TQ5403 Series Wireless Access Point
Version 6.0.3-0.1 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 6.0.3-0.1:

- 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 6.0.3-0.1 firmware filenames are listed here:

- AT-TQ5403-6.0.3-0.1.img.zip
- AT-TQm5403-6.0.3-0.1.img.zip
- AT-TQ5403e-6.0.3-0.1.img.zip

New Features

- Autonomous Management Framework (AMF) Auto-recovery

  This feature is available with Alliedware Plus Operating System version 5.5.3-0.1 AMF Guest Node feature. For more information, see *Alliedware Plus Feature Overview and Configuration Guide* on the Allied Telesis website.

- Redirect URL for AMF Application Proxy

  This feature is available only when configured from Vista manger EX. For more information, see Vista Manager EX and AMF-SEC documents on the Allied Telesis website.

- Client Isolation for each VAP
- Two-step auth fro MAC Access Control and Captive Portal

  This feature can be enabled when Captive Portal is enabled.

Enhancements

- The following data to notify to Vista Manager EX are added:
  - The access point's wireless utilization
  - RX rates of associated wireless clients
  - The access point's CPU utilization
  - Usernames of WPA Enterprise Authentication
  - Wireless interface name when a duplicate auth happens
- The access point supports wireless terminals with fixed IP addresses on Proxy ARP-enabled VAP.
- The access point supports the client statistics counter for the Channel Blanket VAP.

  The client statistics counter can be displayed on the floor MAP page of Vista Manager EX.

- Reject log entries are added for MAC Address Control.
  - When authentication is rejected by the MAC Address List or External RADIUS:

    `hostapd: athX: reject STA yy:yy:yy:yy:yy:yy due to MAC Authentication`
  - When authentication is rejected by AMF Application Proxy (AMF-SEC):

    `hostapd: athX: reject STA yy:yy:yy:yy:yy:yy due to Application Proxy`
- The Passpoint Web Management Interface is improved.
- 3DES Cipher Suites is removed from TLSv1.2 so that administrators cannot access Web Management Interface with 3DES.

Resolved Issues

The following list is applied to all three models:

- Vista Manager EX might have indicated a config application failure when applying a configuration to the access point.
- Wireless clients were not able to re-connect to the access point sometimes after they repeated connecting and disconnecting without Captive Portal authentication on a Captive Portal-enabled VAP.
- SNMP username and password were able to be set as empty when SNMPv3 was selected.
- The access point issued a connection success log on a connection failure event when a wireless client executed duplicate auth on MFP-enabled VAP.
- Users were able to retrieve SNMP MIB objects using an invalid communication name.
- The access point unnecessarily issued the following log message when rebooting or changing setting.

  ```
  daemon.err uhttpd[XXXX]: bind(): Address in use
  ```

- Neighbor AP Detection timing was sometimes off by 1 minute.
- Captive Portal did not function correctly when the session-timeout was set to 0 and the access point was managed by Vista Manager EX.
- The access point might not have issued syslog messages.
- A space was added at the end of SSID in association/disassociation logs.
- The access point issued a VLAN 0 assigned log when AMF-Security assigned No VLAN to a wireless client.
- An extra “.0” was added to the OID of an SNMPv3 trap, which the access point sent.
- A user password might have been lost when the user tried to access the Web interface of the access point while the settings of the access point were changed from Autonomous Wave Control (AWC).
- An error message was displayed on the Web Interface of the access point when the settings of Radio 3 were changed.
- The access point did not issue a timeout log message even when a RADIUS request of MAC Authentication was time out if only primary RADIUS server was registered.
- Client isolation did not function when Proxy ARP was enabled.

The following list is applied to the TQ5403 and TQ5403e models:

- The access point unnecessarily issued the following log when a wireless client connects to Channel Blanket VAP.

  ```
  Removing STA due to association advertisement
  ```

- Handing over was sometimes not done successfully when a wireless client was moved to the power saving mode.
- The TKIP settings was not displayed on the VAP Security page when Channel Blanket and TKIP were both enabled.

- The access point sometimes tried to get an IP address from DHCP with an invalid MAC address when Channel Blanket was enabled on the access point.
- Some Channel Blanket-enabled access points sent a Block Ack frame to a wireless client.
- Channel Blanket-enabled access points sometimes stopped to send beacons and rebooted automatically when the wireless chip detected an error.
- Channel Blanket-enabled access points sometimes issued a wireless client disassoc log even when the wireless client was not disconnected.
- The power value that the access point requested to the PoE switch with LLLDP was different from the max power consumption of the PoE power specification.

Limitation

Here is the limitation for the TQ5403 Series Access Points version 6.0.3-0.1 management software:

- OpenFlow is not supported. (TQ5403 and TQ5403e)
- 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 limitations on Channel Blanket version 6.0.3-0.1 management software:

- Band Steer is not supported with Channel Blanket.
- Neighbor AP Detection is not supported with Channel Blanket.
- Changing the setting of Duplicate AUTH received is not supported.
- Changing the Proxy ARP setting is not supported.
- All radios 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 settings are not supported.
- The VAP VLAN ID and Control VLAN ID settings are not supported.

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 VALN 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 Management VALN 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 Manage 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 Hostname and SNMP System Name.
- 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 save the Secondary RADIUS Server Key value as empty.
- Access points might disconnect inactive 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.”
- When Dynamic VLAN is enabled, the access pint returns a wrong value to the OID: 1.3.1.2.1.17.4.3.1.1 (MAC address information) request.
- The access point in Single Chanel mode generated extraneous “Removing STA due to association advertisements” event messages in the system log. (TQ5403 and TQ5403e only)

- When a wireless client re-connects to Single Channel VAP using PMK cache, the access point might issue a connection log message including RADIUS Server IP address. (TQ5403 and TQ5403e only)
- The access point might issue an unnecessary log message: Removing STA due to association advertisement when a wireless client is connected to the access point. (TQ5403 and TQ5403e only)
- Wireless clients might not be able to immediately reconnect after disconnecting when 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 boots.
- When booted, 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 manually booting the access point to activate the change. You do not need to boot the access point when changing the setting from Disconnect to Ignore.
- 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.

- The RADIUS attribute “Session-timeout” must be disabled in VAPs with Channel Blanket. (TQ5403 and TQ5403e only)
- The access point might shut down when wireless clients connect and disconnect repeatedly between Channel Blanket VAPs. (TQ5403 and TQ5403e only)
- The access point might not generate technical support information when a significant number of wireless clients connect to Channel Blanket VAP. (TQ5403 and TQ5403e only)
- IEEE802.11w (MFP) should be disabled on access points using Channel Blanket. (TQ5403 and TQ5403e only)
- In rare cases, the wireless module stops responding. When detecting the module with no responding, the access point restarts itself. (TQ5403 and TQ5403e only)
- The access point reboots when detecting an invalid behavior the wireless chip. (TQ5403 and TQ5403e only)
- The satellite access point takes 2 or 3 minutes to reconnect AWC-SC when detecting an error on the wireless chip. (TQ5403 and TQ5403e only)
- 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.

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.alliedtelesis.com/support.**