Access Point tab. It is now a separate tab in the VAP/Security window. Its new title is MAC Access Control. Refer to Figure 2.

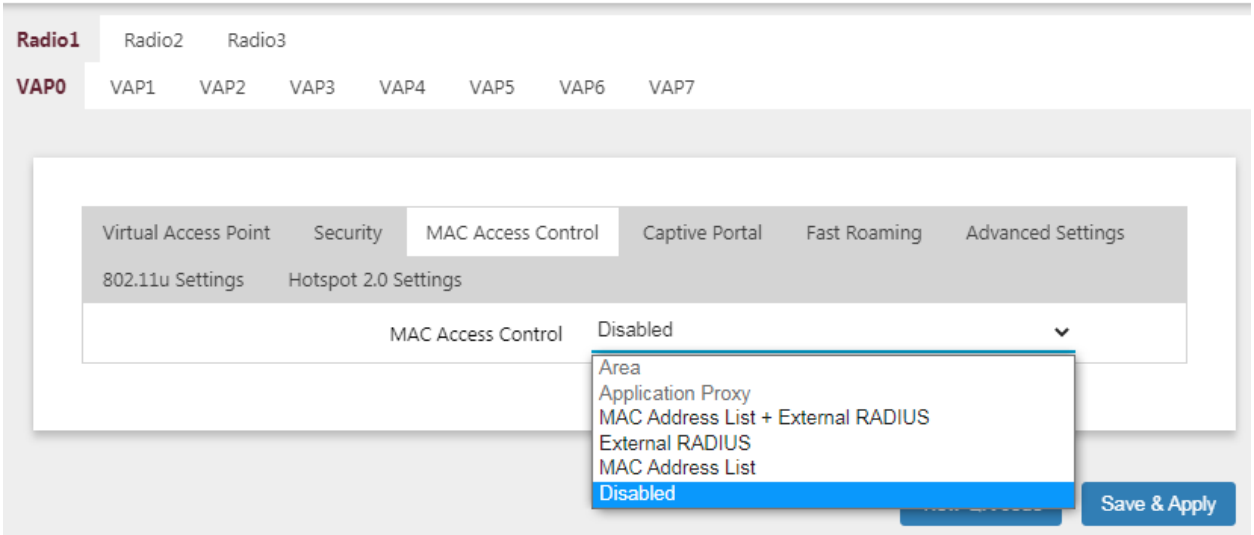

Figure 2. MAC Access Control Tab

The menu options are described in Table 3.

Table 3: MAC Access Control Menu

Menu Selection	Definition
Area	Authenticates wireless clients based on their MAC addresses and physical locations in Channel Blankets. Requires Vista Manager EX v3.2.1 or later and the AWC plug-in.
Application Proxy	Authenticates clients using the AMF Application Proxy in the AWC plug-in and AMF-SEC, Requires Vista Manager EX v3.6.0 or later and the AWC plug-in and AMF Security Controller (AMF-SEC) v2.2.0 or later.
MAC Address + External RADIUS	Authenticates MAC addresses of wireless clients by combining the on-board MAC address filter with a RADIUS server on your network. Refer to “MAC Filtering and RADIUS Server Authentication” on page 15.

Table 3: MAC Access Control Menu (Continued)

Menu Selection	Definition
External RADIUS	Authenticates MAC addresses of wireless clients with a RADIUS server on your network. Refer to the *TQ5403 Wireless Access Points Management Software User's Guide.*
MAC Address List	Authenticates MAC addresses of wireless clients using the MAC address filter in the access point. Refer to the *TQ5403 Wireless Access Points Management Software User's Guide*.
Disables	Disables MAC address authentication on the VAP.

Captive Portal Menu Selection

The Captive Portal menu selection has moved. In previous versions it was an option in the Virtual Access Point tab. It is now a separate tab in the VAP/Security window. Refer to Figure 3.

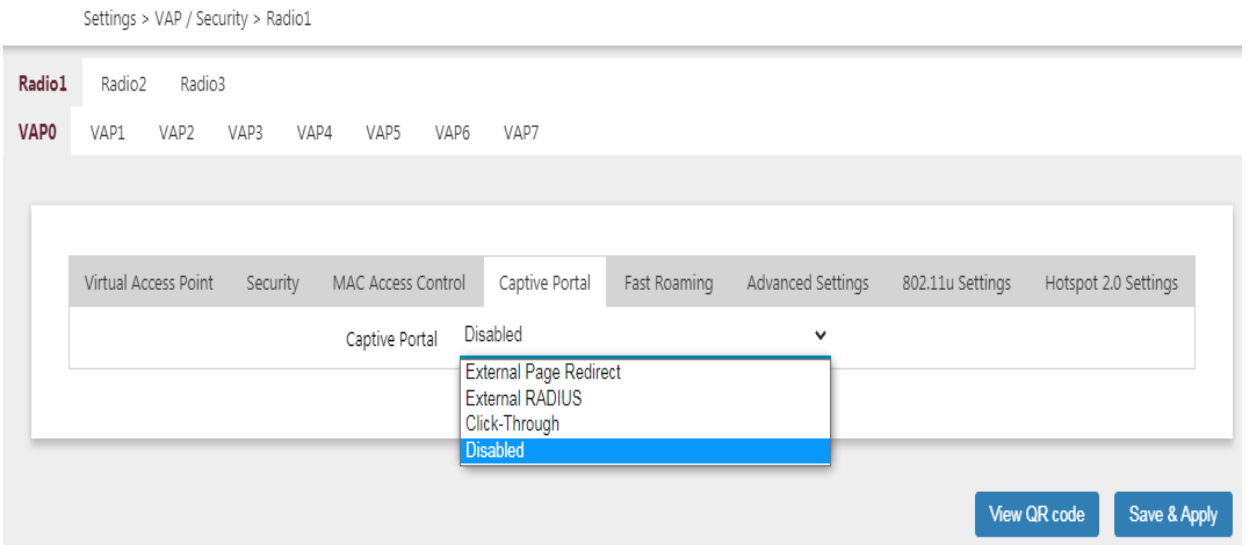

Figure 3. Captive Portal Menu Selection

The menu options are described in Table 4.

