# TQ6602 Wireless Access Point
# Version 7.0.1-4.1 Software Release Notes

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



## Firmware File

The firmware filename for the TQ6602 version 7.0.1-4.1 access point is:

- ❒ AT-TQ6602-7.0.1-4.1.img

For instructions on how to upgrade the firmware on the TQ6602 access point, see the *TQ6602 Wireless Access Point Management Software User’s Guide* at **www.alliedtelesis.com/library.**

## New Features

The following new features were added to version 7.0.1-4.1 for the TQ6602 wireless access point:

- ❒ Support for preventing wireless clients connected to Channel Blanket environment from being forced into Power Save mode.

## Enhancements

The following enhancements were added to version 7.0.1-4.1 for the TQ6602 wireless access point:

- Security Association Query timeout log has been added. If an access point queries a wireless client for a Management Frame Protection (MFP) and the wireless client does not respond, the access point will send a SA Query timeout log including the wireless client's disconnect log.
- A reject log output has been added for when a wireless client is denied connection by AMF Security in VAP, with Application Proxy enabled:
  - hostapd : wdevXapY: reject STA zz:zz:zz:zz:zz:zz due to Application Proxyzz:zz:zz:zz:zz:zz : Wireless client MAC address
- A reject log message has been added to indicate when a wireless client is denied connection by MAC access control, MAC address lists or external RADIUS:
  - hostapd: wdevXapY: reject STA zz:zz:zz:zz:zz:zz due to MAC Authenticationzz:zz:zz:zz:zz:zz : Wireless client MAC address
- In Proxy ARP, the upper limit of ARP cache entries has been extended from 2048 to 8192.
- Beacons that include Partial Virtual Bitmap (PVB) sent from access points in the same Channel Blanket are now synchronized.

## Specification Changes

The following specification changes were added to version 7.0.1-4.1 for the TQ6602 wireless access point:

- To increase security the device GUI and Captive Portal authentication page cannot be accessed using:
  - 3DES encryption
  - TLSv1.0, TLSv1.1 or TLSv1.2
- For models sold in Japan:
  - the GUI default time zone is now Asia/Tokyo
  - the GUI default language is now 'Japanese'

## Resolved Issues

The following issues were resolved in Version 7.0.1-4.1 for the TQ6602 wireless access point:

- The No Acknowledgment field on QoS page would display empty even when WiFi Multimedia (WMM) was Disabled.
- The access point would issue a detect beacon transmission log when the configuration of the access point was changed.

- If an access point had a VAP configured with WPA Enterprise mode WPA2/WPA3 (CCMP), it was not displayed on the Neighbor AP page.
- When RADIUS accounting was enabled for Radio 2 web authentication, the accounting request [Stop] was not sent when wireless client has session timeout after web authentication.
- With Channel Blanket, memory leaks occasionallyoccurred with continuous connections/ disconnections.
- Querying OID 1.3.6.1.2.1.17.4.3.1.1 (MAC address information) returned an incorrect response.
- With SNMPv3, settings could be applied even with user name and password were blank.
- If an access point had a hidden SSID, SNMP would not display a blank for the SSID in the neighbor AP list.
- “5s” was showing in the “Week” options for “Daylight Saving Time Start Date” and “Daylight Saving Time End Date” on the “Time” setting page.
- "Saturday” could not be applied to the daylight saving time end day via wireless LAN controller.
- When using Channel Blanket, if security is set to "CCMP+TKIP", the setting values were not shown in the AP GUI.
- With neighbor AP detection, if a scan failed 5 times, the scan detection interval would shift by 1 minute.
- Changes could not be applied on the Radio or VAP/Security settings from the access point's GUI when MAC Access Control was set to Application Proxy from the Vista Manager EX AWC Plug-in.
- With Channel Blanket enabled, and an AP is assigned an IP address via DHCP, the DHCP packet could contain an incorrect MAC address, when the following functions were enabled:
  - Dynamic VLAN
  - Virtual IP address for Captive Portal
- When a RADIUS query received no response from the primary RADIUS server and the query was resent after 3 seconds, instead of waiting for a response, failover to the secondary RADIUS server occurred.
- The following error message was incorrectly displayed when an access point was powered by IEEE802.11at (PoE+) and LLDP was enabled: "Operating under IEEE802.3af PD power restrictions. Please change to IEEE802.3at or AC power.”
- The access point's system time would sometimes be incorrect when powered up. The system and time and AWC Plugin would not be synchronized, resulting in statistics and the number of connected clients not being displayed.
- When changing Radio mode, the following unnecessary text was included in the popup message: "In addition, any VAP currently configured for WPA will have the CCMP (AES) cipher suite enabled."
- When the access point detected an error in the wireless chip and was trying to recover while the AMF Application Proxy was up and running, the access point might have rebooted.

