TQ6403 GEN2 Wireless Access Points
Version 9.0.5-0.1 Software Release Notes

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

Supported Platforms

The following access points supports version 9.0.5-0.1:

- TQ6403 GEN2
- TQm6403 GEN2

The firmware filenames are:

- AT-TQ6403GEN2-9.0.5-0.1.img
- AT-TQm6403GEN2-9.0.5-0.1.img

For instructions on how to upgrade the management software on the TQ6403 GEN2 wireless access points, see the *TQ6403 GEN2 Access Points Installation Guide* at **www.alliedtelesis.com/library.**

Specifications for Easy Setup

Here are the specifications for Easy Setup:

Note
This section only applies to the TQm6403 GEN2 access point.

- Default Radio configuration depends upon regions:
  - Japan, United States, Canada, and Taiwan: All Radios are enabled.
  - All other countries: All Radios are disabled.
- The default settings of VAP0 on Radio1, Radio2, and Radio3 are:
  - VAP/Security > Security > Mode: WPA Personal
  - VAP/Security > Security > WPA Version: WPA2 and WPA3
  - VAP/Security > Security > Cipher Suites: CCMP
  - VAP/Security > Security > IEEE802.11w (MFP): Enabled

New Features

Version 9.0.5-0.1 for the TQ6403 GEN2 and TQm6403 GEN2 wireless access points added support for the following new features:

- Support for allowing different MAC Address lists to be set for each VAP.
  - Create Multiple MAC address lists from the Settings > MAC Address List page.
  - Select MAC address lists for each VAP on the Settings > VAP/Security >MAC Access Control page.
- Register up to a total of 3072 wireless clients from the Settings > MAC Address List page.
- Support for 'Transmit unlearned ARP packet'. Enable this on the Settings > VAP/Security page, when Proxy ARP is enabled.
- Support for 'Client Packet Analysis' with AWC plugin for Vista Manager EX.

  When enabled on the plugin, the AP will share logs containing wireless client information such as when the following has occurred:
  - a DHCP Discovery packet has been sent.
  - a DHCP Acknowledge packet has been sent.
  - an IP address has been received via DHCP.
  - an ARP resolution has been completed with the default gateway.
  - a DNS resolution with the DNS server has been completed.

  Note:
  - This function applies only when a wireless client has received an IP address from DHCP.
  - This function does not apply when the wireless client uses fixed IP addresses.
  - This function is not supported for Channel Blanket VAPs.

When enabled, the following wireless information will be sent from the AP to the AWC plugin:

- OS name
- Host name

- ❒ Support for sharing the following wireless client information with the wireless LAN controller:
  - VLAN ID
  - Security
  - WPA version
  - Channel noise
  - SNR (Signal-to-Noise Ratio)

Specification Changes

Here are the specification changes for version 9.0.5-0.1:

- ❒ When Band Steering is enabled, IEEE802.11v and IEEE802.11k are forcibly enabled on all VAPs. There will not be any visible change of settings in the configuration.
- ❒ Changes to the following log outputs:

  1. When a connection is rejected by the MAC access control function, the reason for the rejection is added to the end of the log. The reasons for the rejection are displayed as one of the following:
     - Allow List
     - Deny List
     - RADIUS
     - Allow List + RADIUS
     - Deny List + RADIUS
  2. When a wireless client is connected, the VLAN ID it is assigned to is added to the log output.

Resolved Issues

Here are the resolved issues for version 9.0.5-0.1:

- ❒ [AWC-CB] When both Dynamic VLAN and IEEE802.1r fast-roaming were enabled, a Dynamic VLAN user may have been disconnected from the AP.
- ❒ During MAC Authentication, an AP would sometimes send a RADIUS Request packet with an incorrect NAS-IP-Address attribute.
- ❒ [AWC-CB] Beacon sequence numbers sent by APs were not synchronized.
- ❒ When an AP received an IP address from DHCP server, an unnecessary "Start HTTP service" log would be displayed on the console.
- ❒ When specifying an encryption key to download a Technical Support file, sometimes the retrieval would fail.

- [AWC-CB] When a wireless client tried to reconnect to an AP, the AP would incorrectly detect an issue and start the recovery operation.
- Band Steering would stop working when updates to the steering candidate list failed.
- When the mode was set to IEEE 802.11b/g/n and the bandwidth set to 40Mhz on Radio 1, 1Mbps could not be disabled from the Legacy Rate Set.
- When a wireless client was connecting to an AP, band steering would be performed unintentionally before the connection was completed. This would result in Band Steering (using IEEE802.11v) not functioning for a while.
- [AWC-CB] When a wireless client attempted to connect to an AP while the AP is applying a configuration, occasionally the AP would reboot.
- When Vista Manager mini was used to apply a Passpoint OSU icon file, the process would not finish and the AP configuration would not be completed.
- When Neighbor AP detection is changed from 'Enabled' to 'Disabled', the Neighbor AP list would not be cleared.
- When upgrading from v9.0.4-0.1 or earlier to v9.0.4-1.1, v9.0.4-2.1 or v9.0.4-0.1, the LAN2 port would not link up.
- When Band Steering was enabled, unnecessary functions would be performed.

