



TQ6602 Wireless Access Point Version 7.0.1-2.1 Software Release Notes

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

- “Firmware File,” next
- “New Features” on page 1
- “Enhancements” on page 2
- “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 4
- “Supported Countries” on page 5
- “Contacting Allied Telesis” on page 6

Firmware File

The firmware filename for the TQ6602 version 7.0.1-2.1 access point is:

- AT-TQ6602-7.0.1-2.1.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 7.0.1-2.1 access point:

- Captive Portal
- Re-authentication Timer

Enhancements

The following enhancements are made to the TQ6602 version 7.0.1-2.1 access point:

- ❑ Radar detection behavior
- ❑ All VLAN frames can be forwarded to WDS regardless of the WDS VAP's VLAN ID.

Specification Change

The following changes are made to the specifications in the TQ6602 version 7.0.1-2.1 access point:

- ❑ When MAC Filtering is enabled, the access point checks the MAC address in the Authentication packet instead of the MAC address of the probe request.

Resolved Issues

The following issues were resolved in Version 7.0.1-2.1 for the TQ6602 wireless access point:

- ❑ The access point might have issued an error entry, "sh: ap-bootstrap-cmd: not found," when the status of the wireless interface was switched.
- ❑ When a loop including a WDS link occurred, WDS links were not able to communicate correctly even after the configuration was changed and the loop state was resolved.
- ❑ Radio 2 might have changed the channel when the access point detected radar.
- ❑ When External RADIUS with WPA Enterprise or MAC Filtering and the Secondary RADIUS were configured, the access point was not able to save the settings of other VAPs.
- ❑ An invalid format IP address was accepted for Static IP Address, Default Gateway, and DNS Nameserver.
- ❑ Fast Roaming could not be enabled on the Web interface.
- ❑ The allow action for MAC Filtering did not function when the MAC address list was empty.
- ❑ The handover log did not include the SSID.
- ❑ A wireless client's VLAN ID was changed when IEEE802.11r roaming with Dynamic VLAN was enabled.
- ❑ Airtime Fairness might not have worked properly when enabled on both Radios 1 and 2.
- ❑ No limit was set to a dump file that was generated during the recovery process when the access point detected a microcode error.
- ❑ When the access point detected a microcode error, the recovery process was terminated due to timeout and the access point restarted.
- ❑ When the Hidden SSID was enabled, a wireless client might not have been able to reconnect to the access point when it was disconnected from the access point in the power-saving state.

- ❑ When a wireless client was repeatedly connected and disconnected while the dynamic VLAN was enabled, the wireless client might not have been able to be reconnected and a tech-support information file was not generated.
- ❑ Even when 80MHz was selected for Radio Bandwidth, the band was not used properly for some wireless clients.

Known Issues

Here are the known issues for the TQ6602 version 7.0.1-2.1 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.
- ❑ 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.
- ❑ A wireless client might be disconnected if Airtime Fairness is enabled. Allied Telesis recommends disabling Airtime Fairness when it is not used.

- ❑ When Channel Blanket is enabled, the Management VLAN supports only untagged configurations.

Limitations

Here are the limitations for the TQ6602 version 7.0.1-2.1 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
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.
- 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

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.