



TQ5403 Wireless Access Point Series Version 6.0.1-4.1 Software Release Notes

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

- “Supported Platforms,” next
- “Unsupported Features” on page 2
- “New Features” on page 2
- “Supported Countries” on page 10
- “Enhancements” on page 11
- “Specification Change” on page 11
- “Resolved Issues” on page 12
- “Known Issues” on page 12
- “Operational Notes” on page 13
- “Contacting Allied Telesis” on page 14

Supported Platforms

Version 6.0.1-4.1 is 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 firmware filenames for Version 6.0.1-4.1 for the wireless access points are shown here:

- AT-TQ5403-6.0.1-4.1.img
- AT-TQm5403-6.0.1-4.1.img
- AT-TQ5403e-6.0.1-4.1.img

Unsupported Features

Version 6.0.1-4.1 does not support the following features:

- Channel Blankets
- Smart Connect

New Features

Virtual IP Address

This release 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 System > Network tab. Refer to Figure 1.

The screenshot shows the Network configuration page in a web interface. The left sidebar contains a menu with categories: Monitoring, Settings, System, LAN, Radio, VAP / Security, QoS, MAC Address List, File Upload, Maintenance, and Account. The main content area is titled 'Network' and includes tabs for Time, Web, SNMP, Log, LED, LLDP, Hardware, and OpenFlow. The configuration fields are as follows:

Hostname	AT-TQ5403e
Connection Type	DHCP
Get Hostname from DHCP	Disabled
DNS Nameserver	
Virtual IP address for Captive Portal	

A blue 'Save & Apply' button is located at the bottom right of the configuration area.

Figure 1. Virtual IP Address for Captive Portals

Note

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

External Page Redirection

This new feature enables the wireless access point to redirect clients of captive portals to remote web servers for the logon windows. This feature, which requires RADIUS to authenticate the clients, 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 2. 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.

The screenshot displays the configuration interface for a Virtual Access Point (VAP0) under Radio1. The interface includes tabs for Radio2 and Radio3, and VAP1 through VAP7. The main configuration area has tabs for Virtual Access Point, Security, Fast Roaming, Advanced Settings, 802.11u Settings, and Hotspot 2.0 Settings. The Virtual Access Point tab is active, showing various settings. A red box highlights the Captive Portal section, where the 'External Page Redirect' option is selected in the dropdown menu. Below this, the 'External Page URL' field is empty. The 'Redirect Type (after user is authenticated)' is set to 'Disabled'. The 'Primary RADIUS Server IP' is 192.168.1.1, and the 'Secondary RADIUS Server IP' is 192.168.1.11. Both RADIUS server keys are masked with dots. The 'RADIUS Port' is 1812, and 'RADIUS Accounting' is 'Disabled'. Other settings include 'Status' (Enabled), 'Mode' (Access Point), 'SSID' (allied24), 'VLAN ID' (1), 'Hidden SSID' (Disabled), 'MAC Filtering' (Disabled), 'Walled Garden' (disabled), and 'Hotspot 2.0' (Disabled). At the bottom right, there are 'View QR code' and 'Save & Apply' buttons.

Setting	Value
Status	Enabled
Mode	Access Point
SSID	allied24
VLAN ID	1
Hidden SSID	Disabled
MAC Filtering	Disabled
Captive Portal	External Page Redirect
External Page URL	
Redirect Type (after user is authenticated)	Disabled
Primary RADIUS Server IP	192.168.1.1
Primary RADIUS Server Key	•••••
Secondary RADIUS Server IP	192.168.1.11
Secondary RADIUS Server Key	•••••
RADIUS Port	1812
RADIUS Accounting	Disabled
Walled Garden	
Hotspot 2.0	Disabled

Figure 2. External Page Redirect Option in the Virtual Access Point Tabs

RADIUS Accounting on Captive Portals

This release adds support for RADIUS accounting of wireless clients on captive portals. It allows you to collect client usage statistics. RADIUS accounting is supported on all radios and VAPs of External RADIUS and External Page Redirection captive portals. Refer to Figure 3.

