TQ1402 and TQ5403 Wireless Access Point Series
Versions 5.4.3 to 6.0.1-2.1 Software Release Notes

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

Version 6.0.1-2.1

Supported Platforms

Version 6.0.1-2.1 is supported on the following wireless access points:

- TQ1402
- TQm1402
- TQ5403
- TQm5403
- TQ5403e

For instructions on how to upgrade the management software on wireless access points, refer to the *TQ1402 Wireless Access Points Management Software User’s Guide* or *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 6.0.1-2.1 for the wireless access points are shown here:

- AT-TQ1402-6.0.1-2.1.img
- AT-TQm1402-6.0.1-2.1.img
- AT-TQ5403-6.0.1-2.1.img
- AT-TQm5403-6.0.1-2.1.img
- AT-TQ5403e-6.0.1-2.1.img

New Features

This new feature applies to the TQ1402 Series:

- New Easy Setup window in the on-board web browser management interface - The new window contains many of the basic settings you might configure during the first management session of the wireless access points. The window allows you to specify whether the IP address will be dynamic or static and, if static, the static IP address, subnet mask, and default gateway. It also lets you set the basic settings for VAP0 on both 2.4GHz and 5GHz radios, as well as the login name and password to the web browser interface.

  Note
  The Easy Setup window has two mode settings for VAP0: Cell and Single Channel. The Single Channel option is not supported in this release.

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

This new feature applies to all TQ1402 and TQ5403 Wireless Access Points:

- Quick Response (QR) codes for the VAPs - You can now 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 ASCI
  - Static WEP / Authentication: Shared Key / Key Type: HEX or ASCI
  - 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 in the on-board web browser management interface of the TQ1402 and TQ5403 Wireless Access Point series. Refer to Figure 1 on page 3. The button is also available in the new Easy Setup window in the TQ1402 Wireless Access Point series.
  - QR codes are not supported on VAPs that use RADIUS servers or AWC to authenticate wireless clients.
  - The wireless access points come with default QR codes for VAP0 for Radio1 and Radio2. The QR codes are the same for both radios. Refer to Figure 2 on page 3.

