TQ5403 Series Wireless Access Point
Version 6.0.2-0.1 Software Release Notes

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

Supported Platforms

The following access points support version 6.0.2-0.1:

- TQ5403
- TQm5403
- TQ5403e

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

The version 6.0.2-0.1 firmware filenames are listed here:

- AT-TQ5403-6.0.2-0.1.img.zip
- AT-TQm5403-6.0.2-0.1.img.zip
- AT-TQ5403e-6.0.2-0.1.img.zip

New Features and Enhancements

- Session Key Refresh Rate
- Session Key Refresh Action
- User ID is added to an 802.1x authentication log.
- An information collecting function is added to control beacons for Channel Blanket. (TQ5403 and TQ5403e only)
- The access point issues a log message when a wireless client connects to or disconnect from the access point.

Resolved Issues

- The access point had 802.11 Frame Aggregation and Fragmentation vulnerability issues.
- The access point did not share the authentication result for Captive Portal under AWC plug-in management.
- When the Captive Portal setting was changed from External RADIUS to Click-through via AWC plug-in, the access point might have been rebooted unexpectedly.
- Enabling Fast Roaming with Dynamic VLAN was enabled changed the VLAN ID of wireless clients.
- When Captive Portal was enabled or WPA Enterprise security was selected, the access point re-authenticated wireless clients every one hour even though the session key refresh rate was set to zero.
- When WPA Enterprise security was selected, the access point re-authenticated wireless clients every one hour even though RADIUS session timeout was set to longer than one hour.
- Even when Management Frame Protection was enabled, Duplicate AUTH Received functioned.
- The access point might have replied an incorrect value to an OID 1.3.6.1.2.1.17.4.3.1.1 request.
- Neighbor AP Detection (SyncScan) might not have worked when Radio 2.4GHz was disabled.
- Reset Button was not able to be disabled via AWC with Vista Manger Mini.
- Setting different IP Addresses and Secret values to AMF Application Proxy Server for VAPs via AWC Plug-in might have caused the access point to reboot unexpectedly.
- AWC Plug-in might not have been able to manage the access point after it was disconnected from AWC Plug-in.
- The quarantine log messages sent by AMF Application Proxy included unexpected characters.
- The access point might have shut down when wireless clients connected and disconnected repeatedly.
- When the access point with Channel Blanket received a packet from a wireless client at the same time as a Radio disconnection process run, the access point might have been rebooted. (TQ5403 and TQ5403e only)

- When firmware was upgraded, the access point issued an unnecessary log message: Division by zero in kernel. (TQ5403 and TQ5403e only)
- The access point might not have communicated to a wireless client when the wireless client using more than one TID repeated hangover. (TQ5403 and TQ5403e only)
- The access point issued an unintended log message when Channel Blanket was used. (TQ5403 and TQ5403e only)
- When the access point with its maximum number of wireless clients opened the Associated Client page, the access point might have been rebooted unexpectedly. (TQ5403 and TQ5403e only)
- When trying to collect technical support information, the access point might have been rebooted unexpectedly. (TQ5403 and TQ5403e only)
- When a wireless client using WPA-PSK (TKIP) connected to the access point with Channel Blanket, after handover, the wireless client was not able to communicate to access points. (TQ5403 and TQ5403e only)
- Setting all the parameters of Passpoint might have caused the access point to reboot.
- WPA3 on VAP0 did not function correctly when the configuration was made via AWC Plug-in.
- Captive Portal might have not functioned correctly when the 50th HTTP website was entered in the Walled Garden registration list.
- When AMF Application Proxy used Isolation as the action, wireless clients using PMKSA cache reconnected from the access point after isolation because the access point assigned a wrong VLAN ID.
- Using Radio 2 might have caused the access point to reboot.
- When three Online Sign-Up (OSU) server icons were set via Vista Manager mini, the access point was not manageable with Wireless LAN Controllers.
- When an OSU server icon was set via Vista Manager mini, the OSU icon upload page did not display correctly.
- When Security was set to WPA Enterprise and AMF Application Proxy was enabled, AMF action did not work after wireless clients started roaming.
- Handing over a wireless client to Channel Blanket VAP might have caused the access point to reboot.
- When the access point sent statistics information to a wireless controller, it might have been unable to manage the access point.
- When the “/” character in SSIDs was entered via the AWC plug-in, the plug-in displayed the character incorrectly.
- Handing over a wireless client to Channel Blanket VAP might have caused the access point to reboot. (TQ5403 and TQ5403e only)
- After sending statistics information to a wireless controller, the access point might not have been manageable via the wireless controller. (TQ5403 only)

Specification Changes

The following changes are made to the specifications in version 6.0.2-0.1 management software:

- Transporting WDS to VLAN IDs is supported.
- TKIP is supported when Channel Blanket is managed by AWC with Vista Manger mini. (TQ5403 and TQ5403e only)
- The Tx power displayed on the Status page was changed from a dBm value to max, high, middle, low, or min.
- Issuing an SA timeout query log

  When a valid SA Query Response is received from a wireless client within the SA Query timeout, the access point issues a an SA timeout query log entry.
- Association advertisement is supported when Channel Blanket or AWC-SCL is selected. (TQ5403 and TQ5403e only)
- The session timeout values are shared among the access points when Fast Roaming is used.