The screenshot shows a configuration page for a Virtual Access Point (VAP0) under Radio1. The 'Advanced Settings' tab is selected. The 'Captive Portal' is set to 'External RADIUS'. The 'RADIUS Accounting' field is set to 'Enabled' and the 'RADIUS Accounting Port' is set to '1813'. These two fields are highlighted with a red box. Other settings include Status: Enabled, Mode: Access Point, SSID: allied24, VLAN ID: 1, Hidden SSID: Disabled, MAC Filtering: Disabled, Authentication Page Proxy: Disabled, Redirect Type: Disabled, Primary RADIUS Server IP: 192.168.1.1, Secondary RADIUS Server IP: 192.168.1.11, and RADIUS Port: 1812. At the bottom, there are buttons for 'View QR code' and 'Save & Apply'.

Virtual Access Point	Security	Fast Roaming	Advanced Settings	802.11u Settings	Hotspot 2.0 Settings
Status	Enabled		▼		
Mode	Access Point		▼		
SSID	allied24				
VLAN ID	1				
Hidden SSID	Disabled		▼		
MAC Filtering	Disabled		▼		
Captive Portal	External RADIUS		▼		
Authentication Page Proxy	Disabled		▼		
Redirect Type (after user is authenticated)	Disabled		▼		
Primary RADIUS Server IP	192.168.1.1				
Primary RADIUS Server Key	●●●●●				
Secondary RADIUS Server IP	192.168.1.11				
Secondary RADIUS Server Key	●●●●●				
RADIUS Port	1812				
RADIUS Accounting	Enabled		▼		
RADIUS Accounting Port	1813				
Walled Garden					
Hotspot 2.0	Disabled		▼		

Figure 3. RADIUS Accounting on Captive Portals

Walled Garden

This new 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 4.