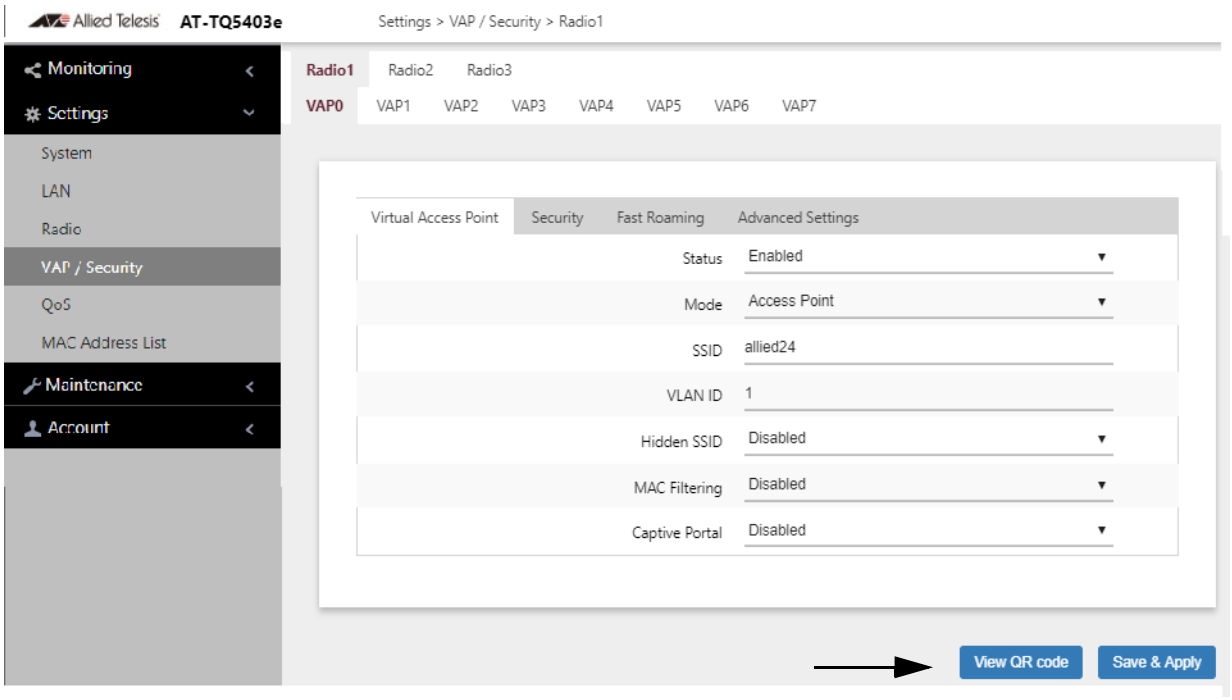

Figure 1. View QR Code Button

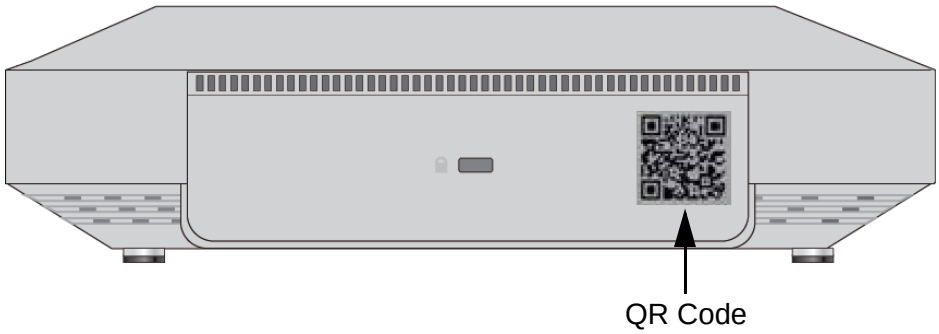

Figure 2. QR Code

This new feature applies to the TQ5403 and TQm5403 Wireless Access Points:

- New Cascade setting for the LAN2 port - Earlier firmware versions allowed you to combine LAN1 and LAN2 ports on the wireless access point to form a static link aggregation to double the bandwidth between the device and your wired network. This release adds the new Cascade setting for LAN2. It allows the port to function as a regular Ethernet port for a wired network device so that you can connect another network device to your wired network. The device can be an end node, such as a personal computer or printer, or a networking device, such as a switch or router. Refer to Figure 3.