Limitation

Here is the limitation for the TQ5403 Series Access Points version 6.0.2-0.1 management software:

- OpenFlow is not supported for the TQ5403 and TQ5403e access points.

Limitations on Channel Blanket

Here are the limitations on Channel Blanket version 6.0.2-0.1 management software:

- Band Steer is not supported with Channel Blanket.
- Neighbor AP Detection is not supported with Channel Blanket.
- All radios in Channel Blanket have to have the same settings.

When Channel Blanket Radio is Enabled

- Changing the RTS threshold is not supported.
- Airtime Fairness is not supported.

When Channel Blanket VAP is Enabled

- Changing the Broadcast Key Refresh Rate is not supported.
- RADIUS Accounting is not supported.
- Fast Roaming is not supported.
- Pre-authentication is automatically disabled.
- Dynamic VLAN is automatically disabled.

- ❒ The Session-Timeout RADIUS attribute is automatically disabled.
- ❒ Captive Portal is automatically disabled.
- ❒ Changing the Inactivity Timer value is not supported.
- ❒ IEEE802.11w (MFP) is not supported. It should be disabled.

Channel Blanket Settings

- ❒ The Management VLAN ID and Control VLAN ID settings are not supported.
- ❒ The VAP VLAN ID and Control VLAN ID settings are not supported.

Wireless Clients' Behavior on Channel Blanket

- ❒ Communications of wireless clients are interrupted when the access point is turned off or reboots. It takes approximately two minutes for the wireless clients connected to the access point that was turned off or rebooted to restore communications.

Known Issues

- ❒ Access points do not synchronize Hostname and SNMP System Name.
- ❒ When only one access point with Channel Blanket enabled is up and running, wireless clients are not able to communicate with the Channel Blanket VAP correctly.
- ❒ The access point might save the Secondary RADIUS Server Key value as empty.
- ❒ Access points might disconnect inactive clients several seconds before the expiration of the Inactivity Timer.
- ❒ Do not use the Associated Client window in the web browser interface to disconnect clients on Wireless Distribution System (WDS) children.
- ❒ In rare instances, the hardware and software tables may develop inconsistencies that can cause access points to reset. This is entered in the log as “kernel: Rebooting due to DMA error recovery.”
- ❒ When Dynamic VLAN is enabled, the access pint returns a wrong value to the OID: 1.3.1.2.1.17.4.3.1.1 (MAC address information) request.
- ❒ When Management Frame Protection (MFP) is enabled, MFP disconnects a wireless client, who requests multiple connections; however, a successful connection log message is issued incorrectly.
- ❒ The access point in Single Chanel mode generated extraneous “Removing STA due to association advertisements” event messages in the system log. (TQ5403 and TQ5403e only)
- ❒ When a wireless client re-connects to Single Channel VAP using PMK cache, the access point might issue a connection log message including RADIUS Server IP address. (TQ5403 and TQ5403e only)
- ❒ The access point might issue an unnecessary log message: Removing STA due to association advertisement when a wireless client is connected to the access point. (TQ5403 and TQ5403e only)
- ❒ 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 on the TQ5403 or TQ5403e access point, or 127 clients on 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 the default IP address in SNMP traps and NTP requests when booted. This occurs 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 not always 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 connections between access points and AMF members.
- 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) when 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 when 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 instances, the access point managed with the AWC plug-in might not be able to save their configurations, in which case Vista Manager EX displays an error message. Saving the configuration again is usually successful.
- When the OSU icon is set via AWC with Vista Manger mini, some parameters in the access point configuration are saved with unintended values.
- The RADIUS attribute “Session-timeout” must be disabled in VAPs with Channel Blanket. (TQ5403 and TQ5403e only)
- The access point might shut down when wireless clients connect and disconnect repeatedly between Channel Blanket VAPs. (TQ5403 and TQ5403e only)
- The access point might not generate technical support information when a significant number of wireless clients connect to Channel Blanket VAP. (TQ5403 and TQ5403e only)
- IEEE802.11w (MFP) should be disabled on access points using Channel Blanket. (TQ5403 and TQ5403e only)

- In rare cases, the wireless module stops responding. When detecting the module with no responding, the access point restarts itself. (TQ5403 and TQ5403e only)
- Even when CCMP+TKIP is configured, the access point Web interface does not display the settings. To view the settings, use Vista Manager EX or AWC Plug-in. (TQ5403 and TQ5403e only)
- The access point might not prompt a wireless client to disconnect its connection when the wireless client saves and applies its wireless settings. In this case, the client must disconnect and reconnect again.
- You cannot set channels 10-13 on the 40MHz bandwidth on the 2.4GHz Radio1.
- Do not use the AWC plug-in to assign WPA3 or “WPA2 and WPA3” security to VAP0 on a radio. WPA3 will not work correctly. Assign a different security to VAP0. WPA3 and “WPA2 and WPA3” are supported on all other VAPs. This issue only applies when using the AWC plug-in to set VAP0 security.
- Link-up and link-down traps use the OID that is not defined in the ifindex/ifAdminStatus/ifOperStatus as a network interface.

Smart Connect (AWC-SC)

- Smart Connect (AWC-SC) reserves the IP address 172.31.0.0/24 for its auto-discovery feature. Do not use that address on any other network device.
- 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 inconsistent.

Supported Countries

The TQ5403, TQm5403, and TQ5403e wireless access points are supported in the countries listed in Table 1. The table includes the firmware versions that initially supported 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.

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**.