TQ5403 Series of Wireless Access Points
Version 5.4.1 Software Release Notes

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

Supported Platforms

Version 5.4.1 is supported on these wireless access points:

- ❒ TQ5403
- ❒ TQ5403e

Version 5.4.1 is not supported on the TQm5403 wireless access point.

For instructions on how to upgrade the management software on the wireless access points, refer to the latest version of 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 firmware filenames for Version 5.4.1 are listed here:

- ❒ AT-TQ5403-5-4.1.b02.img
- ❒ AT-TQ5403e-5.4.1.b02.img

New Features in Version 5.4.1

This release adds support for the TQ5403e Wireless Access Point in India and the TQ5403 Wireless Access Point in Israel. Refer to Table 1.

Supported Countries

The wireless access points are supported in the countries listed in Table 1. Included in the table are 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

There are no enhancements in Version 5.4.1.

Specification Changes

There are no specification changes in Version 5.4.1.

Resolved Issues

There are no resolved issues in Version 5.4.1.

Known Issues

- The access point does not synchronize Hostname and SNMP System Name.
- If 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.
- The Access point that receives their IP addresses from a DHCP server might send SNMP traps with the default IP address when the access points are reset or powered on.
- Wireless clients might not be able to connect to a Channel Blanket VAP if only one access point is running Channel Blankets.
- When the Secondary RADIUS Server Key is entered, the access point might not save the entered key and save the field as empty.
- The access point might increment the Received Counter for a VAP even 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 the SSIDs of rogue access points as “NULL” when the rogue access points 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 their 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 used VID 1 for RADIUS packets.
- You must reset the access point after changing the Duplicate AUTH Received parameter in the Advanced Settings Tab from Ignore to Disconnect, to activate the change. You do not have to reset the access point after changing the setting from Disconnect to Ignore.
- Configuration changes for a radio is void if the changes are made after the status of the radio became Out Of Channels (OCC) because radar signals were detected.

The following issues are applied only to the TQ5403 and TQ5403e access points:

- When the VAP is with Channel Blanket enabled, the inactivity timer settings for RADIUS is disabled.
- The access point might fail when wireless clients frequently connect and disconnect among Channel Blanket VAPs.
- When there is only one access point with Channel Blanket enabled, wireless clients are not able to correctly communicate through Channel Blanket VAPs.
- You might fail to collect Technical Support Information if multiple wireless clients connect to the Channel Blanket VAP.

Operational Notes

Here are the operational notes for this release.

- When saving and applying the 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 when use 40MHz bandwidth on 2.4GHz Radio1.
- Do not set the Maximum Clients parameter to more than 200 with the web browser interface.

Histories

New Features History

Version 5.4.0 New Features

Here are new features in this release.

- The Delivery Traffic Indication Message (DTIM) period can be set from Settings > VAP/Security > Advanced Settings page or by Vista Manager EX v.3.1.0 or later.

- The DTIM period for Channel Blanket can be set by Vista Manager EX, but not from the access point's Web Interface.
- The value of the RSSI threshold for beacon is synchronized with the value on Vista Manager EX v.3.1.0 or later.

Version 5.3.1 New Features

Here are new features in this release.

- The VAP/Security window in the web browser interface has a new Advanced Settings tab.
- The Inactivity Timer, Duplicate AUTH Received, and Association Advertisement fields in the Advanced Settings are supported in AT-Vista Manager EX v3.0.2 and the AWC plug-in.
- The access points with version 5.3.1 can be managed with AT-VIST Manager EX v2.5.x or v3.0.x.

Version 5.3.0 New Features

Here are new features in this release.

- Support for TQ5403e wireless access point
- Captive portals
- Association advertisements
- Intrusion Detection System (Requires the AWC plug-in.)

Note
You can configure captive portals with the web browser interface or AT-Vista Manager EX v3.0.x and the AWC plug-in.