Table 4: Captive Portal Menu

Menu Selection	Definition
External Page Redirect	Redirects clients to an external URL for the logon window and authenticates them with an external RADIUS server. Refer to “External Authentication Page Redirection on Captive Portals” on page 17.
External RADIUS	Directs clients to an external authentication page proxy for the logon window and authenticates them with an external RADIUS server. Refer to *TQ5403 Wireless Access Points Management Software User’s Guide.*
Click-Through	Displays an introductory web page stored on the wireless access point to the clients of the captive portal. The captive portal provides no client authentication. Refer to *TQ5403 Wireless Access Points Management Software User’s Guide*.
Disabled	Disables captive portals on the VAP.

IEEE802.11w (MFP)

The menu selections of the IEEE802.11w (MFP) option have changed. The option is located in the Settings > VAP/Security > WPA Personal Security window and WPA Enterprise Security window. Refer to Figure 4. The available selections depend on the WPA version. The new selections are listed here:

- Disabled: IEEE802.11w (MFP) is disabled.
- Capable: The access point allows clients that support or do not support IEEE802.11w to connect to the VAP.
- Required: The switch permits only clients that support IEEE802.11w to connect to the VAP. It blocks non-compliant clients.

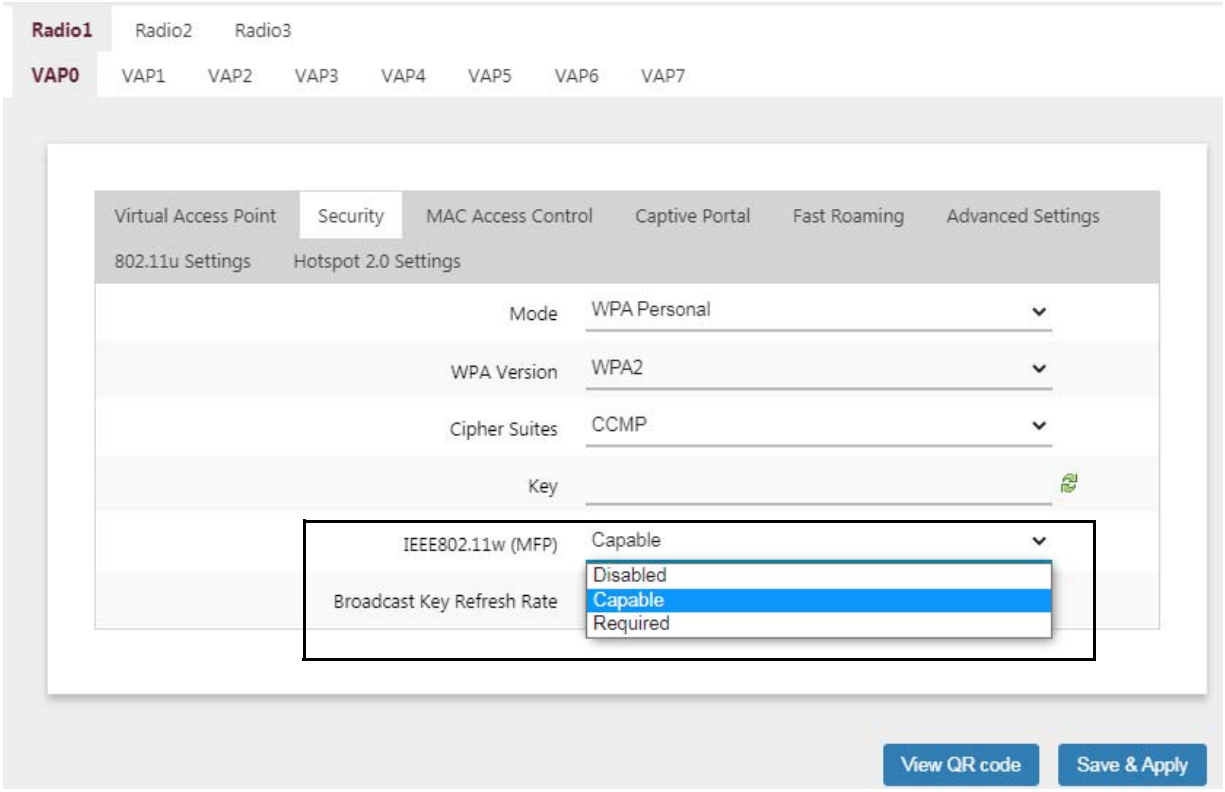

Figure 4. IEEE802.11w (MFP) Option in the WPA Personal Security Tab

MAC Filtering and RADIUS Server Authentication

The MAC Address Control menu has the new option “MAC Address List + External RADIUS.” Refer to Figure 5. It lets you use both the on-board MAC address filter as well as a RADIUS server on your network to authenticate wireless clients on VAPs. In previous versions you could authenticate clients using either method, but not both at the same time.

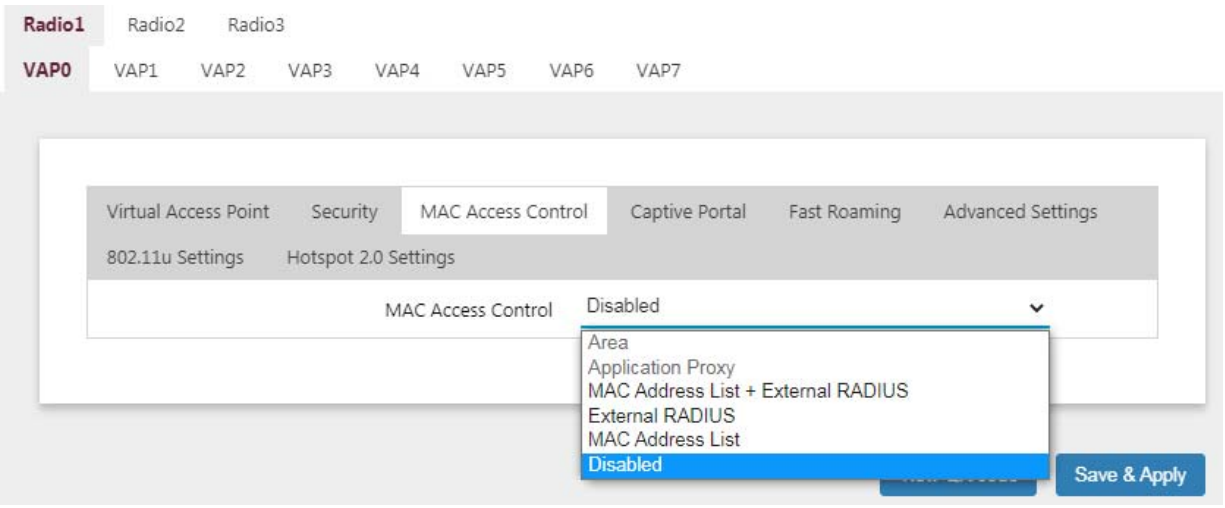

Figure 5. MAC Address List + External RADIUS Menu Selection

The new option 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.

