TQ6602 Wireless Access Point
Version 7.0.1-3.2 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 7.0.1-3.2 access point is:

- AT-TQ6602-7.0.1-3.2.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.**

Enhancements

The following enhancements were added to version 7.0.1-3.2 for the TQ6602 wireless access point:

- Channel Blanket and Temporal Key Integrity Protocol (TKIP) are able to be activated at the same time.
- Wireless client statistics are available on the Cell and Channel Blanket modes.
  - You can check the Tx and/or Rx counters of an associated wireless client using Vista Manager EX.
- LED color for PoE
  - You can change the LED color for PoE by going to Settings > System > LED page.

Resolved Issues

The following issues were resolved in Version 7.0.1-3.2 for the TQ6602 wireless access point:

- The access point occasionally shut down when a wireless client was repeatedly connected and disconnected.
- The access point deleted a dump file when the Vista Manager EX obtained technical support information.
- [AWC Channel Blanket] The access point failed to transmit packets from a wireless client at the Hand-Over.
- After the access point booted up, it occasionally failed to gain an IP address from DHCP.
- The settings of Channel Blanket were not stored on the backup configuration file.
- [AWC Channel Blanket] The access point occasionally shut down when a wireless client was disconnected from a Channel Blanket VAP.
- The access point failed to send Captive Portal authentication information to the Vista Manager EX when the session timeout of Captive Portal was set to 0.
- The access point occasionally failed to issue syslog messages.
- [AWC Channel Blanket] the access point occasionally disconnected wireless clients when the Channel Blanket access point booted up.
- The access point occasionally failed to apply a configuration from the Vista Manager EX.
- [AWC-Channel Blanket] The MAC address of the Channel Blanket access point occasionally changed to another address.
- Web authentication on the Captive Portal VAP was not executed when a user repeatedly to disconnect a wireless client.
- The access point issued a VLAN 0 assigned log when AMF-Security set no vlan to a wireless client.
- The access point added “.0” to the OID of SNMPv3 traps.
- The access point in WDS occasionally shut down when the number of wireless clients communicating over the WDS link increased.
- The the IF-MIB counter of a radio interface might have returned an incorrect value: "ifOutErrors", "fOutUcastPkts", or "ifOutDiscards."
- The total power that each access point requested to a PoE switch in LLDP and the max power consumption of the PoE power specification did not match.
- A user password might have been lost when the user tried to access the access point via the Web interface while settings were applied from AWC Wireless Controller.
- IEEE802.11ax wireless clients occasionally did not communicate.
- The access point in WDS occasionally shut down when a user changed the configuration.
- When the session timeout was set by the RADIUS server even in a Channel Blanket VAP, wireless clients were disconnected according to the session timeout value set by the RADIUS server.

- The handover of a wireless client did not occur among the access points in the Channel Blanket network when the wireless client was in the power-saving mode and only transmitting non-data frames. The handover was required wireless clients to transmit data frames.
- A wireless client might have been disconnected from a Channel Blanket VAP when the wireless client was in the power-saving mode.
- Wireless clients were not able to connect to the access point with the WPA2 TKIP when the WPA version was set to the WPA and WPA2 option and the cipher suite was set to CCMP and TKIP option.
- The access point might have shut down when wireless clients roamed among Channel Blankets when both Channel Blanket and Advertise Association were enabled.
- The access point rebooted irregularly for recovery when detecting a Neighbor AP.
- Wireless clients were not able to communicate among them when the mode was set to the WPA2 personal and the Cipher Suites field was set to CCMP.
- When an IP address was once used to authenticate a wireless client, the authentication specified in Capital Portal would not be completed for another wireless client with the same IP address.
- In the Channel Blanket, the access point might not have received frames from wireless clients correctly during their handover and have shut down.
- In Channel Blanket, when Vista Manager EX and AWC plug-in applied a configuration to the access point, it might have shut down due to a conflicting internal processes of the access point.
- 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.
- In Channel Blanket, the access point that was not supposed to return ACKs returned ACKs.

Known Issues

Here are the known issues for the TQ6602 version 7.0.1-3.2 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 issues an error log when a Radio status setting is changed.
- The access point might send a Neighbor AP detection report without an SSID to Vista Manager.
- Multiple unicast de-authentication packets are sent to the Radio 2 interface when a wireless client is disconnected due to a setting change.
- 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 No Acknowledgment field on QoS page displays empty even when WiFi Multimedia (WMM) is selected Disabled.
- The access point issues a detect beacon transmission log when the configuration of the access point is changed.
- The access point shuts down when multiple AMF-Security IP addresses or a secret key is set to each VAP.
- You cannot save and apply Saturday as the Daylight Saving Time End Day by Vista Manager EX and AWC Plug-in.
- 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.
- Communication might delay on the Channel Blanket VAP when a wireless client enters the power saving mode.
- A VAP with Dynamic VLAN enabled cannot use IPv6 communication when the IPv6 Router Advertisement IP auto-configuration is enabled.
- Do not apply changes on the Radio or VAP/Security settings from the Web Interface of the access point when the MAC Access Control is set to Application Proxy from Vista Manager EX and plug-in.

  Making a change on the Radio or VAP/Security settings from the Web Interface resets the MAC Access Control to its default setting when the MAC Access Control is set to Application Proxy.
- 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.
- 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.
- The access point does not display, on the Neighboring AP page, an access point including a VAP that is configured with the WPA Enterprise mode, WPA2 and WPA3 versions, and CCMP in the Cipher Suites.

Limitations

Here are the limitations for the TQ6602 version 7.0.1-3.2 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 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.
- 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 7.0.1-3.2 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**.