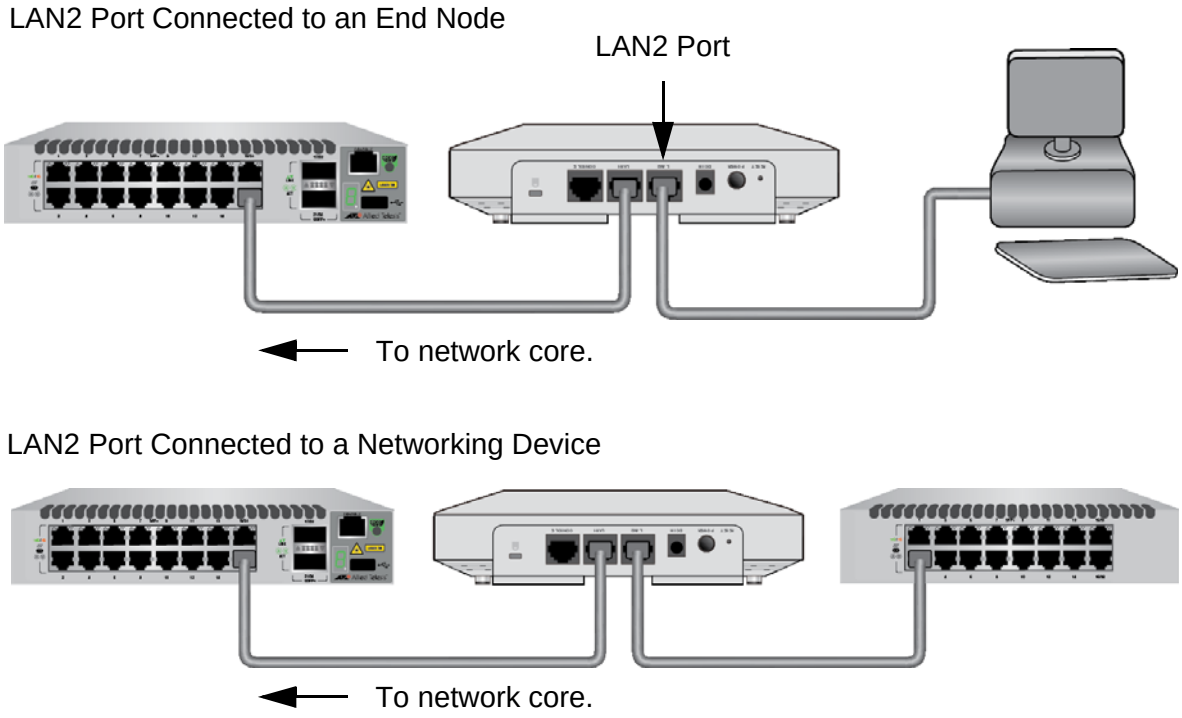

Figure 3. Cascade Mode for the LAN2 Port

Supported Countries

The TQ5403, TQ5403e, 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

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

Country	TQ5403	TQm5403	TQ5403e
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.

The TQ1402 and TQm1402 Wireless Access Points are supported in the countries in Table 2.

Table 2: Supported Countries for the TQ1402 and TQm1402 Wireless Access Points

Country	TQ1402	TQm1402
Australia	v6.0.0-0.2	v6.0.0-0.2
European Union	v6.0.0-0.2	v6.0.0-0.2
Hong Kong	v6.0.0-0.3	v6.0.0-0.3
India	v6.0.0-0.3	v6.0.0-0.3
Japan	v6.0.0-0.2	v6.0.0-0.2
Korea	v6.0.0-0.3	v6.0.0-0.3
Malaysia	v6.0.0-0.3	v6.0.0-0.3
New Zealand	v6.0.0-0.2	v6.0.0-0.2
Singapore	v6.0.0-0.3	v6.0.0-0.3
Taiwan	v6.0.0-0.3	v6.0.0-0.3
Thailand	v6.0.0-0.3	v6.0.0-0.3
United States	v6.0.0-0.2	v6.0.0-0.2
Vietnam	v6.0.0-0.3	v6.0.0-0.3

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

Enhancements

This enhancement applies to the TQ5403 and TQ5403e Wireless Access Points:

- This release adds support for using an external RADIUS server to authenticate wireless clients of Channel Blankets by their MAC addresses. The feature is activated in the web browser management interface with the External RADIUS selection. The pathway is shown here:

  Settings - > VAP/Security -> Radio# -> VAP# -> MAC Filtering

This enhancement applies to all TQ1402 and TQ5403 Wireless Access Points:

- This release increases the maximum number of addresses for the on-board MAC address filter to 2048 addresses. You use the on-board filter to authenticate clients based on their MAC addresses.

Specification Changes

These specification changes apply to the TQ1402 and TQm1402 Wireless Access Points:

- The default settings for Radio1 and Radio2 are changed to Enabled from Disabled.
- The default settings for VAP0 on Radio1 and Radio2 are as follows:
  - SSID: allied-########
  - Security setting: WPA2 and WPA3
  - Cipher: CCMP
  - Password: Sixteen characters

  Please note the following guidelines:
  - The SSID and Password are unique on each wireless access point.
  - The above settings apply only to new TQ1402 and TQm1402 Wireless Access Points. They do not apply to systems that are upgraded to version 6.0.1-2.1.

These specification changes apply to all TQ1402 and TQ5403 Wireless Access Points:

- When the Network Time Protocol (NTP) client is activated, the access points continuously transmit NTP queries every five seconds until they receive a response.
- If your video screen displays the web browser management windows incorrectly, try clearing the cache in your web browser.