Virtual IP Address for Captive Portals

This feature lets you assign 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. The option is set in the Settings > System > Network tab. Refer to Figure 6.

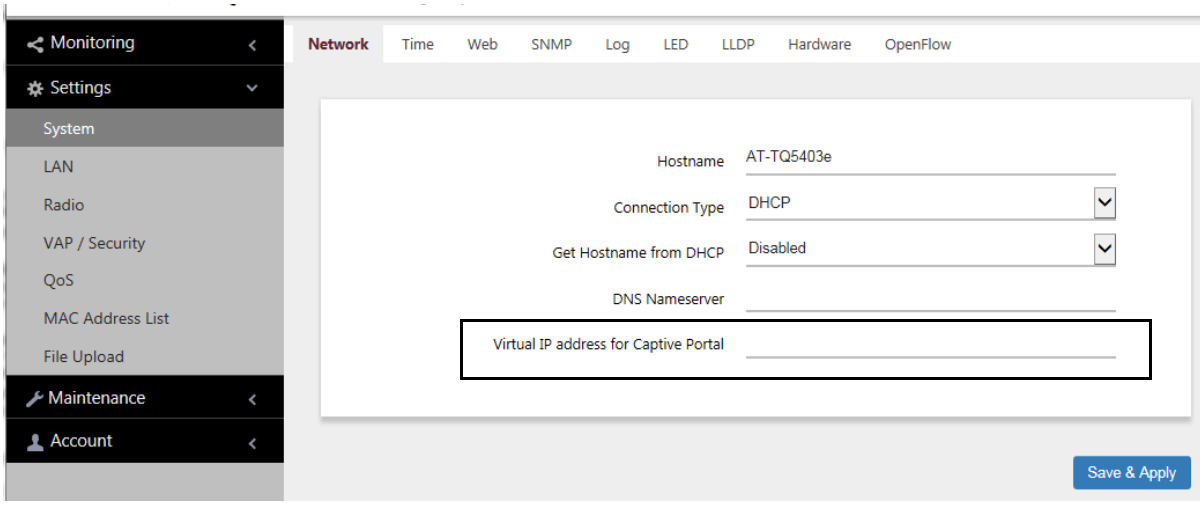

Figure 6. Virtual IP Address for Captive Portals

Note
This option is not supported with Wireless Distribution System (WDS) bridges,

External Authentication Page Redirection on Captive Portals

This feature 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. It is found in the Captive Portal pull-down menu in the Virtual Access Point tab. Refer to Figure 7. When you select the 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. You can specify only one URL.

