TQ5403e Wireless Access Point
Version 5.4.2 Software Release Notes

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

Supported Platforms

Version 5.4.2 is supported on the TQ5403e wireless access point. It is not supported on the TQ5403 and TQm5403 wireless access points.

For instructions on how to upgrade the management software on wireless access points, refer to the TQ5403 Wireless Access Points Management Software User's Guide, available on the Allied Telesis Inc. web site at **www.alliedtelesis.com/support.**

Management Software Filenames

The filename for Version 5.4.2 for the TQ5403e wireless access point is shown here:

❐ AT-TQ5403e-5.4.2.b03.img

New Features in Version 5.4.2

❐ Added Network Time Protocol (NTP) synchronization log events to the web browser interface and Autonomous Wave Controller (AWC) plug-in.

Supported Countries

The wireless access points are supported in the countries listed in Table 1. The table includes the version numbers of the first firmware releases to support the countries.

Table 1: Supported Countries

Country	TQ5403	TQm5403	TQ5403e
Australia	v5.0.0	v5.1.1	v5.3.0
Canada	v5.3.0	v5.3.0	v5.3.1
China	v5.3.1	N/A[1]	N/A
European Union	v5.0.0	v5.1.1	v5.3.0
Hong Kong	v5.1.0	v5.1.0	v5.3.1
India	v5.1.1	v5.1.1	v5.4.1
Israel	v5.4.1	N/A	N/A
Japan	v5.0.0	v5.1.1	v5.3.0
Korea	v5.2.0	v5.2.0	v5.3.1
Malaysia	v5.1.0	v5.1.0	v5.3.1
New Zealand	v5.0.0	v5.1.1	v5.3.0
Singapore	v5.1.0	v5.1.0	v5.3.1
Taiwan	v5.3.0	v5.3.0	v5.3.1
Thailand	v5.1.0	v5.1.0	v5.3.1
United States	v5.0.0	v5.1.1	v5.3.0
Vietnam	v5.2.0	v5.2.0	v5.3.1

1. Not available.

Note

The wireless access points support dynamic frequency selection (DFS) on 5GHz channels designated by countries or regions as DFS channels.

Enhancements

None.

Specification Changes

None.

Resolved Issues

The following issues were resolved in v5.4.2 for the TQ5403e wireless access point:

❑ The wireless access point did not forward traffic from wireless clients that received VLAN assignments from the OpenFlow protocol that were different from its VAP VLANs.

❑ Manager passwords that contained special characters did not work correctly with the web browser interface.

❑ Radio transmission powers set with the AWC plug-in were displayed incorrectly in the web browser interface.

❑ The access point generated unnecessary CPU interrupts that slowed traffic throughput.

Known Issues

❑ The access point does not synchronize Hostname and SNMP System Name.

❑ When IEEE802.11w Management Frame Protection is enabled, some wireless clients might not be able to reconnect after disconnecting.

❑ Channels 12 and 13 are not selected in Auto Channel Selection when the Channel parameter is set to Auto.

❑ Access points that receive their IP addresses from DHCP servers might send SNMP traps with their default IP address when reset or powered on.

❑ Wireless clients might not be able to connect to Channel Blanket VAPs when only one access point is running Channel Blankets.

❑ The access point does not always save new values for the Secondary RADIUS Server Key.

❑ The access point might increment the Received Counter for a VAP when there are no clients.

❑ An access point that is managed by AT-Vista Manager EX with AWC plug-in enters an error message in the log when you click on the Radio 1 VAP0 tab in the VAP/Security page.

❑ The access point reports as "NULL" the SSIDs of rogue access points that hide their SSIDs.

❑ The access point might fail to operate properly as an AMF Guest node, affecting these features:

- Recognition as an AMF guest node

- Backup as an AMF Guest node

- Recover as an AMF Guest node

The issue can be resolved by linking down and linking up the connection between the access point and AMF member.

❒ When rebooted, access points that receive their IP addresses from DHCP servers might initially use their default IP addresses in packets to NTP servers. This occurs when access points send NTP packets before receiving their IP addresses from DHCP servers.

❒ Access points transmit two DHCP discover packets (untagged and tagged VID 1) when the Management VLAN tag setting is disabled.

❒ Management VLAN cannot use tagged VID 1. When VID for a VAP is set to other than 1, dynamic VLAN assignment cannot use VID 1 for RADIUS packets.

❒ Changing the Duplicate AUTH Received parameter in the Advanced Settings Tab from Ignore to Disconnect requires resetting the access point to activate the change. You do not have to reset the access point after changing the setting from Disconnect to Ignore.

❒ The access point disables the inactivity timer settings for RADIUS in a VAP when you enable Channel Blanket.

❒ The access point might fail if wireless clients frequently connect and disconnect between Channel Blanket VAPs.

❒ Channel Blankets are not supported when the feature is enabled on only one access point.

❒ The Technical Support Information feature might not be successful when multiple wireless clients are connected to Channel Blanket VAPs.

❒ Channel Blankets do not support IEEE802.11w Management Frame Protection (MFP).

❒ The access point might discard broadcast packets on Channel Blanket VAPs during periods of heavy broadcast traffic.

❒ The access point might discard packets with the MAC address prefix "02:" when the OpenFlow protocol is enabled.

Operational Notes

Here are the operational notes for this release.

❒ When saving and applying wireless settings, the access point prompts wireless clients to disconnect their wireless connections, but depending on the clients, the wireless connections might be maintained. In that case, please reconnect the client again.

❒ Cannot set channels 10-13 on the 40MHz bandwidth on 2.4GHz Radio1.

❒ Do not set the Maximum Clients parameter to more than 200 with the web browser interface.

Contacting Allied Telesis

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

❒ 24/7 Online Support — Enter our interactive support center to search for answers to your product questions in our knowledge database, to check support tickets, to learn about RMAs, and to contact Allied Telesis Inc. technical experts.

❒ USA and EMEA phone support — Select the phone number that best fits your location and customer type.

❒ Hardware warranty information — Learn about Allied Telesis Inc. warranties and register your product online.

❒ Replacement Services — Submit a Return Merchandise Authorization (RMA) request via our interactive support center.

❒ Documentation — View the most recent installation and user guides, software release notes, white papers, and data sheets for your products.

❒ Software Downloads — Download the latest software releases for your managed products.

For sales or corporate information, go to **www.alliedtelesis.com/purchase** and select your region.