TQ5403 Series of Wireless Access Points
Version 6.0.1-1.1 Software Release Notes

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

- “Supported Platforms,” next
- “Management Software Filenames” on page 2
- “New Features in Version 6.0.1-1.1” on page 2
- “Supported Countries” on page 2
- “Enhancements” on page 3
- “Specification Changes” on page 3
- “Resolved Issues” on page 4
- “Known Issues” on page 4
- “Operational Notes” on page 6
- “Contacting Allied Telesis” on page 7

Supported Platforms

Version 6.0.1-1.1 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.**

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. For wireless networks that have Channel Blankets, Allied Telesis recommends disabling the feature on all access points before updating the firmware. Do not enable Channel Blankets again until after all units have been updated.

Management Software Filenames

The firmware filenames for Version 6.0.1-1.1 for the wireless access points are shown here:

- AT-TQ5403-6.0.1-1.1.img
- AT-TQm5403-6.0.1-1.1.img
- AT-TQ5403e-6.0.1-1.1.img

New Features in Version 6.0.1-1.1

- The access points now support AWC Smart Connect (AWC-SC) for quick configuration of new or replacement units. The feature requires Vista Manager and the AWC plug-in or AlliedWare Plus and Vista Manager mini. The default setting for AWC-SC on the access points is enabled. Access points automatically search for AWC-SC links when reset or powered on.
- The access points now support Centralized Authentication Data for improved handling of roaming clients. The feature requires Vista Manager and the AWC plug-in or AlliedWare Plus and Vista Manager mini.
- Channel Blankets now support Association Advertisements for improved handling of roaming clients.
- The access points now support DHCP Option 43.
- The access points now support Client Location Estimation in the AWC plug-in.
- The access points now support SNMPv3. (Vista Manager and the AWC plug-in, and AlliedWare Plus and Vista Manager mini do not support SNMPv3.)
- The access points now provide area authentication of wireless clients in floor maps in Vista Manager EX v3.2.1 or later.

Supported Countries

The wireless access points are supported in the countries listed in Table 1. The table includes the version numbers of the first firmware releases to support the countries.

Table 1: Supported Countries

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

Table 1: Supported Countries (Continued)

Country	TQ5403	TQm5403	TQ5403e
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

- The number of VAPs for Channel Blankets has been increased to three from two.
- The time zone can now be set from the AWC plug-in.
- This version adds Network Time Protocol (NTP) synchronization log events to the web browser interface and AWC plug-in.
- The technical support function now includes information on dynamic VLANs.

Specification Changes

- 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

The following items apply to the TQ5403, TQ5403e, and TQm5403 access points:

- The access point generated unnecessary log entries when managed by both the web browser interface and Vista Manager EX.
- The state of the link on the Ethernet port sometimes fluctuated up and down when the access point initialized its management software during reboots.
- SNMP community names that had “#” as the first character did not work.
- Wireless clients could not connect when VAP VIDs and dynamic VIDs were the same.
- Access points stopped forwarding traffic if you displayed the associate wireless clients table while it was updating the table.
- The access point rebooted when part of a WDS bridge.
- The access point could not save its configuration when the first character in an SSID was a space.
- The access points did not allow special characters in an SSID set with the AWC plug-in.
- The access point would be assigned a different IP address by a DHCP server after a firmware upgrade or downgrade.
- The access point failed to properly load its configuration settings after multiple reboots.
- In rare circumstances, the recovery process failed.
- Enabling Dynamic VLAN could corrupt the configuration file.
- The web browser interface displayed the wrong TX Power when it was set with AWC from Vista Manager EX.
- Radios that had VAPs with spaces in their SSIDs experienced unpredictable operations

The following item applies only to the TQ5403e access point:

- The access point displayed its web browser graphical interface incorrectly after transmitting unnecessary SysRq log outputs.

Known Issues

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. For wireless networks that have Channel Blankets, Allied Telesis recommends disabling the feature on all access points before updating the firmware. Do not enable Channel Blankets again until after all units have been updated.

- The access point does not synchronize Hostname and SNMP System Name.
- 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 point.
- 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.
- Wireless clients might not be able to connect to Channel Blanket VAPs when only one access point is running Channel Blankets.
- The access point does not always save new values for the Secondary RADIUS Server Key.
- The access point might increment the Received Counter for a VAP when there are no clients.
- An access point that is managed by AT-Vista Manager EX with AWC plug-in enters an error message in the log when you click on the Radio 1 VAP0 tab in the VAP/Security page.
- The access point reports 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.
- The access point might transmit non-traffic related packets from its radios when initializing the management software during reboots.
- 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 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.
- The access point might not always send the Clear to Send (CTS) signal when clients send the Ready to Send (RTS) signal before connecting to the access point.
- The access point 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.
- 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.
- In rare instances, inconsistencies may occur in the hardware and software tables, which can cause the access point to reset. This is registered in the log as “kernel: Rebooting due to DMA error recovery.”

Note
The following items apply to the TQ5403 and TQ5403e access points. They do not apply to the TQm5403 access point.

- The access point disables the inactivity timer settings for RADIUS in a VAP when you enable Channel Blanket.
- The access point 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.
- Allied Telesis recommends enabling IEEE802.11w (MFP) in WPA Personal Security and Association Advertisements in Advanced Settings under VAP security when using Channel Blankets.
- This release does not support the OpenFlow protocol on TQ5403 and TQ5403e access points.

Operational Notes

Here are the operational notes for this release.

- 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 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 client service 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.

Contacting Allied Telesis

If you need 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.