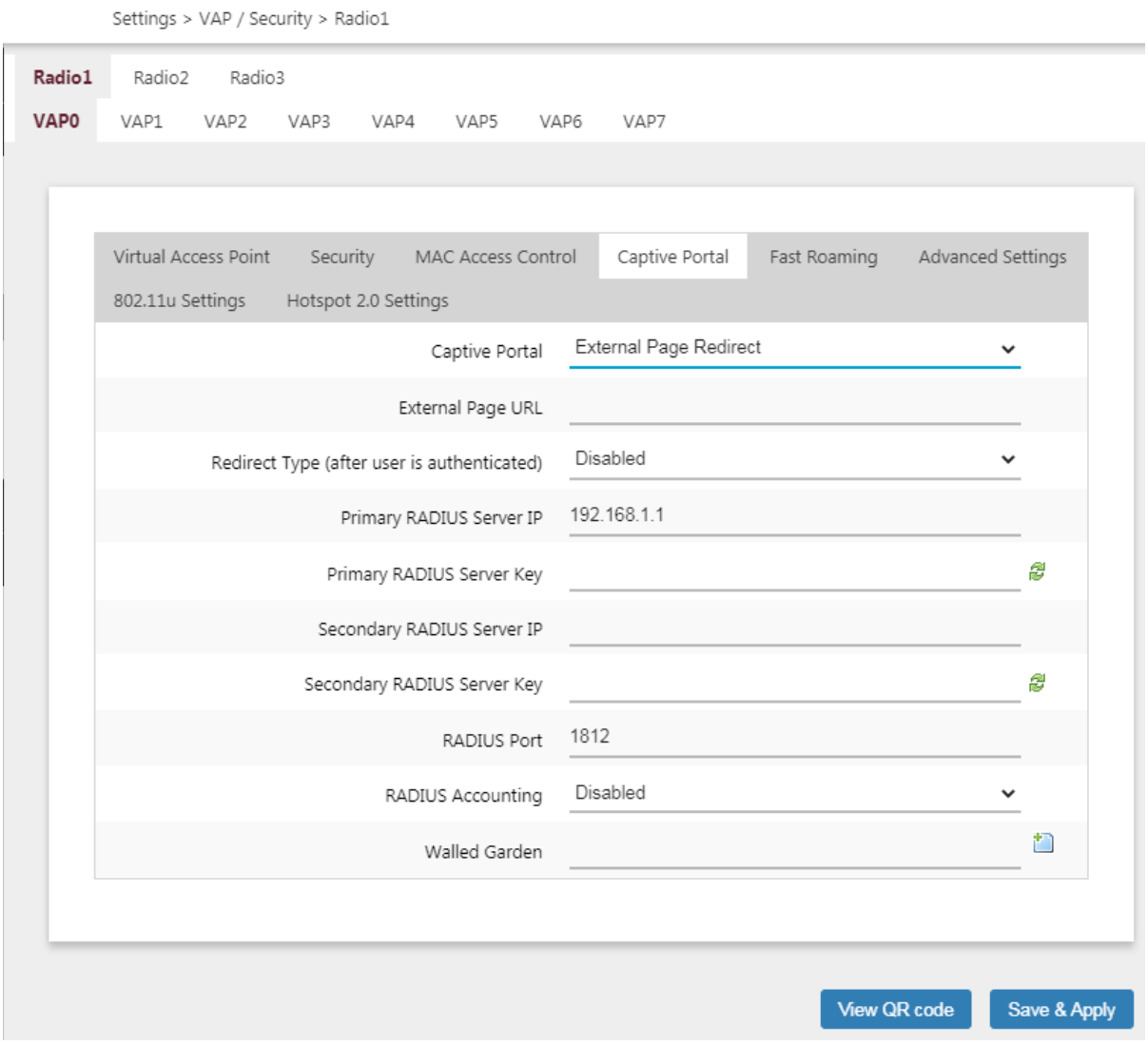

Figure 7. External Page Redirect Option in the Virtual Access Point Tabs

RADIUS Accounting on Captive Portals

This feature adds support for RADIUS accounting of wireless clients on captive portals. It allows for the collection of client usage statistics. RADIUS accounting is supported on all radios and VAPs of External RADIUS and External Page Redirection captive portals. Refer to Figure 8.

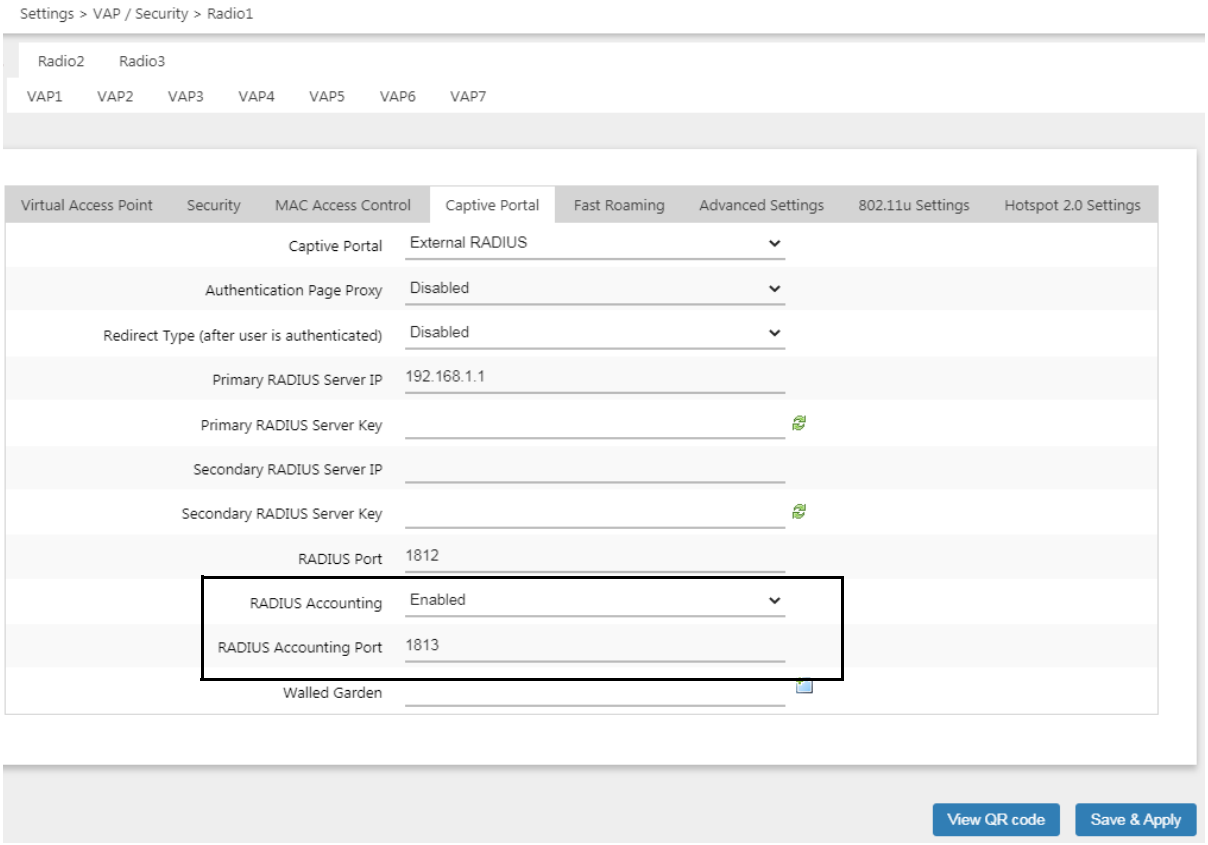

Figure 8. RADIUS Accounting on Captive Portals

Walled Gardens on Captive Portals

This feature lets you specify 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. Refer to Figure 9.