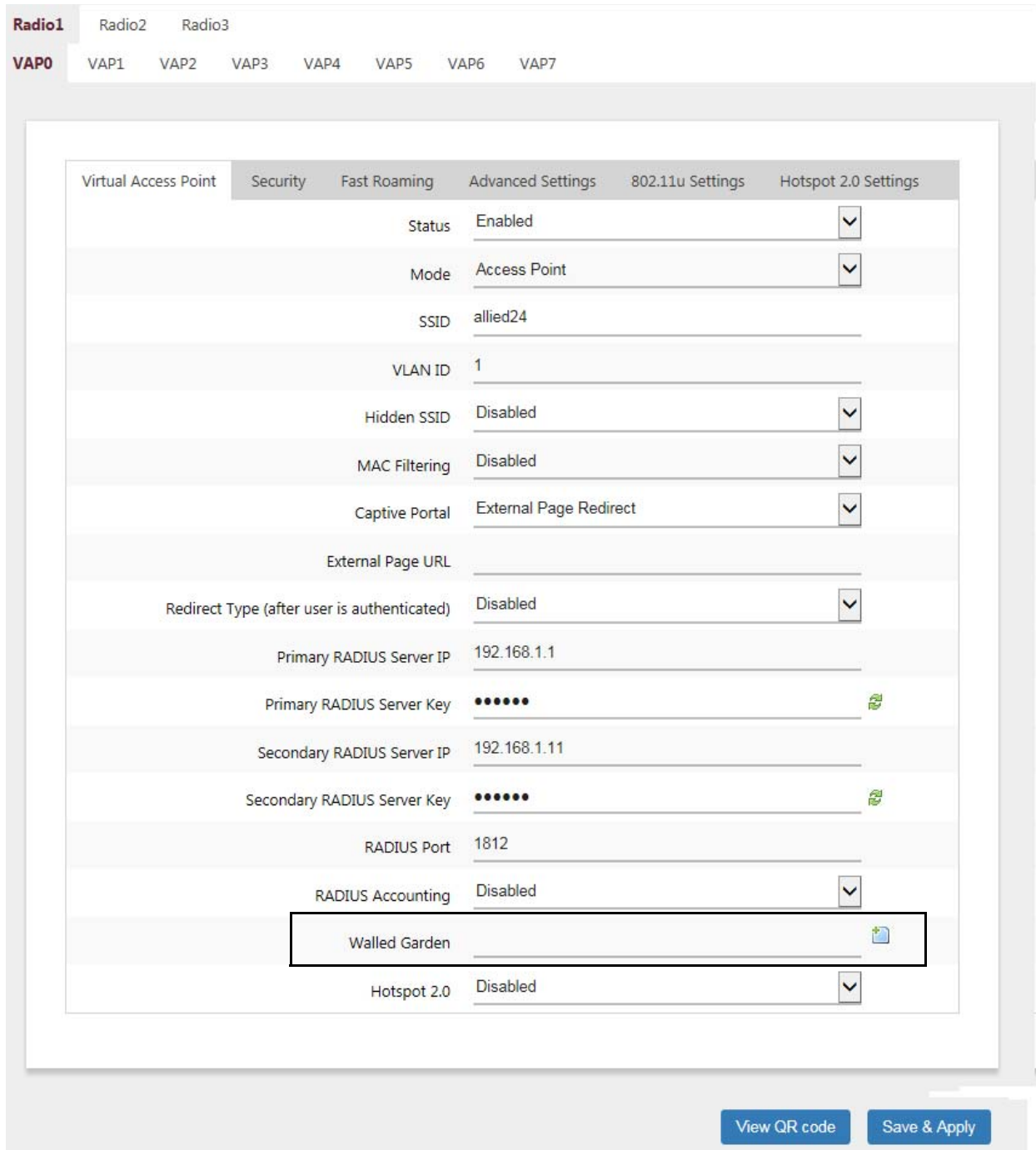


Figure 4. Walled Garden Option in the Virtual Access Point Tab

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 5 for an example.

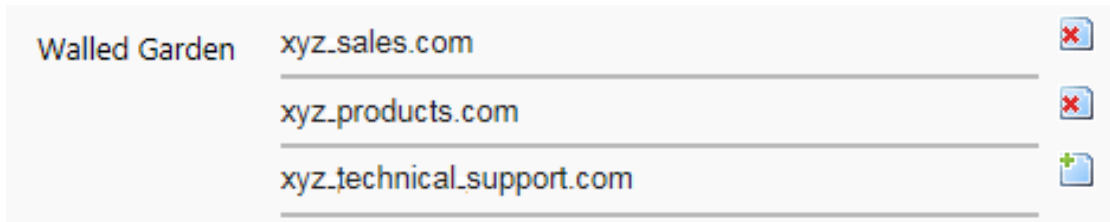


Figure 5. Example of HTTP URLs of Approved Web Sites for the Walled Garden

Hotspot 2.0

This release 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 6.

