TQ5403 Series Wireless Access Point
Version 6.0.3-0.2 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 6.0.3-0.2:

- AT-TQ5403
- AT-TQm5403
- AT-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 6.0.3-0.2 firmware filenames are listed here:

- AT-TQ5403-6.0.3-0.2.img.zip
- AT-TQm5403-6.0.3-0.2.img.zip
- AT-TQ5403e-6.0.3-0.2.img.zip

Specification Changes

- When a client was handed over from one AP to another AP in a Channel Blanket, the following log entry used to be produced: "WMI_EVENT_ALLOC_FAILURE (0x5555)". This log entry is no longer produced.

Resolved Issues

The following issues were present in v6.0.3-0.1 and have been resolved in v.6.0.3-0.2.

The following list applies to all three models:

- In rare cases, if an invalid management frame was sent from a wireless client, the AP would unexpectedly restart.
- In a Channel Blanket environment, the AP may have unexpectedly restarted when detecting invalid behavior on the wireless chip.
- When the AP received a frame for a wireless client for the first time from the wired side, it could not correctly forward the frame wirelessly if any of the following features were enabled:
  - Dynamic VLAN
  - Captive portal Virtual IP address
  - AMF Application Proxy
  - WDS
- When the AP queried its primary RADIUS server and received no response, it would correctly resend the query after 3 seconds. However, it would also query its secondary RADIUS server at that time, instead of waiting for the second query to the primary server to time out.
- If the AP produced a large number of debug log messages in a short amount of time, this could consume too much memory and cause the AP to unexpectedly restart.
- When LLDP PoE negotiation is enabled, the following warning message was displayed in the AP's GUI: "Operating under IEEE 802.3af PD power restrictions. Please change to IEEE 802.3at or AC power." This message is no longer displayed.
- The following error log message was produced when obtaining Technical Support Information: "daemon.err uhttpd[4486]: ln: atmf_agent_log/atmf_agent_log: File exists". This message is no longer displayed.
- If the AP's system time was set to a future time, and then the time was corrected by synchronization with the AWC plug-in in Vista Manager, then the AWC plug-in would not display the AP's statistics and the number of connected clients.
- If a wireless client had the same IP address as the IP address of a wireless client that had previously been authenticated through web authentication on the AP, then that wireless client could not be authenticated through web authentication.
- If recovery from a wireless module error was unsuccessful, the AP could unexpectedly restart.
- If you changed the "Mode" setting of a wireless LAN from 802.11a or 802.11b/g to another mode (including 802.11n), a pop-up box displayed unnecessary log messages. These messages are no longer displayed.
- In rare cases, the AP restarted unexpectedly when Dynamic VLAN was enabled.
- Vista Manager mini did not correctly apply the Passpoint osu-providers method-list settings. This prevented Passpoint from operating correctly.

- When the Passpoint OSU Status was enabled, it was possible to apply the settings without entering the OSU SSID and OSU Providers Server URI. Now these values must be entered.
- It was not possible to get the MIB value of the "atkkWiAcClientTable" for a large number of wireless client connections. The attempt would take too long and time out.
- If the AP was powered off and on multiple times in a short period of time, and then you tried to produce a Technical Support file for the AP, then the AP could unexpectedly restart.

The following list applies to Channel Blanket (AWC-CB) and/or Smart Connect (AWC-SC) on the TQ5403 and TQ5403e models:

- When the wireless client association frame length was greater than 255 bytes, the AP failed to connect to the Channel Blanket VAP.
- When Channel Blanket and Smart Connect were used together, the number of participating APs in Channel Blanket may not have matched the number of allocated APs.
- With Smart Connect, when the wireless connection was disconnected because a satellite AP was in an abnormal state, it could take several minutes to reconnect.
- If the VAP used in Smart Connect got into an abnormal state while the Smart Connect link was down, an unexpected restart could occur during recovery from the abnormal state.
- In rare situations, an unexpected restart could occur when using Channel Blanket.
- When a wireless client was connected to a VAP in a Cell configuration in a hybrid Channel Blanket and Cell environment, association advertisement did not work.
- During multicast communication in Channel Blanket environment, too much memory could be consumed and the AP could unexpectedly restart.
- When a client was roaming from a Cell to a Channel Blanket, or between Channel Blankets, the client’s attempts to re-connect with a Reassociation Request were sometimes unsuccessful.

Limitations

Here is the list of limitations for the TQ5403 Series Access Points version 6.0.3-0.2 management software:

- OpenFlow is not supported. (TQ5403 and TQ5403e)
- When saving and applying settings, the access point prompts wireless clients to disconnect; however, connection with some clients might not be disconnected. In the case, disconnect and connect the clients again.
- 10 to 13 channels cannot be selected on the 40MHz bandwidth on 2.4GHz Radio1.
- The maximum number of clients is up to 200 when the value is set on the web interface.
- Do not use the 172.31.0.1/24 IP address when AWC-SC auto discovery is used.
- Do not use other VAPs on the same radio if using AWC-SC.
- The root access point and satellite access points must have the same VID settings for the client service when using AWC-SC.
- AWC-SC cannot use with AMF guest node.

- A switch must not use DHCP Snooping on the access point that is connected to a network if using AWC-SC.
- The WPA3-personal or WPA3+WPA2-personal setting is not applied correctly to VAP0 using AWC. In this case, use other VAPs.