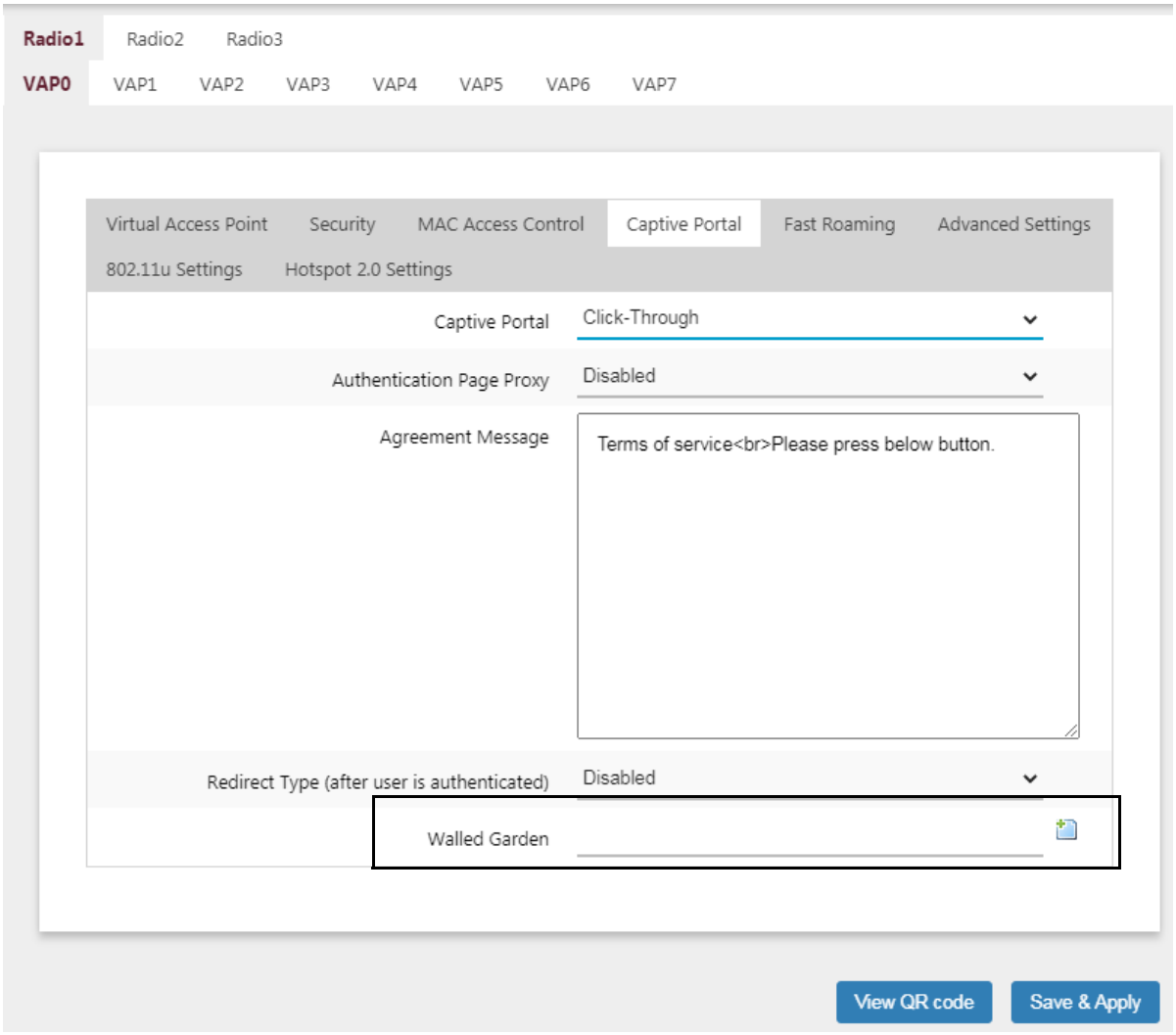

Figure 9. Walled Garden Option in the Captive Portal Tab

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. Refer to Figure 10 on page 20 for an example.

Figure 10. Example of HTTP URLs of Approved Web Sites for the Walled Garden

Hotspot 2.0 and WiFi Certified Passpoint on Captive Portals

This feature adds support for WiFi Certified Passpoint on captive portals. The feature allows mobile devices that support the IEEE 802.11u standard to automatically connect to subscribed Hotspot 2.0 services through the wireless access points. The feature is available on all radios, VAPs, and captive portals. Refer to Figure 11.

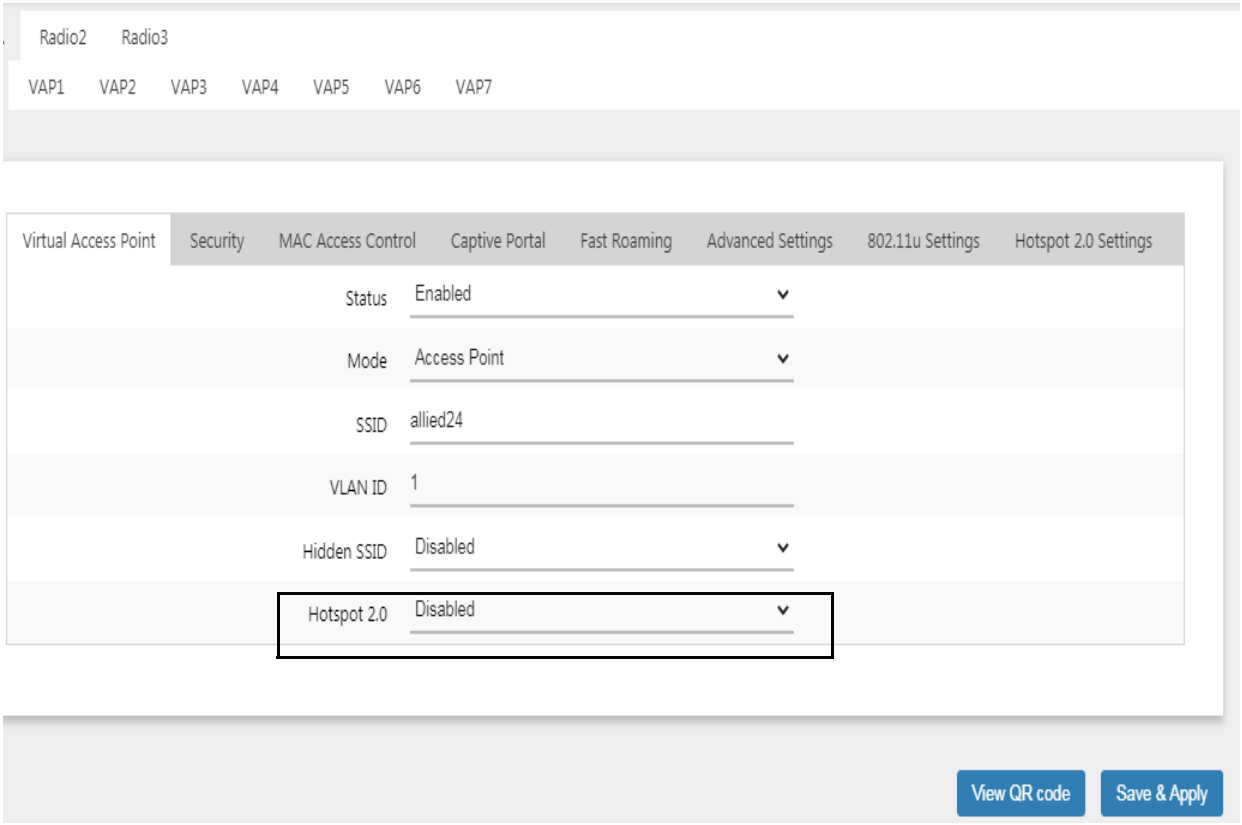

Figure 11. Hotspot 2.0 Option in the Virtual Access Point Tab

Configure the settings in the Hotspot 2.0 Settings tab before enabling the feature. Refer to Figure 12.

