# TQ5403 Series Wireless Access Point
# Version 6.0.4-0.2 Software Release Notes

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

## Supported Platforms

The following access points support version 6.0.4-0.2:

- AT-TQ5403
- AT-TQm5403
- AT-TQ5403e

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

The version 6.0.4-0.2 firmware filenames are listed here:

- AT-TQ5403-6.0.4-0.2.img.zip
- AT-TQm5403-6.0.4-0.2.img.zip
- AT-TQ5403e-6.0.4-0.2.img.zip

## New Features

- ❒ Support for verifying RADIUS packets. This feature prevents RADIUS protocol forgery attacks and is available in Settings > VAP/Security on the following pages:

  Settings > VAP/Security >

  - Security >Mode: WPA Enterprise

  MAC Access Control > MAC Access Control:

  - External RADIUS
  - MAC Address List + External RADIUS

  Captive Portal > Captive Portal:

  - External RADIUS
  - External Page Redirect

  If you are using a local RADIUS server on an AlliedWare Plus router or switch, the AlliedWare Plus device must be running version 5.5.4-2.1 or later.

## Resolved Issues

The following applies to all three models:

- ❒ During a firmware update, messages would be displayed in English when the language was set to Japanese.
- ❒ 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.
- ❒ When applying Web-GUI settings, invalid numeric entries, such as beginning with a "0" and decimals, were allowed to be saved & applied instead of rejected.
- ❒ The access point occasionally reboots when a large number of log files were output.
- ❒ When Neighbor AP Detection was enabled, unnecessary logs would be output.
- ❒ When accessing a neighbor AP list with a private MIB, an SNMP process would sometimes restart.
- ❒ When a wireless client was being authenticated through PMK (Pairwise Master Key), re-authentication would not occur even when the time set in the RADIUS session timeout attribute was reached.
- ❒ After initially authenticating using PMK, if PMK timed out and the device reauthenticated using RADIUS, the log would show it was reauthenticated using PMK.
- ❒ After initially authenticating using PMK, if the session timed out and the device was reauthenticated using RADIUS, the log would show it was reauthenticated using PMK.
- ❒ If a wireless client sent multiple PMKIDs during 4-way handshakes when connecting, the connection would sometimes fail.
- ❒ The Proxy ARP feature stopped when one wireless client would send NeighborSolicitation frames with 8 different IPv6 address.

- With Vista Manager EX v3.12.X or later, when an AP Profile with security WEP and Key Type "ASCII" was applied, the radio wave output of the access point would stop and wireless clients would be disconnected.
- When the Captive Portal page was viewed over HTTPS, the Captive Portal page would sometimes become inaccessible.
- A firmware upgrade would sometimes fail if Application Proxy had been configured on more than one VAP.

  NOTE:

  - If upgrading from v6.0.3-0.2 (or older) to v6.0.4-0.2, a reboot may occur and the upgrade will fail. Therefore, disable all configured AMF Application Proxy before beginning the upgrade. (This issue will not occur if changing version from v6.0.4-0.2 to any other version).
- When specifying an encryption key to download a Technical Support file, sometimes the retrieval would fail.
- Depending on the switch the access point was connected to, packet loss and throughput decrease could be observed.
- A reboot could be observed when a device was roaming between different wireless interfaces within the same access point.

The following list applies to Channel Blanket (AWC-CB) and/or Smart Connect (AWC-SC) on the TQ5403 and TQ5403e models:

- With AWC-SC enabled, the Security tab would not appear when accessing the SSID "sc-initial-provisioning" VAP in the VAP/Security Settings page on the AP’s GUI.

## Limitations

Here is the list of limitations for the TQ5403 Series Access Points version 6.0.4-0.2 management software:

- OpenFlow is not supported.
- When saving and applying settings, the access point prompts wireless clients to disconnect; however, connection with some clients might not be disconnected. In the case, disconnect and connect the clients again.
- 10 to 13 channels cannot be selected on the 40MHz bandwidth on 2.4GHz Radio1.
- The maximum number of clients is up to 200 when the value is set on the web interface.
- Do not use the 172.31.0.1/24 IP address when AWC-SC auto discovery is used.
- Do not use other VAPs on the same radio if using AWC-SC.
- The root access point and satellite access points must have the same VID settings for the client service when using AWC-SC.
- AWC-SC cannot use with AMF guest node.
- A switch must not use DHCP Snooping on the access point that is connected to a network if using AWC-SC.