Resolved Issues

These resolved issues apply to all TQ1402 and TQ5403 Wireless Access Points:

- Access points sent invalid information to AT-Vista Manager EX about hidden SSIDs on neighboring access points, causing AT-Vista Manager EX to ignore the neighboring access points.
- Activating the Neighbor AP Detection feature reduced performance of the access point.
- Access points experienced problems activating VAPs when VAP security was changed from WEP to WPA3.
- There was a problem activating radios after configuring WDS or WPA3 with AT-Vista Manager EX.
- The access point did not save the Passphrase for WPA3-PSK with encryption in its configuration file.
- The NTP client remained active after the time setting was changed to Manual from NTP.
- SNMP daemon experienced problems with DHCP IP lease timing.
- Access points had problems with Captive Portals when using Management VLAN Tags or dynamic VLANs.
- MAC address filtering using an external RADIUS server did not work if the User-Password-Format password contained the “%” symbol.
- The access point did not restart the NTP client after restoring a backup configuration file.
- Access points had problems using the last available channels on radios.

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

- The time zone setting did not work correctly after access points were updated to v6.0.1.
- Radion3 channel settings were blank after changing the country setting from BD Bangladesh to BE Belgium. (The wireless access points do not support Bangladesh or Belgium.)

These resolved issues apply to the TQ1402 and TQm1402 Wireless Access Points:

- The RTS Threshold setting in the Advanced Radio Settings window for the 2.4GHz radio did not work.
- Access points erroneously changed the state of the Dynamic Frequency Selection to Out of Channels (OOC) when using W52 or W53.
- Access points generated invalid messages when creating the Technical Support file.

Known Issues

These known issues apply to all TQ1402 and TQ5403 Wireless Access Points:

- Access points do not synchronize Hostname and SNMP System Name.
- Channel Blankets are not supported when the feature is enabled on only one access point.
- 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.”

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

- When IEEE802.11w Management Frame Protection is enabled, some wireless clients might not be able to 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 selected 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 rebooted, 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 rebooted, 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.

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

- The RADIUS attribute “Session-timeout” is disabled in VAPs in Channel Blankets.
- Access points might fail if wireless clients frequently connect and disconnect between Channel Blanket VAPs.
- Channel Blankets are not supported when the feature is active on only one access point.
- The Technical Support Information feature might not be successful when multiple wireless clients are connected to Channel Blanket VAPs.
- IEEE802.11w (MFP) should be disabled on access points using Channel Blankets.
- This release does not support the OpenFlow protocol on TQ5403 and TQ5403e access points.
- Association Advertisements should be enabled on access points using Channel Blankets.
- 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.

These known issues apply to the TQ1402 and TQm1402 Wireless Access Points:

- 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.

Operational Notes

These operational notes apply to the TQ5403 Series:

- When saving and applying wireless settings, the access point might prompt wireless clients to disconnect their wireless connections. Depending on the clients, the wireless connections might be maintained. In that case, the clients have to reconnect client again.
- 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.
- Do not use the network IP address 172.31.0.0/24 when using the auto-discovery feature in AWC-SC. The network IP address is reserved by AWC-SC.
- You cannot configure VAPs on radios that are using AWC-SC.
- Root and satellite access points that are using AWC-SC need to have the same VID settings.
- AWC-SC cannot pass through AMF Guest nodes. Consequently, access points connected to AMF Guest nodes cannot use AWC-SC.
- AWC-SC and DHCP snooping should not be used on the same network. The results may be unpredictable.
- This release does not support the Whitelist Authentication option in the MAC Filtering feature in the Virtual Access Point tab.

These operational notes apply to the TQ1402 Series

- The access points, which have only one Ethernet LAN port, do not support LLDP.
- The access points do not support the OpenFlow protocol. The OpenFlow tab in the web browser interface is not functional.
- Radio1 supports up to 120 clients and Radio2 up to 200 clients.
- Radio1 does not support WPA3 when set to WPA Enterprise.
- The ”WPA2 and WPA3” setting is only available with WPA Personal.
- The access points do not support Proxy ARP. The Proxy ARP settings in the Advanced Settings window in the web browser interface are not functional.
- This release does not support the Whitelist Authentication option in the MAC Filtering feature in the Virtual Access Point tab.