Note
Version 5.3.0 requires AT-Vista Manager EX v3.0.x

Version 5.2.5 New Features

Here are no new features in this release.

Note
Version 5.2.5 requires AT-Vista Manager EX v2.5.x or v3.0.x.

Version 5.2.0 New Features

Here are new features in this release.

- Adds support for the TQ5403e access point.

- Adds WEP for 64 bit (ACSII, HEX) and 128 bit (HEX) to on-board web interface and AWC plug-in.
- Adds External RADIUS authentication to MAC filter to on-board web interface and AWC plug-in.
- Adds WMM/ APSD to on-board web interface and AWC plug-in.

Here are enhancements to his release:

- Adds FCC dynamic frequency selection (DFS).
- Allows the access point to obtain its host name from a DHCP server.
- Allows the Hidden SSID function to be changed when band steering is enabled.
- Adds syslog when maximum wireless clients are exceeded.
- Allows the access point to send client IP addresses and traffic counters to the AWC plug-in.

Version 5.1.1 New Features

None.

Version 5.1.0 New Features

Here are the new features in this release.

- Support for the AWC-CB function (AT-Vista Manager EX v2.4.1 with AWC Plug-in Management)
- Support for the Band-steering function
- Support for IEEE802.11r Fast Roaming using WPA-ENT
- Support for the Timezone and Daylight Saving setting. These settings can be set from “Settings > System > Time” page including “Timezone” and a check box for “Enable Daylight saving”
- Support for Internet Explorer 11 with "Compatibility View"
- Support for Link Aggregation
- Support for enabling/disabling Reset Button
- Support for IEEE 802.11r PMK-R0 Lifetime function
- Support Private MIB

Enhancements History

Version 5.3.0 Enhancements

- The Virtual Access Point tab has a new Inactivity Timeout parameter. The parameter is used to control how long wireless access points permit inactive wireless clients to remain associated.

Version 5.2.5 Enhancements

There are no enhancements for Version 5.2.5.

Version 5.1.1 Enhancements

- The maximum number of wireless client connections for Channel Blanket VAP has been extended from "200" to "500". When the AT-Vista Manager EX AWC Plug-in manages AP with Channel Blanket configuration, the number of maximum client of Radio interface which is enabling Channel Blanket is now “500”.

Specification Upgrades History

Version 5.4.0 Specification Upgrades

This release adds the following specification change:

- The channel selection method for DFS detection is changed. When a radar signal is detected, DFS assigns a channel from the auto channel selection regardless of whether the channel is set to auto or static channel.

Version 5.3.0 Specification Upgrades

TQ5403 and TQm5403 access points with v5.3.0 add models for Taiwan and Canada. Please note the following concerning these new models:

- You cannot change their Country setting.
- V5.3.0 observes the new Taiwan regulations regarding wireless access points.
- An access point with Taiwan selected as the Country setting retains that setting when upgrade.
- You cannot downgrade them to earlier firmware versions.

Version 5.2.5 Specification Upgrades

There are no specification changes for Version 5.2.5.

Version 5.1.0 Specification Upgrades

- The frames from wireless STA are sent as untagged if management VLAN tag enabled, management VID sets without 1, and the following conditions:
  - VLAN ID of VAP is set to “1”
  - Assigned VID 1 by dynamic VLAN
- After firmware upgraded, the configuration applied when AP is managed by AT-Vista Manager EX AWC Plug-in at first time
- Changed file format to zip when acquiring Technical Support Information from AT-Vista Manager EX AWC Plug-in
- Changed minimum Tx Power from 10% to 1%
- Changed the behavior of session timeout of Web-UI.
  - Web-UI moves to login page if session timeout.
  - Web-UI redirects to the page before session timeout when re-login after session timeout