- The WPA3-personal or WPA3+WPA2-personal setting is not applied correctly to VAP0 using AWC. In this case, use other VAPs.

## Limitations on Channel Blanket

Here are the list of limitations on Channel Blanket in the version 6.0.4-0.2 management software:

- Band Steer is not supported with Channel Blanket.
- All access points in Channel Blanket must have the same Radio settings.

### When Channel Blanket Radio is Enabled

- Changing the RTS threshold is not supported.
- Airtime Fairness is not supported.

### When Channel Blanket VAP is Enabled

- Changing the Broadcast Key Refresh Rate is not supported.
- RADIUS Accounting is not supported.
- Fast Roaming is not supported.
- Pre-authentication is automatically disabled.
- Dynamic VLAN is automatically disabled.
- The Session-Timeout RADIUS attribute is automatically disabled.
- Captive Portal is automatically disabled.
- Changing the Inactivity Timer value is not supported.

### Channel Blanket Settings

- The Management VLAN ID and Control VLAN ID cannot be the same.
- The VAP VLAN ID and Control VLAN ID cannot be the same.

### Wireless Clients’ Behavior on Channel Blanket

- Communications of wireless clients are interrupted when the access point is turned off or reboots. It takes approximately two minutes for the wireless clients connected to the access point that was turned off or rebooted to restore communications.

## Specifications and Limitations on Easy Setup

Here is a list of specifications and limitations for Easy Setup:

- When the VAP mode is set to Cell Type, the Radio and VAP0 settings must be configured as follows:
    - Radio1 setting

      Basic Settings > Mode: IEEE802.11b/g/n
    - Radio2 setting

Basic Settings > Mode: IEEE802.11a/n/ac

- Radio1/Radio2 VAP0 settings

  Security > Mode: WPA Personal

  Security > WPA Version: WPA2 and WPA3

  Security > Cipher Suites: CCMP

  Security > IEEE802.11w (MFP): Enabled

❒ When the VAP mode is set to Single Channel, the Radio and VAP0 settings must be configured as follows:

- Radio2 setting

  Basic Settings > Mode: IEEE802.11a/n/ac

  Advanced Settings > Maximum Client: 500

- Radio1/Radio2 VAP0 settings

  Basic Settings > Security Mode: WPA Personal

  Basic Settings > Security WPA Version: WPA2

  Basic Settings > Security Cipher Suites: CCMP

  Basic Settings > IEEE802.11w (MFP): Disabled

  Advanced Settings > Association Advertisement: Enabled

❒ Single Channel can be selected only when AWC-SCL Cluster is enabled.

❒ The Control Frame setting in the Single Channel mode is automatically changed based on the Management VLAN Tag settings of the access point.

- Management VLAN is disabled: Control Frame setting is changed to untagged frame.
- Management VLAN is enabled: Control Frame setting is changed to tagged frame, which is the same as the Management VLAN ID.

## Specifications and Limitations on AWC-SCL Cluster

Here is a list of specifications and operational notes for AWC-SCL Cluster:

❒ The access points in AWC-SCL share the configuration except:

- Host Name
- MAC address
- IP address settings
- SNMP system name, system contact, and system Location
- Transmission power when VAP0 mode is set to the Single Channel Type.

❒ The maximum number of AWC-SCL members is five.

❒ The access points in AWC-SCL cannot be managed by Vista Manager EX or Vista Manager mini.

❒ When the access point in AWC-SCL and the Single Channel type is added to AWC-SCL as a device replacement, the configuration re-apply process automatically runs if the access point has the largest MAC address among the cluster members. As a result, the wireless clients that had been connected to the access point are all disconnected.

## Limitation on the Access Point Setting using Easy Setup

- Setting using both Easy Setup and Vista Manager EX is not supported.

## Limitations on the Access Point Setting using Single Channel Type

- Changing the Radio settings is not supported.

  When the Radio settings are not default values, change the settings to default before setting the Single Channel Type.

- Changing Radio2 VAP0 setting is not supported on “Settings > VAP/Security” page.