Channel Blankets

Known Issues

- Wireless access points may stop forwarding traffic if clients rapidly connect and disconnect from Channel Blanket VAPs.
- Access points might not allow wireless clients to connect to Channel Blanket VAPs when only one access point is running Channel Blankets.
- The Technical Support Information feature might not be successful when multiple wireless clients are connected to Channel Blanket VAPs.
- Channel Blankets might drop broadcast packets during heavy traffic.

Operational Notes

Caution
Do not operate Channel Blankets on access points that have different versions of the firmware. The operations of the access points may be unpredictable. Before updating wireless access points in networks that have Channel Blankets, Allied Telesis recommends disabling the feature on all access points first. You can enable Channel Blankets again after updating all units.

Please 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 rebooted or powered on, access points in Channel Blankets may take up to two minutes before forwarding traffic from wireless clients

Version 6.0.0-1.3

This release applies only to the TQ1402 Series.

New Features

- AWC Plug-in includes centralized MAC address authentication of wireless clients for improved handling of roaming clients. The feature requires Vista Manager EX or Vista Manager mini.

Enhancements

- Access points enter a log entry when inactive wireless clients are timed out.
- The Technical Support file now includes information on dynamic VLANs.

Specification Changes

- Access points use the auto selection feature to select a new channel when a radar signal is detected on a DFS channel, even when the prior channel was selected manually.
- The spelling of Macao has been changed to Macau.
- The waiting time for upgrading firmware on the access points from Vista Manager EX has been increased to prevent unnecessary upgrade terminations.

Resolved Issues

- Access points entered duplicate Informational log entries during DFS CAC events.
- Access points transmitted unnecessary beacon frames on Radio1 when the Legacy Rate was changed.
- SNMP did not work if the first character in the read-only community string was “#”.
- Access points stopped working if wireless clients repeatedly connected and disconnected.
- Access points transmitted untagged packets across network segment boundaries.
- Wireless clients connecting to dynamic VLANs in VAPs with no VLAN names were assigned to the wrong VLAN.
- Dynamic VLANs in WPA3 Enterprise did not work.
- Wireless clients were disconnected when VAP security was changed to None from WPA Enterprise.
- Access points that had a space as the first character in their SSIDs could not save their configurations.
- SSIDs with special characters could not be set from the AWC plug-in.
- The HTTP Port parameter accepted periods.
- Changing Maximum Session or Session Timeout parameters generated error messages.
- The message “Unsaved Changes” was displayed unnecessarily.
- Access points failed to send NTP packets after reboots.
- Access points using Fast Roaming displayed the wrong Security for neighboring access points in the Neighbor AP window.
- Changing the Management VLAN to a value other than 1 caused access points to lose communications.
- The SNMP sysObjectID object returned the wrong value.
- Access points did not recover after multiple reboots.
- Access points displayed error messages during configuration file backup processes in AMF.
- Radio transmission power was adjusted incorrectly after detection of radar on DFS channels.
- Enabling Dynamic VLANs corrupted the configuration file.
- Transmit power was displayed incorrectly for access points managed with Vista Manager EX.
- Spaces in SSIDs caused radios to reboot.
- Daylight Savings Time did not work correctly.
- Changes in the DFS status from OOC to ISM caused changes to radio bandwidths.
- The “Client Identifier” option was not included in DHCP packets.
- Access points could not restore backup configuration files containing the country codes JP or US.
- Displaying the Associate Client window generated unnecessary log entries.
- Radio2 did not work with the BD, ID, and PK country codes.
- Access points did not forward traffic from new wireless clients after VAP security was changed from WPA Enterprise to None.

- Access points did not transmit untagged packets when configured as follows:
  - Management VLAN is disabled.
  - VAP VID is set to a value other than 1.
  - Dynamic VLAN is enabled and authentication information is set to VID 1.
- Corrected a typo in “WPA2 and WPA3.”
- In rare circumstances, wireless clients could not connect to access points.