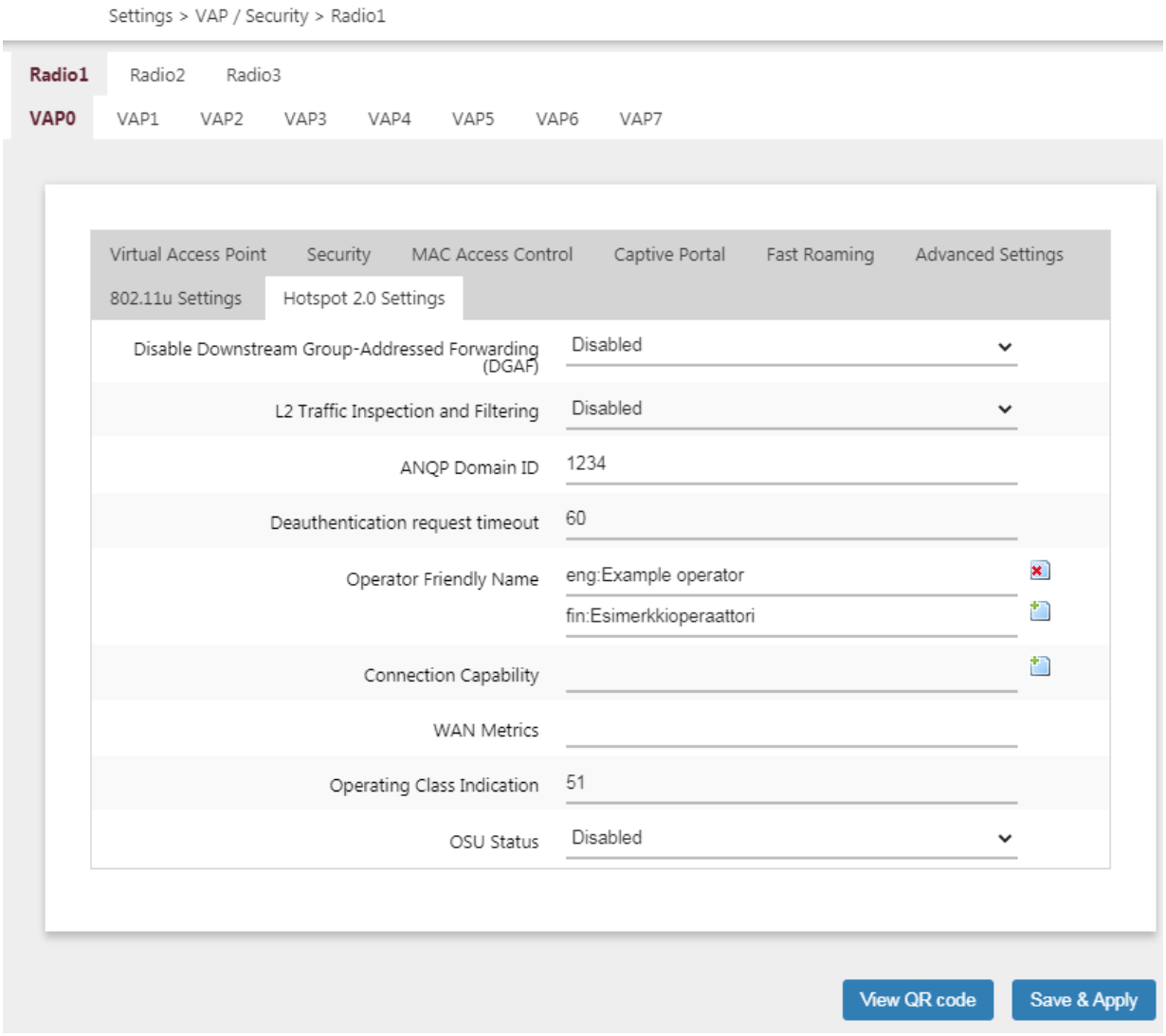

Figure 12. Hotspot 2.0 Settings Tab

802.11u Settings Tab

The wireless access points include an 802.11u Settings tab for VAPs. Refer to Figure 13.

