



TQ6602 Wireless Access Point Version 7.0.1-1.1 Software Release Notes

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

- ☐ “Firmware File,” next
- ☐ “New Features” on page 1
- ☐ “Specification Change” on page 2
- ☐ “Resolved Issues” on page 2
- ☐ “Known Issues” on page 3
- ☐ “Limitations” on page 4
- ☐ “Limitations on Channel Blanket” on page 5
- ☐ “Supported Countries” on page 6
- ☐ “Contacting Allied Telesis” on page 7

Firmware File

The firmware filename for the TQ6602 Version 7.0.1-1.1 access point is:

- ☐ AT-TQ6602-7.0.1-1.1.img

For instructions on how to upgrade the management software on the TQ6602 wireless access point, see the TQ6602 *Wireless Access Point Management Software User's Guide*, available on the Allied Telesis Inc. website at **www.alliedtelesis.com/library**.

New Features

The following new features are added to the TQ6602 version 7.0.1-1.1 access point:

- ☐ Application Proxy
This feature can be enabled with Vista Manager EX version 3.7.0 or later and AWC Plug-in.
- ☐ RTS Threshold
- ☐ The 80+80 MHz option for the Bandwidth (Radio2)
- ☐ Combination with Channel Blanket and Proxy ARP
This feature can be enabled in the CB Profile of Vista Manager EX with AWC Plug-in.

Specification Change

The following changes are made to the specifications in the TQ6602 version 7.0.1-1.1 access point:

- ❑ The maximum number of clients is changed to 500.
- ❑ The access point is able to associate with wireless clients when the RADIUS session-timeout attribute value of “MAC Access Control” External RADIUS is 0.
- ❑ The RSSI is added to a wireless client association log.
- ❑ The supported number of Channel Blanket VAPs is changed to 10.
- ❑ APSD is supported with Vista Manager EX.
- ❑ Association Advertisement is supported with Vista Manager EX.
- ❑ Proxy ARP is supported with Vista Manager EX.

Resolved Issues

The following issues were resolved in Version 7.0.1-1.1 for the TQ6602 wireless access point:

- ❑ An NTP process might have started randomly.
- ❑ The access point might have issued duplicated logs when radar was detected.
- ❑ The RSSI signal icon was not displayed correctly on the Neighbor AP page.
- ❑ The access point issued an error message when it has four or more VAPs with MU-MIMO or OFDMA enabled.
- ❑ The access point transmitted broadcast/multicast frames to unassociated wireless clients.
- ❑ The WPA supplicant information was not included in the technical support information file.
- ❑ The access point might have shut down when it disconnected a wireless client.
- ❑ The access point might have recognized a correct wireless frame as an abnormal frame and restarted the wireless chip.
- ❑ The access point sent a Link Up or Link Down trap with incorrect values in the ifIndex, ifAdminStatus, and/or ifOperStatus.
- ❑ The access point might have shut down when a wireless client was connected and disconnected promptly.
- ❑ A wireless client was not able to connect to a Channel Blanket VAP when the wireless client sent an association frame that was longer than 255 byte.
- ❑ The access point might have disconnected a wireless client on a Channel Blanket VAP when the wireless client's handover occurred.
- ❑ The access point did not issue a wireless client connection log on a cell-operating VAP (non-Channel Blanket VAP) when the access point has both Channel Blanket VAPs and cell-operating VAPs.
- ❑ The source access point might have issued an unnecessary frame to wired networks when a wireless client's handover occurred.

- ❑ The access point might have shut down when more than 240 wireless clients were connected.
- ❑ The RSSI value in a wireless client connection log on Channel Blanket VAPs was not displayed correctly.
- ❑ The access point issued duplicated disassociation logs on Channel Blanket VAPs when disconnecting a wireless client.
- ❑ The Inactivity Timer did not function correctly on Channel Blanket VAP.
- ❑ Wireless clients might not be able to communicate to the access point when another access point in the Channel Blanket rebooted.
- ❑ The access point might have sent a beacon with a wrong sequence number on Channel Blanket VAPs.
- ❑ The access point might have shut down when failing to restart the wireless chip.
- ❑ The access point might have aborted the NTP process and Off LED when detecting a configuration error.
- ❑ The access point might have shut down due to an abnormal processing of the wireless chip.
- ❑ The Client Isolation feature did not work on the VAPs except VAP0.
- ❑ The access point disconnected a wireless client when Vista Manager EX and AWC Plug-in applied the AWC calculation result, even if the change was only the TX power pattern.
- ❑ Wireless clients might not have communicated to cell-operating VAPs (non-Channel Blanket VAPs) when the access point has both Channel Blanket VAPs and cell-operating VAPs.
- ❑ The access point stopped sending beacons when Neighbor AP Detection was enabled and the Channel setting was set to Auto.
- ❑ Wireless clients might not have been able to connect to the cell-operating VAPs (non-Channel Blanket VAPs) with enabled-IEEE802.11w (MFP) when the access point has both Channel Blanket VAPs and cell-operating VAPs.
- ❑ The access point might have shut down when a wireless client's handover occurred.

Known Issues

Here are the known issues for the TQ6602 Version 7.0.1-1.1 management software:

- ❑ The client's User ID and password are not included in the technical support file.
- ❑ The access point might save an empty value for the Secondary RADIUS Server Key even when it is entered properly.
- ❑ The access point might send NTP packets before receiving 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 when 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.
- ❑ Even when a loop state is resolved, WDS access points do not work properly. You must restart all the WDS access points for recovery.
- ❑ 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 the 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.

Limitations

Here are the limitations for the TQ6602 Version 7.0.1-1.1 management software:

- ❑ Zero Wait DFS is not supported.
- ❑ Displaying of Client Traffic Counter, which is operated by Vista Manager, 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 occurs when the number of enabled VAPs of Radio 1 and number of surrounding APs (BSSID) exceed the numbers shown in the table.

Number of Enabling VAPs	Number of Surrounding APs (BSSID)
1	120
3	95

Number of Enabling VAPs	Number of Surrounding APs (BSSID)
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 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.
- ☐ 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.
- ☐ Captive Portal is not supported.
- ☐ The value of the Inactivity Timer cannot be changed.
- ☐ IEEE802.11w(MFP) need 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

The supported countries are the same as the previous version.

Contacting Allied Telesis

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Services & Support section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- ❑ Helpdesk (Support Portal) - Log onto Allied Telesis interactive support center to search for answers to your questions in our knowledge database, check support tickets, learn about Return Merchandise Authorizations (RMAs), and contact Allied Telesis technical experts.
- ❑ Software Downloads - Download the latest software releases for your product.
- ❑ Licensing - Register and obtain your License key to activate your product.
- ❑ Product Documents - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.
- ❑ Warranty - View a list of products to see if Allied Telesis warranty applies to the product you purchased and register your warranty.
- ❑ Allied Telesis Helpdesk - Contact a support representative.

To contact a sales representative or find Allied Telesis office locations, go to **www.alliedtelesis.com/contact**.

Copyright © 2022 Allied Telesis Inc., Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis Inc., Inc. Allied Telesis Inc. and the Allied Telesis Inc. logo are trademarks of Allied Telesis Inc., Incorporated. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners. Allied Telesis Inc., Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis Inc., Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis Inc., Inc. has been advised of, known, or should have known, the possibility of such damages.