TQ6602 Wireless Access Point
Version 7.0.1-4.2 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 7.0.1-4.2 access point is:

- AT-TQ6602-7.0.1-4.2.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.**

Resolved Issues

The following issues were resolved in Version 7.0.1-4.2 for the TQ6602 wireless access point:

- When applying Web-GUI settings, invalid numeric entries, such as beginning with a "0" and decimals, were allowed to be saved & applied instead of rejected.
- When a wireless client was roaming between Radios on the same AP, the connected client list entries would sometimes not be cleared. When the maximum number of entries was reached, new wireless clients could not connect.
- If a wireless client sent multiple PMKIDs during 4-way handshakes when connecting, the connection would sometimes fail.
- During handover with Channel Blanket, some access points could experience unauthorized memory access which could result in a system reboot.
- If the channel was changed by AWC calculation or DFS detection, the access point would sometimes send an abnormal broadcast which the wireless client could not receive, causing communication failure.

- With Vista Manager EX v3.12.X or later, when an AP Profile with security WEP and Key Type "ASCII" was applied, the radio wave output of the access point would stop and wireless clients would be disconnected.
- When the Captive Portal page was viewed over HTTPS, the Captive Portal page would sometimes become inaccessible.
- MIB value “atkkWiAcClients” was not available when a wireless client enabled SNMP.

Known Issues

Here are the known issues for the TQ6602 version 7.0.1-4.2 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.
- If a wireless client's IP address and Virtual IP address are on the same subnet, the Captive Portal authentication page will not appear.
- 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.
- EngineBoots and EngineTime values of SNMPv3 Trap are sent with a value of 0.
- 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.
- When IEEE802.11r/11k/11v is enabled, for some access points with Hidden SSID enabled, information is not shared correctly.

Limitations

Here are the limitations for the TQ6602 version 7.0.1-4.2 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 When Using With 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 7.0.1-4.2 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**.