Resolved Issues History

Version 5.4.0 Resolved Issues

- Communications became unstable when a new access point joined in the Channel Blanket environment. This issue is fixed.
- When Vista Manager EX set the access point's transmission power to other than Max or Min, the actual transmission power of the access point decreased by 0.5dBm once Neighbor Management AP Detection was performed. This issued is fixed.
- The access point's throughput rate decreased significantly when the access point was in the Channel Blanket environment. This issue is fixed.
- Wireless clients consumed the batteries faster in Channel Blanket than out of Channel Blanket. This issue is fixed.
- An iPhone and iPad didn't resume communications after the connected access point rebooted when the access point was with IEEE802.11w(MFP) enabled and in Channel Blanket. This issue is fixed.
- When the Security Mode is None or WPA2, even though the Duplicate AUTH Received is set to Ignore, the access point behaved as it was set to Disconnect. This issue is fixed.
- Even though a wireless client was removed from the old access point's association list when the wireless client was handed over to another access point, the wireless client still received broadcast frames from other than the new access point. This issue is fixed.
- After the access point connected and disconnected repeatedly to a WDS, it failed to reconnect to the WDS. This issue is fixed.
- After a VoIP client was handed over to another access point, the VoIP's first call failed. This issue is fixed.
- If a list of Neighbor AP exceeded 200 access points, the snmpd daemon failed when an snmpget request for the MIB Object of Neighbor AP was received, This issue is fixed.
- When the access pint is with Dynamic VLAN enabled, a wireless client connected to the access point was not able to get an IP address from DHCP server. This issue is fixed.
- The default channel lists for the four countries were fixed as follow:
  - Panama (PA): 1~11, 36~64, 149~165
  - El Salvador (SV): 1~13, 36~64, 149~165
  - Uruguay (UY): 1~13, 36~64, 149~165
  - Venezuela (VE): 1~13, 36~64, 149~165
- The access point's kernel failed to operate when the access point with Neighbor AP Detection enabled or Neighbor Managed AP detection enabled was managed by Vista Manager EX. This issue is fixed.
- The access point's kernel failed to operate when the access point handled errors of the frames received from another access point in the Channel Blanket environment. This issue is fixed.

Version 5.3.0 Resolved Issues

The following resolved issues apply to the TQ5403 and TQm5403 access points.

- The MAC filtering feature did not work properly with the band steering feature.
- The access point sent incorrect RSSI values to the AWC plug-in.
- The Session Timeout value in the Web window did not work correctly.
- The access point sent inaccurate connection times of wireless clients to the AWC plug-in.
- The access point accepted invalid IP addresses in the web management windows.
- The access point damaged its configuration file if it lost power during boot-up.
- The NTP client periodically failed to work correctly if the access point received its IP address configuration from a DHCP server.
- Disabling a radio could cause the access point to stop forwarding traffic on all radios.

Version 5.2.5 Resolved Issues

The following resolved issues apply to the TQ5403 and TQm5403 access points.

- If the channel blanket feature was enabled, access points transmitted broadcast frames even when no wireless clients were connected.
- The Auto Channel Selection option in the Basic Settings window did not work correctly.
- Access points periodically disconnected from the AWC plug-in or stop forwarding traffic when re-applying their configurations from the plug-in.
- The TQm5403 access point generated incomplete or corrupted backup configuration files.

Version 5.2.0 Resolved Issues

The following resolved issues apply to both the TQ5403 and TQm5403 access points.

- Access point output connected log when the number of connected clients exceeds client value.
- Radio interfaces did not work correctly when all radios were enabled and Neighbor AP Detection feature was enabled on all radios.
- Neighbor AP Detection feature failed at access point boot-up with large configuration.
- Access point sends Link trap when trap is disabled.
- Access point failed to use primary RADIUS server when both primary and secondary servers are defined.
- Wireless clients cannot reconnect using PMKSA cache when Dynamic VLAN is enabled.
- Failed to get wireless client information via SNMP-MIB when many wireless clients are connected to access point.

The following resolved issues apply to the TQ5403 access point.