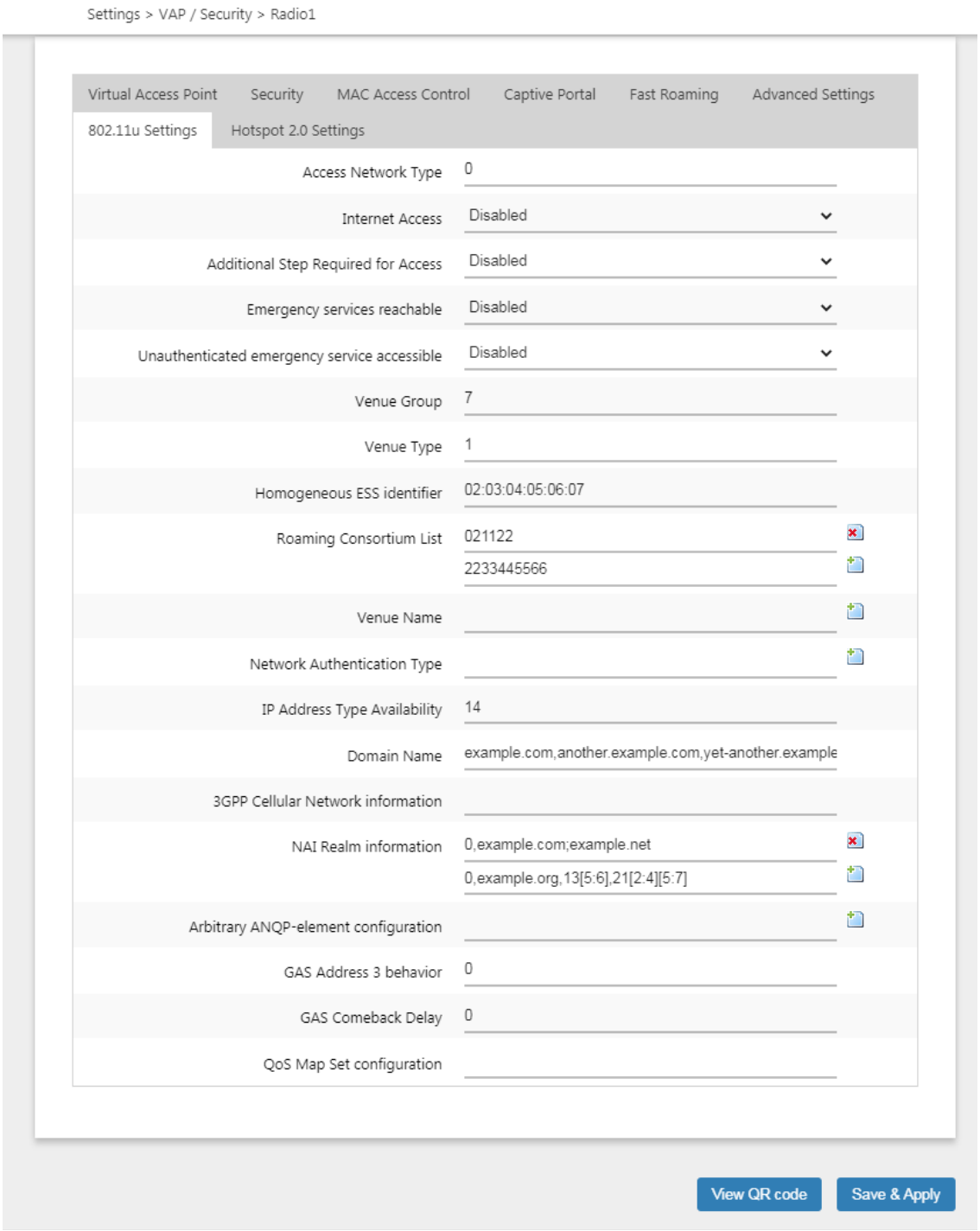

Figure 13. 802.11u Settings Tab

CSV Files for the MAC Address Filter

The new Import from CSV button in the MAC Address List window lets you download a CSV file with client MAC addresses to the MAC address filter on the access point. This simplifies the task of adding the same MAC addresses to multiple access points as well as restoring lists to replacement devices. Rather than entering the MAC addresses individually on the access points, you add them once to a CSV file and then download the file to as many access points as needed. To download a file, click the Import from CSV button in the Settings > MAC Address List window. Refer to Figure 14.

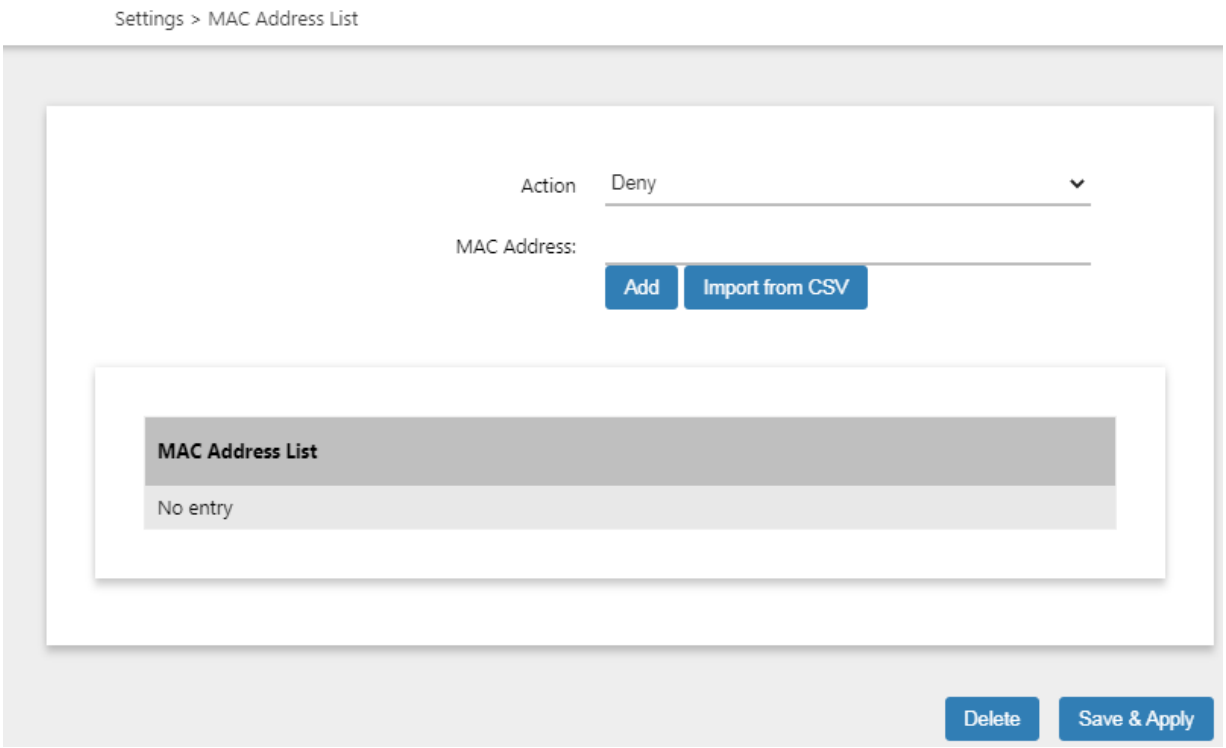

Figure 14. Import from CSV Button in the MAC Address List Window

File Upload Window

The File Uploads window is used to upload Passpoint Online Sign-up (OSU) icon files to the wireless access point. The files contain the authentication server icons that are displayed on the mobile devices when wireless clients connect to a network. Refer to Figure 15.