Known Issues

- Access points do not synchronize Hostname and SNMP System Name.
- Access points do not include “user ID” in the tech-support file when you collect technical support information from Maintenance > Support page, even though the page says that it contains the user ID.
- When Secondary RADIUS Server Key is entered, access points might not save the entered key and instead save the field as empty.
- Access points managed by AT-Vista Manager EX with AWC plug-in might enter error messages in the log when you click on the Radio1 VAP0 tab in the VAP/Security page.
- Access points managed by AT-Vista Manager EX with AWC plug-in report SSIDs of rogue access points as “NULL”. The SSIDs of rogue access points should be reported as empty strings (“”).
- The inactivity timer for disconnecting inactive clients might be inaccurate by several seconds.
- The Disconnect button in the Associated Client page on a WDS parent access point does not disconnect clients on WDS child access points.
- The state of the LAN port changes several times when the access point is booting.
- In rare instances, inconsistencies may occur in the hardware and software tables, which can cause access points to reset. This is registered in the log as “kernel: Rebooting due to DMA error recovery.”
- Access points transmit Ready to Send (RTS) signals on the 2.4GHz Radio 1.
- Access points might support less than 117 clients on Radio 1 if you use all eight VAPs.

Operational Notes

- The access points, which have only one Ethernet LAN port, do not support LLDP.
- The access points do not support the OpenFlow protocol. The OpenFlow tab in the web browser interface is not functional.
- Radio1 supports up to 120 clients and Radio2 up to 200 clients.
- Radio1 does not support WPA3 when set to WPA Enterprise.
- The ”WPA2 and WPA3” setting is only available with WPA Personal.
- The access points do not support Proxy ARP. The Proxy ARP settings in the Advanced Settings window in the web browser interface are not functional.

Version 5.4.3

This release applies to the TQ5403 Series.

New Feature

- Added Network Time Protocol (NTP) synchronization log events to the web browser interface and Autonomous Wave Controller (AWC) plug-in.

Enhancements

- None

Specification Changes

- None

Resolved Issues

- The wireless access point did not forward traffic from wireless clients that received VLAN assignments from the OpenFlow protocol that were different from its VAP VLANs.
- Manager passwords that contained special characters did not work correctly with the web browser interface.
- In Monitoring > Status > Radio page, "Transmission Power" is not displayed correctly when under AT-Vista Manager Ex AWC Plug-in management.
- Access points discarded packets with the MAC address prefix “02:” when the OpenFlow protocol is enabled.
- 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 the access points.
- Spaces in SSIDs caused radios to reset.
- Debug messages were entered twice in the log.
- The TQm5403 wireless access point did not support Channel Blankets.

Known Issues

- Access points do not synchronize Hostname and SNMP System Name.
- Some wireless clients might not be able to reconnect after disconnecting if IEEE802.11w Management Frame Protection is enabled.
- Channels 12 and 13 are not selected 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.
- Channel Blankets are not supported when the feature is enabled on only one access point.
- When Secondary RADIUS Server Key is entered, access points might not save the entered key and instead save the field as empty.
- Access points might increment the Received Counter for a VAP when there are no clients.
- Access points generate an error message in the log when RADIO1 VAP0 is accessed by AWC plug-in.

- Access points report as “NULL” the SSIDs of rogue access points that hide their SSIDs.
- 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 rebooted, 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.
- When rebooted, 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.
- Access points might fail if wireless clients frequently connect and disconnect between Channel Blanket VAPs.
- Channel Blankets are not supported when the feature is enabled on only one access point.
- The Technical Support Information feature might not be successful when multiple wireless clients are connected to Channel Blanket VAPs.
- IEEE802.11w (MFP) in WPA Personal Security is not supported in Channel Blankets.
- Channel Blankets might drop broadcast packets during heavy traffic.

Operational Notes

- When saving and applying wireless settings, access points might prompt wireless clients to disconnect their wireless connections. Depending on the clients, the wireless connections might be maintained. In that case, the clients have to reconnect client again.
- 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.