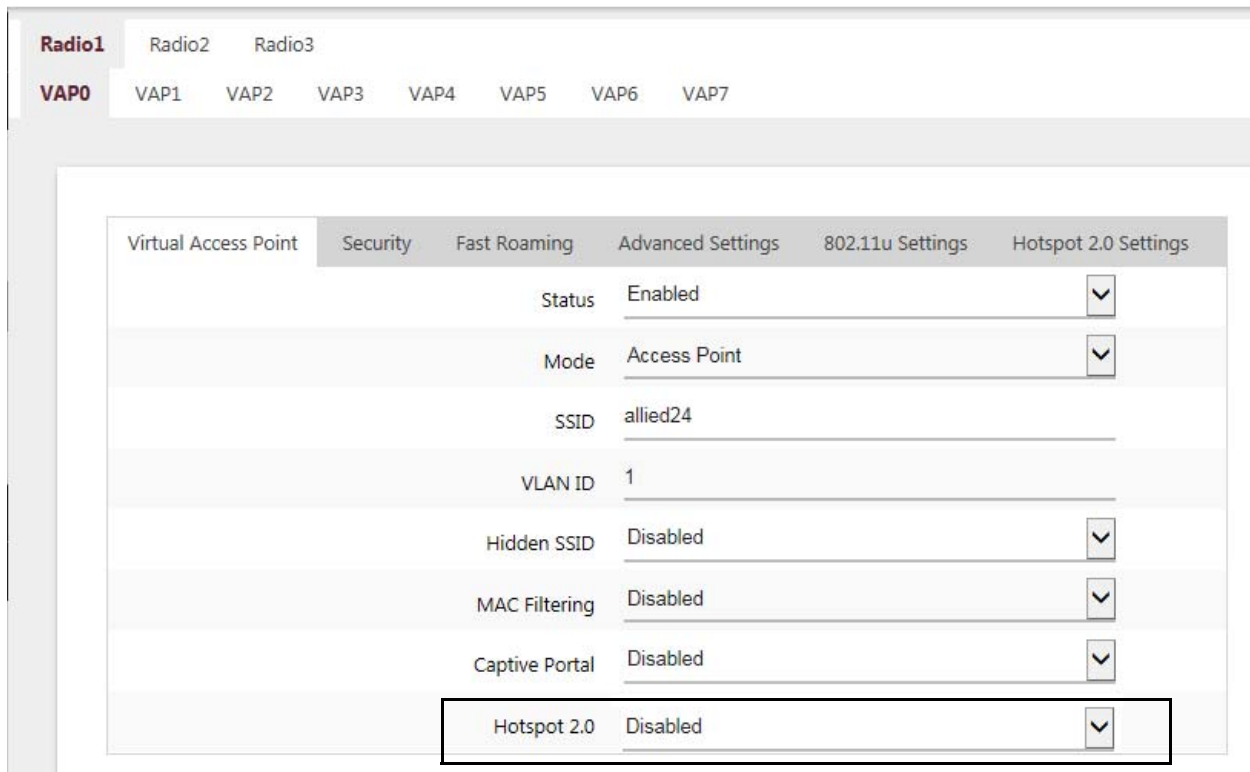


Figure 6. Hotspot 2.0 Option in the Virtual Access Point Tab

Configure the settings in the Hotspot 2.0 Settings tab before enabling the feature. Refer to Figure 7.

The screenshot displays the configuration interface for a radio's Hotspot 2.0 settings. The interface is organized into several sections:

- Navigation:** 'Radio1' is selected, with sub-tabs for 'VAP0' through 'VAP7'. 'VAP1' is the active sub-tab.
- Settings Tabs:** 'Virtual Access Point', 'Security', 'Fast Roaming', 'Advanced Settings', '802.11u Settings', and 'Hotspot 2.0 Settings' are visible. 'Hotspot 2.0 Settings' is the active tab.
- Configuration Items:**
 - Disable Downstream Group-Addressed Forwarding (DGAF):** Set to 'Disabled'.
 - L2 Traffic Inspection and Filtering:** Set to 'Disabled'.
 - ANQP Domain ID:** Set to '1234'.
 - Deauthentication request timeout:** Set to '60'.
 - Operator Friendly Name:** Includes 'eng:Example operator' and 'fin:Esimerkkioperaattori'.
 - Connection Capability:** Includes a 'WAN Metrics' section.
 - Operating Class Indication:** Set to '51'.
 - OSU Status:** Set to 'Disabled'.
- Actions:** 'View QR code' and 'Save & Apply' buttons are located at the bottom right.

Figure 7. Hotspot 2.0 Settings Tab

802.11u Settings Tab

This release includes a new 802.11u Settings tab for VAPs. Refer to Figure 8.

The screenshot displays the configuration page for VAP1 under Radio1. The '802.11u Settings' tab is active, showing the following configuration details:

Virtual Access Point	Security	Fast Roaming	Advanced Settings	802.11u Settings	Hotspot 2.0 Settings
Access Network Type				0	
Internet Access				Disabled	▼
Additional Step Required for Access				Disabled	▼
Emergency services reachable				Disabled	▼
Unauthenticated emergency service accessible				Disabled	▼
Venue Group				7	
Venue Type				1	
Homogeneous ESS identifier				02:03:04:05:06:07	
Roaming Consortium List				021122 2233445566	✕ +
Venue Name					+
Network Authentication Type					+
IP Address Type Availability				14	
Domain Name				example.com,another.example.com,yet-another.example	
3GPP Cellular Network information					
NAI Realm information				0,example.com;example.net 0,example.org,13[5:6],21[2:4][5:7]	✕ +
Arbitrary ANQP-element configuration					+
GAS Address 3 behavior				0	
GAS Comeback Delay				0	
QoS Map Set configuration					

At the bottom of the page, there are two buttons: 'View QR code' and 'Save & Apply'.

Figure 8. 802.11u Settings Tab

CSV Files for the MAC Address Filter

This release lets you download CSV files 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 into 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 to the access point, click the Import from CSV button in the Settings > MAC Address List window. Refer to Figure 9 on page 9.

