TQ6403 GEN2 Wireless Access Points
Version 9.0.4-1.1 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 9.0.4-1.1:

- ❒ TQ6403 GEN2
- ❒ TQm6403 GEN2

The firmware filenames are:

- ❒ AT-TQ6403GEN2-9.0.4-1.1.img
- ❒ AT-TQm6403GEN2-9.0.4-1.1.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 9.0.4-1.1 for the TQ6403 GEN2 and TQm6403 GEN2 wireless access points added support for the following new features

❒ New SNMP MIBs.

Standard MIB
- Support HOST-RESOURCES-MIB
- Support ENTITIY-MIB
- Support ENTITIY-SENSOR-MIB

Private MIB
- IP address of associated wireless client
- NetBIOS name of associated wireless client
- The total number of associated wireless clients

Radio interface information.
- A unique index for each Radio interface
- The radio channel

❒ New Radio mode options:

Radio1:
- IEEE 802.11b/g/n

Radio2:
- IEEE 802.11a/n
- IEEE 802.11a/n/ac

❒ Client Isolation per VAP.

❒ AMF Auto-Recovery.
- AMF Auto-Recovery can only be configured via AMF Master controller.

❒ Wi-Fi Scheduler.
- A user is able to change the status of Radios and VAPs on a schedule.
- Note that the wireless module of the AP will restart when the schedule is running.

❒ Changing the authentication page language for Captive Portal Click-through.

- Two-step authentication for MAC Access Control and Captive Portal. This field will only show on the MAC Access Control GUI if Captive Portal is enabled.
- A new scan method when Neighbor AP Detection is enabled, allowing the scanning method and scan time to be configured. One of the following scan methods can be selected:
  - All Channel (Default setting)
  - One Channel

  'All Channel' scans the entire band. The scan interval is every 5 minutes.

  'One Channel' scans one selected channel. When 'One Channel' is selected, the user can configure:
  - Scan interval:
  - Scan duration:
  - data keep time
- New fields on the “Security > WPA Enterprise” and “MAC Access Control > External RADIUS” page:
  - RADIUS Timeout
  - RADIUS Retransmit
  - Retry interval for Primary

Specification Changes

- The syslog buffer size has been increased from 64Kbyte to 4Mbyte.
- Improvements to configuring Passpoint settings via the GUI.
- “Frequency Band(GHz)” has been added to “Monitoring > Neighbor AP” page and “Monitoring > Associated Client” page.
- When a device reconnects to the network, a DHCP request will be sent immediately. It will not wait for DHCP lease time expiry.

Resolved Issues

Here are the resolved issues for version 9.0.4-1.1:

- When an access point's system time was corrected by the wireless controller's management, the wireless controller's statistics and the number of connected clients were not displayed.
- The Passpoint settings could be applied even if the following fields were not set:
  - NAI Realm information
  - Operator Friendly Name
  - OSU SSID
  - OSU Providers Service
- The access point was not storing the wireless client's transmit counter correctly.
- When multicast unicast conversion was enabled, the access point would block multicast frames received from wired devices.

- The access point occasionally rebooted when a large number of log files were output.
- When Management VLAN Tag was enabled, VLAN-related interface information would incorrectly be included in the Interface MIB.
- When accessing a neighbor AP list with a private MIB, an SNMP process would sometimes restart.
- The access point would occasionally fail to move channels when a radar was detected on channels that are generally reserved for radar.
- Beacons that included AC parameters were showing with no value for WMM Information Element.
- QR Code information would not display if the "View QR code" button was clicked repeatedly.
- A wireless client would fail to connect to the access point using PMKSA cache.
- When the 'Country' is set to PH (Philippines), the Radio 3 (5GHz high band) page would not be displayed.
- When Passpoint is enabled and WPA version is set to 'WPA and WPA2', the cipher suite settings would be empty.
- The maximum number of Realm Names than can be assigned is 10. It was possible to add more than 10 Realm Names and the VAP would then become unavailable.
- In Passpoint settings, when NAI realm entries were 10 or more, the access point would reboot.
- After initially connecting using PMKSA cache, if re-authentication occurred by the RADIUS server, the log would show it was re-authenticated using the PMKSA cache.

Known Issues

Here are the known issues for version 9.0.4-1.1:

- 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.

Limitations

Here are the limitations for version 9.0.4-1.1:

- 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).

Supported Countries

Version 9.0.4-1.1 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**.