TQ6403 GEN2 Wireless Access Points
Version 9.0.4-3.1 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 9.0.4-3.1:

- TQ6403 GEN2
- TQm6403 GEN2

The firmware filenames are:

- AT-TQ6403GEN2-9.0.4-3.1.img
- AT-TQm6403GEN2-9.0.4-3.1.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 configurations depends upon regions:
  - EMEA (CE and UK): All Radios are disabled.
  - RoW (CE and UK): All Radios are disabled.
  - Japan, United States, Canada, and Taiwan: All Radios are enabled.
- 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 9.0.4-3.1 for the TQ6403 GEN2 and TQm6403 GEN2 wireless access points added support for the following new features

- AWC-CB is supported in combination with AT-Vista Manager EX version 3.13.0 or later.
- Dynamic VLAN is supported with MAC Authentication. This feature allows an AP to assign a VLAN ID to a wireless client when authenticating using MAC Authentication.

  Note: if Dynamic VLAN is enabled with both WPA Enterprise and MAC Authentication, the VLAN ID as-signed by WPA Enterprise has higher priority.
- IEEE802.11b rates 1, 2, 5.5 and 11 can be disabled on the Radio page.
- All legacy rates can be selected as the Multicast Tx Rate (on Radio 1 only).
- CCMP is supported for WPA3 Enterprise security mode.
- Support for wildcard entry in Walled Garden.
- Support for DNS Proxy for Walled Garden. When DNS Proxy for Walled Garden is enabled, DNS frames from the wireless client will be managed by the DNS Proxy.
- 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.

Specification Changes

- Information has been added to the wireless disconnection log which indicates whether the originator is an access point or wireless client.

  The following messages have been added:

  - [Not AWC-CB VAP] STA mm:mm:mm:mm:mm:mm disassociated from BSSID zz:zz:zz:zz:zz:zz (EEE) for reason NNN by YYY (YYY: AP or STA)
  - [AWC-CB VAP] STA mm:mm:mm:mm:mm:mm disassociated from CB-BSSID zz:zz:zz:zz:zz:zz (EEE) for reason NNN by YYY (YYY: AP or STA)

Resolved Issues

Here are the resolved issues for version 9.0.4-3.1:

- The access point was sometimes unable to output all log files after the network had recovered from a network loop.
- 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.
- The "STASHED CHANGES" message would sometimes remain even after the "Stash" button had been clicked.
- Firmware upgrade would sometimes fail if Application Proxy had been configured on more than one VAP.
- Invalid numbers for VLAN ID starting with "0" were allowed to be saved & applied instead of rejected.
- The Proxy ARP feature stopped when one wireless client would send Neighbor Solicitation frames with 8 different IPv6 addresses.
- With Channel Blanket, when a wireless client left one access point after it was powered off and joined a new access point, multiple disconnections would sometimes occur on the AP.
- When roaming, if a wireless client moved AP three times, it would then not be able to communicate for up to 120 seconds.
- When "One channel mode" was used, the Scan data keep time would be incorrectly set on disabled radios.
- An AP would sometimes reboot when a profile was applied then the host name changed.

Known Issues

Here are the known issues for version 9.0.4-3.1:

- 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] When both Dynamic VLAN and IEEE802.1r fast-roaming are enabled, a Dynamic VLAN user may be disconnected from the AP.
- [AWC-CB] Sometimes, if an already-associated wireless client attempts to re-authenticate with the AP, the AP will disconnect that client.

Limitations

Here are the limitations for version 9.0.4-3.1:

- 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 Blanket 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 forced to be disabled.
  - The Session-Timeout RADIUS attribute is forced to be disabled.
  - 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 the access point in standalone.
  - 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 9.0.4-3.1 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**.