  When the Radio2 VAP0 settings are not default values, change the settings to default before setting the Single Channel Type; however, the parameters described in the specifications are executed.

- The access points with the same “Single Channel group ID” on different networks in near wireless spatial are not supported.
- Setting to management VLAN ID and Control VLAN ID 1 is not supported.
- More than seven access points in the Single Channel Mode is not supported.

  Establishing a Single Channel with more than seven access points is possible, but not supported.

- The largest MAC address among AWC-SCL cluster’s members is assigned to VAP’s BSSID of the Single Channel Type.

## Known Issues

- Access points do not synchronize the Hostname and the SNMP System Name.
- On the Maintenance > Support Page of the Web UI, in the Technical Support Information section, a note states that the 801.1x authentication log contains the user ID and does not contain the password. In fact, neither the user ID nor the password is included.
- The access point might save the Secondary RADIUS Server Key value as empty.
- Access points might disconnect clients several seconds before the expiration of the Inactivity Timer.
- Do not use the Associated Client window in the web browser interface to disconnect clients on Wireless Distribution System (WDS) children.
- In rare instances, the hardware and software tables may develop inconsistencies that can cause access points to reset. This is entered in the log as “kernel: Rebooting due to DMA error recovery.”
- The SNMPv3 traps EngineBoot and EngineTime are always sent with a value of 0.
- Wireless clients might not be able to immediately reconnect after disconnecting when IEEE802.11w Management Frame Protection (MFP) is enabled.
- For some wireless clients, roaming may be slower than expected if IEEE802.11w Management Frame Protection (MFP) is enabled.

- Do not set the Maximum Clients parameter in the web browser interface to more than 200 clients on the TQ5403 or TQ5403e access point, or 127 clients on the TQm5403 access point.
- Channels 12 and 13 are not activated in Auto Channel Selection when the Channel parameter is set to Auto.
- Access points that receive their IP addresses from DHCP servers might initially use the default IP address in SNMP traps and NTP requests when booted. This occurs when access points send SNMP and NTP packets before receiving their IP addresses from DHCP servers.
- Access points might increment the VAP Received Counter when there are no clients.
- Access points might not always operate properly as AMF Guest nodes, 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 connections between access points and AMF members.
- Access points might transmit unnecessary packets from their radios when initializing the management software during boot up.
- When booted, access points transmit two DHCP discover packets (untagged and tagged VID 1) when the Management VLAN tag setting is disabled.
- The 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.
- Access points managed with the AWC plug-in might take one to two minutes to save their configurations.
- In rare instances, the access point managed with the AWC plug-in might not be able to save their configurations, in which case Vista Manager EX displays an error message. Saving the configuration again is usually successful.
- When the OSU icon is set via AWC with Vista Manger mini, some parameters in the access point configuration are saved with unintended values.
- A wireless client with IPv6 Router Advertisement does not communicate on Dynamic VLAN VAP.
- MAC Access Control does not work when Distributing System is enabled on IEEE802.11r.
- If you select Hidden SSID, you cannot use the following features with fast roaming:
  - IEEE802.11k (Neighbor Reports)
  - IEEE802.11v (BSS Transition Management Frames).

The following list applies to Channel Blanket (AWC-CB) and/or Smart Connect (AWC-SC) on the TQ5403 and TQ5403e models:

- The RADIUS attribute “Session-timeout” must be disabled in VAPs with Channel Blanket.

- The access point might restart when wireless clients connect and disconnect repeatedly between Channel Blanket VAPs.
- When only one access point with Channel Blanket enabled is up and running, wireless clients are not able to communicate with the Channel Blanket VAP correctly.
- The access point might not generate technical support information when a significant number of wireless clients connect to Channel Blanket VAP.
- IEEE802.11w (MFP) should be disabled on access points using Channel Blanket.
- The access point might issue an unnecessary log message of “Removing STA due to association advertisement” when a wireless client is connected to the access point.

## Supported Countries

The TQ5403, TQm5403, and TQ5403e wireless access points are supported in the countries listed in Table 1. The table includes the firmware versions that initially supported the countries.

Table 1: Supported Countries for the TQ5403, TQm5403, and TQ5403e Wireless Access Points

| 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.

## Contacting Allied Telesis

If you need assistance with this product, visit the Allied Telesis web site at **www.alliedteelsis.com/support.**