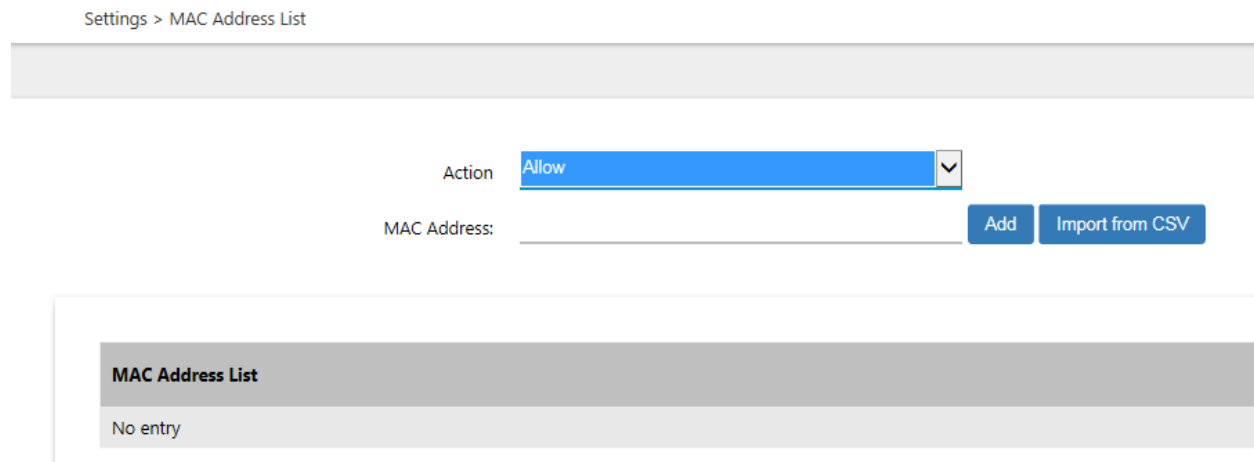


Figure 9. Import from CSV Button in the MAC Address List Window

Vista Manager EX and the AWC Plug-in

The following changes to this version of the management software apply to Vista Manager EX and the AWC plug-in:

- ❑ Expanded configuration of captive portals in AWC.
- ❑ Added support for combining centralized authentication of wireless clients on captive portals with RADIUS accounting.
- ❑ Added support for the white-list feature in AMF Security Controller (AMF-Sec). The feature is listed as "Whitelist" in the MAC Filtering pull-down menu in the Virtual Access Point window in the on-board web browser management interface.

Supported Countries

The TQ5403, TQm5403, and TQ5403e Wireless Access Points are supported in the countries in Table 1. The table includes the version numbers of the first firmware releases to support the countries.

Table 1: Supported 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.

Enhancements

None.

Specification Change

- The menu selections for the IEEE802.11w (MFP) option in the WPA Personal Security tab and WPA Enterprise Security tab have changed. Refer to Figure 10. The new selections are listed here:
 - Disabled: IEEE802.11w (MFP) is disabled.
 - Capable: The access point allows clients that support IEEE802.11w as well as clients that do not support it to connect to the VAP.
 - Required: Only clients that support IEEE802.11w are allowed to connect to the VAP. The switch blocks non-compliant clients.

The available selections depend on the WPA version.