Known Issues

Here are the known issues for version 9.0.5-0.1:

- The Radar Detecting Channel List is cleared when a radio setting is changed.
- The LAN port takes approximately 30 seconds to start communications after it links up.
- The LAN port takes approximately one minute to link up after a wired cable is disconnected and connected if the access point is powered by the AC adapter.
- The access point transmits the following illegal frames to the Port2 when the access point is in the Cascade mode.
  - Source MAC address and Destination MAC address are the same.
  - Source MAC address is a broadcast address.
- On the Legacy Rates on the Advanced Settings page for Radios, you must deselect rates lower than the selected minimum basic rate.
  - The basic rate for Radio 1 can be 1, 2, 5.5, or 11.
  - The basic rate for Radio 2 can be 6, 12, or 24.
- On the Neighbor AP page in Monitoring, the security shows WEP even when it is OSEN. OSEN is a security option, which can be used when Passpoint is enabled.
- Enabling IPv6 communication with IP auto-configuration of IPv6 Router Advertisement does not function on VAPs with dynamic VLAN enabled.
- Even when only the primary RADIUS server is specified, the following log can be issued: “RADIUS No response from Authentication server IP ADDRESS:PORT - failover.”
- If a wireless client in the power saving mode does not respond to the access point, it disconnects the wireless client even before the inactivity timer expires.

- When Vista Manager EX applies a configuration to the access point, the LAN port on the access point goes down for three seconds.
- Vista Manager EX occasionally fails to manage the access point right after the access point boots up.
- When the access point is configured as a part of the Wireless Distribution System (WDS), enabling both MAC Access Control and Fast Roaming (IEEE802.11r) on the access point is not supported.
- The access point with Management VLAN Tag enabled and VLAN ID set to 1 continues to communicate for several minutes even after the VLAN setting of the port on the switch connected to the access point is changed from Tagged 1 to Untagged 1.
- Fast Roaming does not function when Hidden SSID is enabled.
- Single-byte spaces can be entered into the Captive Portal URL field.
- When IEE802.11k is enabled, for some access points with Hidden SSID enabled, information is not shared correctly.
- Invalid numbers for VLAN ID starting with "0" are allowed to be saved & applied instead of rejected.
- A wireless client’s RX rate is shown as rounded down on Vista Manager EX.
- [AWC-CB] The AP may reboot when a network loop occurs.
- [AWC-CB] The AP will sometimes output an error log which includes “softirq: huh, entered softirq”.
- [AWC-CB] Sometimes, if an already-associated wireless client attempts to re-authenticate with the AP, the AP will disconnect that client.
- It may take up to one minute per wireless interface for the number of connected clients to be reflected by the MIB value atkkWiAcAPInfoNumOfSTA.

Limitations

Here are the limitations for version 9.0.5-0.1:

- Wireless Distribution System (WDS) and MU-MIMO / OFDMA cannot be enabled at the same time.
- When Dynamic VLAN is enabled, SNMP cannot get the value of OID 1.3.6.1.2.1.17.4.3.1.1 (MAC address information).

Limitations When Using Channel Blanket (AWC-CB)

Here are the limitations when using Channel Blanket (AWC-CB):

- Limitations on the access point:
  - Enabling Band steer on the access point is not supported.
  - The Change Duplicate AUTH received setting is not supported. Only Duplicate AUTH:ignore is supported.
  - The same radio settings are required on all access points under Channel Blanket.
  - Enabling WDS is not supported.

- Enabling AMF Application Proxy is not supported.
- Enabling AWC-SC VAP is not supported.

❒ Limitations on enabling Channel Blanket on a radio interface:
- Changing the RTS setting is not supported.
- Enabling Airtime Fairness is not supported.

❒ Limitations on enabling Channel Blanket VAP:
- Changing the Broadcast Key Refresh Rate is not supported.
- Changing the Session Key Refresh Rate is not supported.
- Changing the Session Key Refresh Action is not supported.
- Enabling RADIUS Accounting is not supported.
- Pre-authentication is disabled can cannot be enabled.
- The Session-Timeout RADIUS attribute is disabled and cannot be enabled.
- Changing the Inactivity Timer is not supported.
- IEEE802.11w (MFP) should be disabled.

❒ Limitations on the Channel Blanket settings:
- Setting Management VLAN ID and Control VLAN ID is not supported.
- Setting VAP VLAN ID and Control VLAN ID is not supported.

❒ Limitations on Channel Blanket behavior:
- Communications of wireless clients are affected when the access point is turned off or rebooted. It can take up to 2 minutes to restore communication with the AP.

Specifications with Channel Blanket (AWC-CB)

Here are specifications for the access point when using with Channel Blanket (AWC-CB).

Note
The following specifications do not apply to TQ5403, TQ5403e and TQ6602 access points using Channel Blanket.

❒ The access point will begin a deliberate reboot when a configuration from Vista Manager EX using Channel Blanket (AWC-CB) is applied. The access point will reboot in the following scenarios:
- Vista Manager EX applies the Channel Blanket profile settings to the access point for the first time.
- Vista Manager EX applies the Channel Blanket profile settings to an access point that has been configured as a multi-channel access point.
- Vista Manager EX removes the access point from Channel Blanket.

The following log is issued when the access point reboots for the above reasons:

cwmd[xxx]: CWM: APMgr[xxx]: AP XX:XX:XX:XX:XX:XX reboots for applying configuration

Supported Countries

Version 9.0.5-0.1 management software supports the following countries:

- Australia
- Austria
- Belgium
- Bulgaria
- Canada
- China
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hong Kong
- Hungary
- India
- Ireland
- Italy
- Japan
- Latvia
- Lithuania
- Luxembourg
- Malaysia
- Malta
- Netherlands
- New Zealand
- Poland
- Portugal
- Romania
- Singapore
- Slovakia Republic
- Slovenia
- Spain

- Sweden
- Taiwan
- Thailand
- United Kingdom
- United States

Contacting Allied Telesis

If you need assistance with this product, visit the Allied Telesis website at **www.alliedtelesis.com/services**.