Limitations on Channel Blanket

Here are the list of limitations on Channel Blanket in the version 6.0.3-0.2 management software:

- Band Steer is not supported with Channel Blanket.
- All radios in Channel Blanket must have the same Radio 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.

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.

Specifications and Limitations on Easy Setup

Here is a list of specifications and limitations for Easy Setup:

- When the VAP mode is set to Cell Type, the Radio and VAP0 settings must be configured as follows:
  - Radio1 setting

    Basic Settings > Mode: IEEE802.11b/g/n
  - Radio2 setting

    Basic Settings > Mode: IEEE802.11a/n/ac
  - Radio1/Radio2 VAP0 settings

    Security > Mode: WPA Personal

    Security > WPA Version: WPA2 and WPA3

    Security > Cipher Suites: CCMP

    Security > IEEE802.11w (MFP): Enabled
- When the VAP mode is set to Single Channel, the Radio and VAP0 settings must be configured as follows:
  - Radio2 setting

    Basic Settings > Mode: IEEE802.11a/n/ac

    Advanced Settings > Maximum Client: 500
  - Radio1/Radio2 VAP0 settings

    Basic Settings > Security Mode: WPA Personal

    Basic Settings > Security WPA Version: WPA2

    Basic Settings > Security Cipher Suites: CCMP

    Basic Settings > IEEE802.11w (MFP): Disabled

    Advanced Settings > Association Advertisement: Enabled
- Single Channel can be selected only when AWC-SCL Cluster is enabled.
- The Control Frame setting in the Single Channel mode is automatically changed based on the Management VLAN Tag settings of the access point.
  - Management VLAN is disabled: Control Frame setting is changed to untagged frame.
  - Management VLAN is enabled: Control Frame setting is changed to tagged frame, which is the same as the Management VLAN ID.

Specifications and Limitations on AWC-SCL Cluster

Here is a list of specifications and operational notes for AWC-SCL Cluster:

- The access points in AWC-SCL share the configuration except:
  - Host Name
  - MAC address
  - IP address settings
  - SNMP system name, system contact, and system Location
  - Transmission power when VAP0 mode is set to the Single Channel Type.
- The maximum number of AWC-SCL members is five.
- The access points in AWC-SCL cannot be managed by Vista Manager EX or Vista Manager mini.
- When the access point in AWC-SCL and the Single Channel type is added to AWC-SCL as a device replacement, the configuration re-apply process automatically runs if the access point has the largest MAC address among the cluster members. As a result, the wireless clients that had been connected to the access point are all disconnected.

Limitation on the Access Point Setting using Easy Setup

- Setting using both Easy Setup and Vista Manage EX is not supported.

Limitations on the Access Point Setting using Single Channel Type

- Changing the Radio settings is not supported.

  When the Radio settings are not default values, change the settings to default before setting the Single Channel Type.

- Changing Radio2 VAP0 setting is not supported on “Settings > VAP/Security” page.

  When the Radio2 VAP0 settings are not default values, change the settings to default before setting the Single Channel Type; however, the parameters described in the specifications are executed.

- The access points with the same “Single Channel group ID” on different networks in near wireless spatial are not supported.
- Setting to management VLAN ID and Control VLAN ID 1 is not supported.
- More than seven access points in the Single Channel Mode is not supported.

  Establishing a Single Channel with more than seven access points is possible, but not supported.

- The largest MAC address among AWC-SCL cluster’s members is assigned to VAP’s BSSID of the Single Channel Type.

Known Issues

- Access points do not synchronize the Hostname and the SNMP System Name.
- On the Maintenance > Support Page of the Web UI, in the Technical Support Information section, a note states that the 801.1x authentication log contains the user ID and does not contain the password. In fact, neither the user ID nor the password is included.
- 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 point returns a wrong value to the OID: 1.3.1.2.1.17.4.3.1.1 (MAC address information) request.
- Access points in Single Channel mode generate extraneous “Removing STA due to association advertisements” event messages in their system log. (TQ5403 and TQ5403e only)
- When a wireless client re-connects to Single Channel VAP using the PMK cache, the access point might issue a connection log message including the RADIUS Server IP address. (TQ5403 and TQ5403e only)
- The access point might issue an unnecessary log message of “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 (MFP) is enabled.
- For some wireless clients, roaming may be slower than expected if IEEE802.11w Management Frame Protection (MFP) is enabled.
- 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 boot up.
- When booted, access points transmit two DHCP discover packets (untagged and tagged VID 1) when the Management VLAN tag setting is disabled.
- The 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.
- 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 restart 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)
- A wireless client with IPv6 Router Advertisement does not communicate on Dynamic VLAN VAP.
- MAC Access Control does not work when Distributing System is enabled on IEEE802.11r.
- The SNMPv3 traps EngineBoot and EngineTime are always sent with a value of 0.
- If you select Hidden SSID, you cannot use the following features with fast roaming:
  - IEEE802.11k (Neighbor Reports)
  - IEEE802.11v (BSS Transition Management Frames).
- When AWC-SC is enabled on an AP and you access the SSID "sc-initial-provisioning" VAP in the VAP/Security Settings page on the AP’s GUI, the security tab is not displayed.

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, visit the Allied Telesis web site at **www.alliedtelesis.com/support.**