- The access point notifies wireless client information as connected client to the AWC plug-in when the number of connected clients exceeds maximum clients value on channel blanket VAP.
- The traffic counter did not count correctly when channel blanket VAP is enabled.
- Duplicate BSSID is displayed on Radio1 VAP page when channel blanket is enabled.
- Access point sends unnecessary logs when wireless clients connect and disconnect from channel blanket VAP.
- Access point notifies wireless clients information as connected to AWC plug-in when access point rejects connecting wireless clients by MAC filter on channel blanket VAP.
- Access point sometimes stopped functioning when channel blanket feature is enabled.
- Access point sometimes provided incorrect information about channel blanket to AWC plug-in.

Version 5.1.1 Resolved Issues

- In Monitoring > Statistics page, counters of "Packets Received" and "Bytes Received" of VAP always show zero. This is issue is resolved.
- When Management VLAN Tag is enabled and Management VLAN ID is set to “1”, AP can not establish Channel Blanket. This is issue is resolved.
- AP output the RADIUS accounting log when the wireless client connects to VAP which is not set WPA-Enterprise setting. This is issue is resolved.
- LAN interface does not launch after restore v5.0.0/v5.0.1 version’s configuration. This is issue is resolved.
- AP disconnects connected clients when getting Technical Support Information. This is issue is resolved.

Version 5.1.0 Resolved Issues

- The multicast rate limit was not applied to the broadcast frame.
- AP can not specify a subnet to allow communication for SNMP.
- In Monitoring > Status > Radio page, "Transmission Power" is not displayed correctly when under AT-Vista Manager Ex AWC Plug-in management.
- DNS server is incorrect set when more than one DNS Server is set in the lease information of the DHCP server.
- AP can not name resolution for NTP server, if input length of FQDN is 176 or more characters.
- Even if "Interval to Synchronize" time comes after failing name resolution for NTP server, AP does not send query again.
- AP which is “Connection Type: DHCP” always send DHCP discover packet when changing configuration.
- The specification of Mobility Domain for IEEE802.11r is more than four characters, but it can be set up three or less characters from Web-UI.
- When SNMP trap is enable, in boot up delay for 30 seconds until it becomes under Vista Manager management

- Multicast TX Rate "5.5" setting is not applied correctly from AT-Vista Manager EX AWC Plug-in.
- Legacy Rate setting is not applied correctly from AT-Vista Manager EX AWC Plug-in.
- When Bandwidth setting was set to 40 MHz, AP can not set 116 ch.
- When AT-Vista Manager EX AWC Plug-in applied a configuration which is large size to the AP, AP sometimes left from AT-Vista Manager EX AWC Plug-in.
- When Radio 2 is set to Bandwidth 80 MHz with some VAPs enable, Bandwidth of Radio 2 become 20 MHz.
- AP does not transmit specific IP multicast packets to wireless client from Ethernet port.
- In the IP address setting page, the fourth octet couldn't set "0" and "255".
- In Monitoring > Neighbor AP page, Security was not displayed correctly.
- When the AP was under the management of the AT-Vista Manager EX AWC Plug-in, the AWC management process of AP is restarted.
- Even if AP receives DHCP NAC, AP does not send DHCP discovery.
- AP occurs memory-leak when some wireless clients frequently connect and disconnect to VAP which is enabled Dynamic VLAN.
- AP displays the security of the detected AP which is setting by WEP as "None" on Neighbor AP page.
- AP can not name resolution for SNMP server, if input length of FQDN is 176 or more characters.
- When Management VLAN of AP is enabled, AT-Vista Manager EX AWC Plug-in failed to apply configuration to AP.
- Secondary RADIUS setting is not able to disable from AT-Vista Manager EX AWC Plug-in.
- AP can not be re-managed by AWC Plug-in if all Radio interfaces are disabled setting.

Initial Release: Firmware: 5.0.0 B11

The following issues are included in V5.0.0:

- Support for AT-Vista Manager EX v2.4.0 with AWC Plug-in Management is included.
- Channel blanket is not supported.

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.