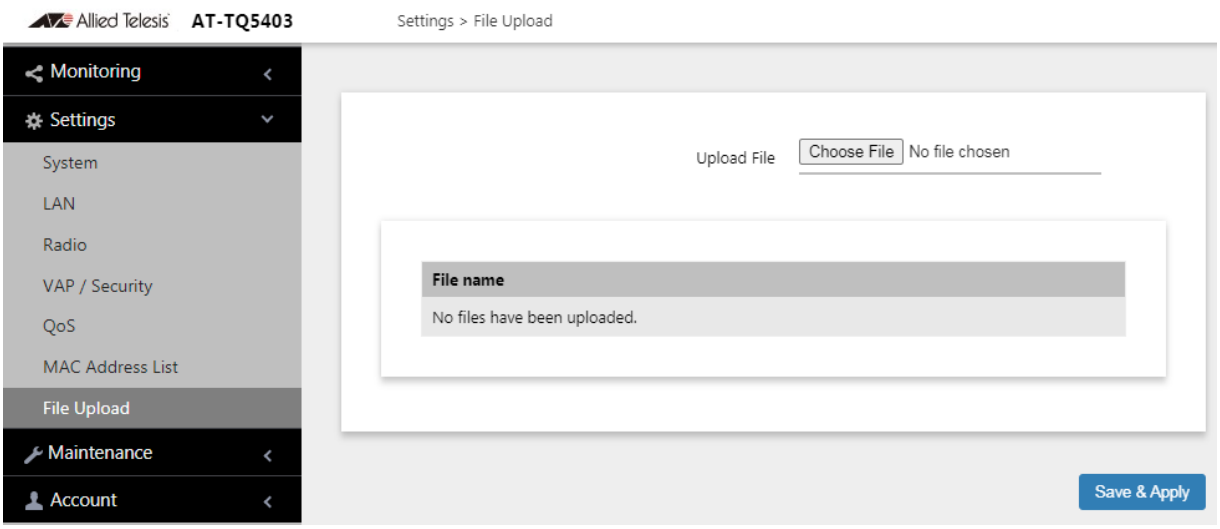

Figure 15. File Upload Window

Advanced Settings Tab

The Advanced Settings, shown in Figure 16, has the following undocumented options:

- DTIM Period - Controls the transmission of buffered broadcast and multicast packets. Wireless access points transmit the packets after beacons. The DTIM period defines the number of beacons that wireless access points transmit before transmitting the buffered packets. At a DTIM period setting of 1, wireless access points transmit buffered packets after every beacon. At a DTIM period setting of 2, units transmit buffered packets after every two beacons
- BSS Transition Management - Enables or disables 802.11v Basic Service Set transition management.

Definitions of the other parameters can be found in the *TQ5403 Wireless Access Points Management Software User's Guide*.

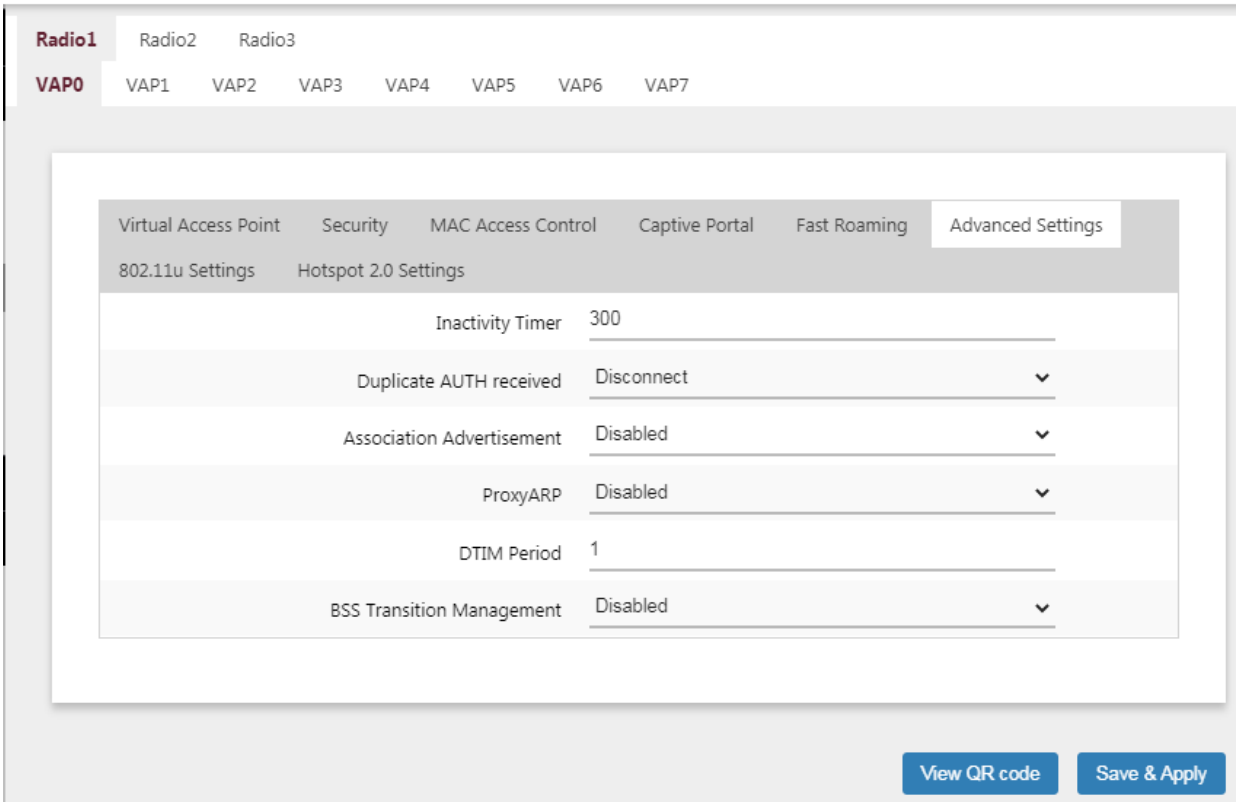

Figure 16. Advanced Settings Tab

Contacting Allied Telesis

If you need assistance with this product, the Services & Support section of the Allied Telesis web site at **www.alliedtelesis.com/services-support** has links to the following technical services:

- 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**.