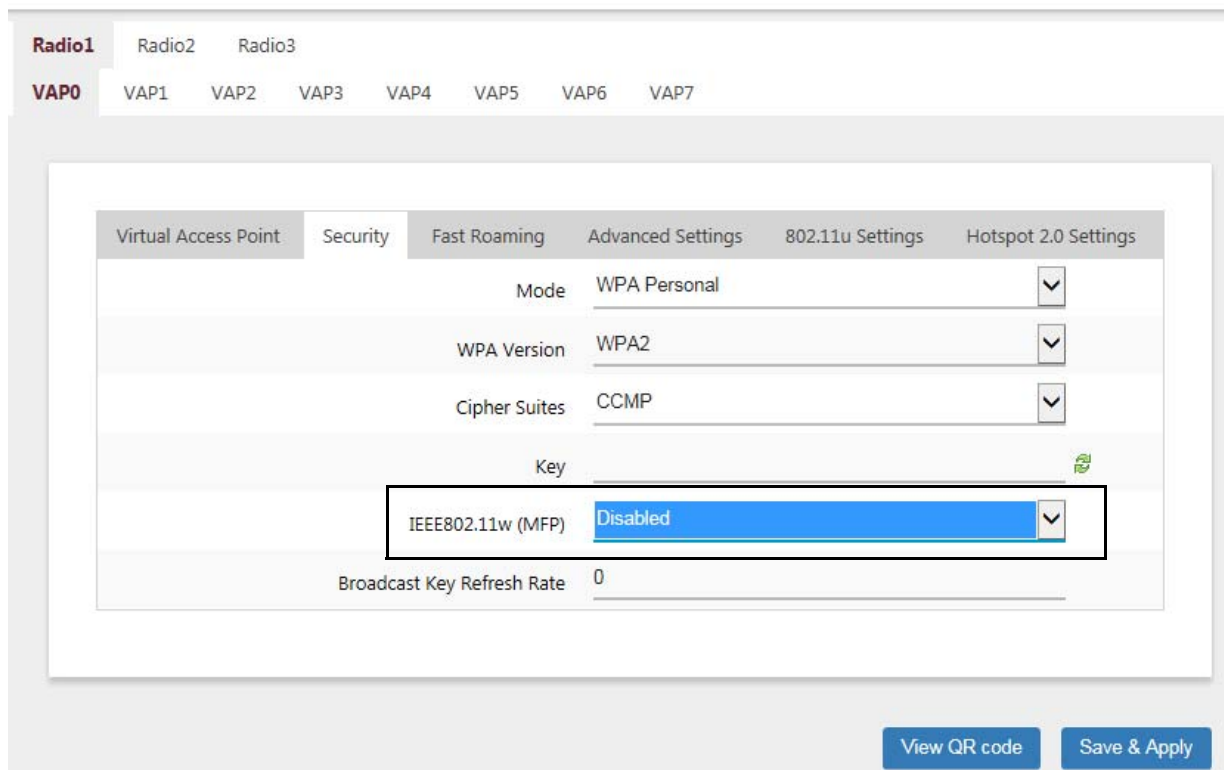


Figure 10. IEEE802.11w (MFP) Option in the WPA Personal Security Tab

Resolved Issues

- The access point generated the log message “sh: cf: unknown operand” because of DHCP lease time.
- The access point did not always respond to web browser management after it was booted
- The time stamp in the technical support file was incorrect.
- Changes made to SNMP settings with the on-board web browser interface were not reflected in Vista Manager EX (AWC Lite).
- NTP synchronization did not always work correctly after the access point was booted.
- The access point did not validate the format of the IP address in the Static IP Address field.
- The access point added unnecessary folders in memory when generating the technical support file.

Known Issues

These known issues apply to the TQ5403, TQm5403, and TQ5403e Wireless Access Points:

- Access points do not synchronize Hostname and SNMP System Name.
- Access points do not always save new values in the Secondary RADIUS Server Key value.
- Access points might disconnect inactive clients several seconds before the Inactivity Timer expires.
- Do not use the Associated Client window in the web browser interface to disconnect clients on WDS children.
- In rare instances, inconsistencies may occur in the hardware and software tables that can cause access points to reset. This is entered in the log as “kernel: Rebooting due to DMA error recovery.”
- When IEEE802.11w Management Frame Protection is enabled, some wireless clients might not be able to immediately reconnect after disconnecting.
- Activating IEEE802.11WW (MFP) in WPA Personal Security may cause delays in the handling of roaming clients by the access points.
- 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 send SNMP traps with their default IP address when reset or powered on.
- Access points might increment the Received Counter for a VAP when there are no clients.
- The access point might fail to operate properly as an AMF Guest node, 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.

- ❑ When booted, access points that receive their IP addresses from DHCP servers might initially use their default IP addresses in packets to NTP servers. This occurs when access points send NTP packets before receiving their IP addresses from DHCP servers.
- ❑ The access point might transmit non-traffic related packets from its radios when initializing the management software during reboots.
- ❑ 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 resetting the access point to activate the change. You do not need to reset the access point after changing the setting from Disconnect to Ignore.
- ❑ It may take one to two minutes for the access point to save its configuration when managed with the AWC plug-in.
- ❑ In rare cases, access points managed by AWC plug-in cannot save their configurations, in which case Vista Manager displays an error message. Saving the configuration again is usually successful.
- ❑ This release does not support the OpenFlow protocol on TQ5403 and TQ5403e access points.

Operational Notes

- ❑ When saving and applying its wireless settings, the access point might prompt wireless clients to disconnect their wireless connections. Clients who disconnect will have to reconnect again.
- ❑ You cannot set channels 10-13 on the 40MHz bandwidth on the 2.4GHz Radio1.
- ❑ Do not set the Maximum Clients parameter to more than 200 with the web browser interface.

Contacting Allied Telesis

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

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

For sales or corporate information, go to www.alliedtelesis.com/purchase and select your region.

Copyright © 2020 Allied Telesis Inc., Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis Inc., Inc. Allied Telesis Inc. and the Allied Telesis Inc. logo are trademarks of Allied Telesis Inc., Incorporated. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners. Allied Telesis Inc., 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., 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., Inc. has been advised of, known, or should have known, the possibility of such damages.