TQ5403 Wireless Access Point Series
Version 6.0.1-6.2 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 v6.0.1-6.2 firmware filenames are listed here:

- AT-TQ5403-6.0.1-6.2.img.zip
- AT-TQm5403-6.0.1-6.2.img.zip
- AT-TQ5403e-6.0.1-6.2.img.zip

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.

New Features and Enhancements in v6.0.1-6.2

- This version adds the new SkyDefender feature. The feature allows access points to build access lists from the MAC addresses of wireless devices, and register clients by user information, such as personal names or employee identification numbers. SkyDefender requires Vista Manager EX v3.7.0 or later and AlliedWare Plus v5.5.1-1.1 or later with Vista Manager mini. Refer to the *Vista Manager EX User Guide* and *Wireless Management (AWC) with Vista Manager mini User Guide* for details.
- The Technical Support file in the Maintenance > Support window of the on-board web browser management now includes a log of clients' connections and disconnections. It has a maximum storage of 16,131 entries. The entries include the dates and times of the actions, the radios and VAPs, the clients' MAC addresses, and brief event descriptions. An example is shown here:

  ```
  [2021/09/04 07:29:09] ath1: STA:11:22:33:44:55:66 WPA event 1 notification
  ```

  The "ath" value indicates the VAP and radio on the wireless access point:

  ath0 = VAP0 - Radio1
  ath1 = VAP0 - Radio2
  ath2 = VAP0 - Radio3
  ath01 = VAP1 - Radio1
  ath11 = VAP1 - Radio2
  ath12 = VAP1 - Radio3
  and so on.
- If the access point boots because of a fault condition without generating fault output, it performs the Linux dmesg command and stores the kernel ring buffer data in the Technical Support file.

Resolved Issues in Version 6.0.1-6.2

General

- Link up/down traps used wrong OIDs.
- Access points stopped transmitting broadcast frames on the radios after receiving frames with incorrect LLC headers on the LAN port.

AWC Plug-in

- In rare cases, firmware updates of access points from the AWC plug-in failed.

Channel Blankets

- Packets were lost when access points handed over roaming clients in Channel Blankets.

Smart Connect

- Smart Connect stopped monitoring children, causing the Root access point to reboot.

Vista Manager EX

- The System LED and NTP stopped functioning when the access point resolved VAP configuration mismatches.

Known Issues

General

- Access points do not synchronize Hostname and SNMP System Name.
- Access points might not always save your changes to Secondary RADIUS Server Key fields in the web browser interface.
- 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.
- Access points might boot if there are inconsistencies in their hardware and software tables. The 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 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 cases, access points 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.
- 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.
- Do not use the “/” character in SSIDs if managing the access point with the AWC plug-in. The plug-in displays the character incorrectly.
- 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.

Smart Connect (AWC-SC)

- Smart Connect 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.

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 inconsistent. 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.
- Channel Blankets require a minimum of two access points.
- Wireless access points in Channel Blankets might freeze when clients rapidly connect and disconnect from VAPs.
- The Technical Support Information feature might not work with Channel Blankets.
- IEEE802.11w (MFP) should be disabled 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.

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**.