- Even when Fast Transition of Fast Roaming is enabled, Fast Roaming does not function if Dynamic VLAN is disabled. Dynamic VLAN must be enabled to use Fast Roaming
- RADIUS Access-Request sometimes did not include NAS-IP-Address attribute.
- In Channel Blanket, after applying settings from the wireless LAN controller, the Channel Blanket VAP was sometimes not enabled and the wireless client was not be able to connect.
- The access point occasionally shut down when a large number of log files were output.
- When accessing a neighbor AP list with a private MIB, an SNMP process would sometimes restart.
- Sometimes DHCP would not assign an IP address to certain wireless devices on the 5GHz channel.
- In Channel Blanket, an unexpected reboot could occur.
- A wireless client would fail to connect to the access point when being authenticated through PMK (Pairwise Master Key).
- When proxy ARP was enabled, ARP continued to send responses for several minutes after the wireless device was disconnected.
- Association logs were not output when the wireless client connect to a VAP.
- After initially authenticating using PMKSA cache, if PMK timed out and the device reauthenticated using RADIUS, the log would show it was reauthenticated using PMKSA cache.
- After initially authenticating using PMKSA cache, if the session timed out and the device was reauthenticated using RADIUS, the log would show it was reauthenticated using PMKSA cache.

## Known Issues

Here are the known issues for the TQ6602 version 7.0.1-4.1 management software:

- The client's User ID and password are not included in the technical support file.
- The access point saves a value for the secondary RADIUS IP or secondary RADIUS server key even when only one of them is entered. Saving incomplete secondary RADIUS server information does not affect any operation.
- The access point might send NTP packets before obtaining its IP address from DHCP servers.
- When a wireless client's password includes the "%" symbol, the access point does not allow the wireless client to connect to a WEP VAP.
- The access point issues an error log when a radio interface starts up.
- When Band steering is enabled on Radio1 and Hidden SSID is enabled on VAPs, the access point does not allow wireless clients to connect to the VAPs on Radio1.
- The TX and RX rates on the Associated Clients page are displayed incorrectly.
- An ad hoc device is displayed as an AP in the type field on the Neighbor AP page.
- A wireless client fails to connect to the access point using PMKSA cache.
- The access point issues an error log when the firmware is upgraded or the access point is reset to the Factory Default.
- The access point might send a Neighbor AP detection report without an SSID to Vista Manager.
- The access point might detect radar incorrectly.
- The access point displays the Neighbor AP with WEP security to None.
- The access point might issue a radar detection log when the channel is changed.
- The access point displays WPA3 Enterprise (GCMP) as WPA3 Enterprise (CCMP) on the Neighbor AP page.
- The access point issues a detect beacon transmission log when the configuration of the access point is changed.
- When Client Isolation is enabled on Channel Blanket, Client Isolation must be disabled on the radio settings of the access point. If Client Isolation is enabled on the radios of the access point, wireless clients connected to a Channel Blanket VAP might be able to communicate among them.
- When all of the access points that belong to the same Channel Blanket start at the same time, it takes approximately three minutes for wireless clients connected to the Channel Blanket VAP to start communicating among them. However, wireless clients and devices on the wired network might start communicating less than three minutes even while wireless clients cannot communicate among them.
- When a wireless client is denied connection by the MAC Address filter, a disconnection log entry that the access point issues does not include a reason, which the MAC Address filtering denied the client.
- Enabling IPv6 communication with IP auto-configuration of IPv6 Router Advertisement does not function on VAPs with dynamic VLAN enabled.

- More than 50 pages in Walled Garden is registered even though the access point only supports up to 50 pages.
- Wireless clients might be disconnected if the access point in Channel Blanket failed to a communication check from the wired network.
- Combining WDS and radar channels (W53 and W56) is not supported. When using WDS, do not select W53 or W56 channel.

## Limitations

Here are the limitations for the TQ6602 version 7.0.1-4.1 management software:

- Zero Wait DFS is not supported.
- Displaying of Client Traffic Counter, which is operated by Vista Manager EX, is not supported for the access point.
- Wireless clients may not be able to connect via the Radio 1 interface in certain conditions. Allied Telesis verified that this behavior occurred when the number of enabled VAPs of Radio 1 and number of surrounding APs (BSSID) exceeded the numbers shown in the table.

| Number of Enabling VAPs | Number of Surrounding APs (BSSID) |
|---|---|
| 1 | 120 |
| 3 | 95 |
| 5 | 75 |
| 10 | 55 |
| 16 | 35 |

  In real environments, this behavior may occur even if the numbers are not exceeded. It is likely caused in conditions when the wireless spatial is congested by low-rate packets.

## Limitations on Channel Blanket

The Channel Blanket feature has the following limitations:

### Limitations on the Access Point

- Band Steer is not supported.
- Neighbor AP Detection is not supported.
- All access points on Channel Blanket need to have the same Radio settings.
- WDS is not supported.
- Association Advertisement is not supported.

### Limitations on the Blanket Radio Interface

- The value of the RTS Threshold cannot be changed.
- Airtime Fairness is not supported.
- OFDMA is not supported.
- MU-MIMO is not supported.

### Limitations on Channel Blanket-enabled VAP

- The value of the Broadcast Key Refresh Rate cannot be changed.
- The value of the Session Key Refresh Rate cannot be changed.
- The value of the Session Key Refresh Action cannot be changed.
- RADIUS Accounting is not supported.
- Fast Roaming is not supported.
- Dynamic VLAN is forced to be disabled.
- The Session-Timeout RADIUS attribute is forced to be disabled.
- The value of the Inactivity Timer cannot be changed.
- IEEE802.11w(MFP) needs to be disabled.

### Limitations on the Blanket Settings

- The Management VLAN ID and Control VLAN ID cannot be specified to the same VLAN.
- The VAP VLAN ID and Control VLAN ID cannot be specified to the same VLAN.

### Limitations on the Blanket Behavior

- When the access point is turned off or rebooted, it takes approximately two minutes to restore the communication with wireless clients that is connected to the access point.

## Supported Countries

Version 7.0.1-4.1 continues to support the following countries:

- Australia
- Austria
- Belgium
- Bosnia and Herzegovina
- Bulgaria
- Canada
- China
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Gibraltar
- Greece

- ❒ Hong Kong
- ❒ Hungary
- ❒ Iceland
- ❒ India
- ❒ Ireland
- ❒ Italy
- ❒ Japan
- ❒ Latvia
- ❒ Liechtenstein
- ❒ Lithuania
- ❒ Luxembourg
- ❒ Macedonia
- ❒ Malaysia
- ❒ Monaco
- ❒ Montenegro
- ❒ Netherlands
- ❒ New Zealand
- ❒ Norway
- ❒ Poland
- ❒ Portugal
- ❒ Romania
- ❒ Serbia
- ❒ Singapore
- ❒ Slovakia Republic
- ❒ Slovenia
- ❒ Spain
- ❒ Sweden
- ❒ Switzerland
- ❒ Taiwan
- ❒ Thailand
- ❒ Turkey
- ❒ Ukraine
- ❒ United Kingdom
- ❒ United States
- ❒ Viet Nam

## Contacting Allied Telesis

For more information, go to **www.alliedtelesis.com**.