TQ6702e 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 point supports version 9.0.4-1.1:

- ❒ TQ6702e GEN2

The firmware filename for the TQ6702e GEN2 version 9.0.4-1.1 access point is:

- ❒ AT-TQ6702eGEN2-9.0.4-1.1.img

For instructions on how to upgrade the firmware on the TQ6702e GEN2 access point, see the TQ6702e GEN2 *Access Point Installation Guide* at **www.alliedtelesis.com/library**.

New Features

Version 9.0.4-1.1 for the TQ6702e GEN2 wireless access point added support for the following new features:

- ❒ Per VAP Airtime Fairness Percentage control.
  - “Manual” has been added to the Airtime Fairness on the Radio page.
  - When setting the Airtime Fairness to Manual, a “Pre-allocated Airtime Percentage” item will appear in the Advanced Settings tab for each VAP.
  - Airtime Fairness “Enabled” has been changed to “Evenly”
- ❒ 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
- The total number of associated wireless clients for each radio

- New Radio mode options:

  Radio1:

  - IEEE 802.11b/g/n

  Radio2:

  - IEEE 802.11a/n
  - IEEE 802.11a/n/ac
- Changing RTS Threshold value.
- Multicast to Unicast conversion.
- AMF Application Proxy.
  - AMF Application Proxy can only be set from AT-Vista Manager.
- Client Isolation per VAP.
- Inter VAP wireless client isolation.
  - the Inter VAP wireless client isolation feature allows two VAPs with the same VLAN ID set for the same Radio to block VAP communication.
- 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

Enhancements

- Improved GUI response time of VAP/Security page:
  - Pages will switch immediately when selecting VAP0 to VAP15.
  - A “Stash” button has been added to the VAP/Security page.

  When changing settings for multiple VAPs at once, press the Stash button after editing the settings for each VAP, and then press “Save & Apply” at the end.

Specification Changes

- Proxy ARP support for wireless clients with static IP (not using DHCP) has been added.

  Proxy ARP will now respond with IP information to the following packets:
  - ARP request
  - ARP reply

  in addition to:
  - ARP Probe
  - ARP Announcement
  - DHCP ACK
- 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 the TQ6702e GEN2 access points version 9.0.4-1.1:

- When the access point was initialized with the Reset button, two identical log entries were added to the reboot.log.
- The AP would sometimes delete the login username and password if configuration from Vista Manager EX was applied at the same time as the AP's Web GUI was accessed.
- The access point would sometimes reboot when a configuration was applied by Vista Manager EX.
- 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.
- When changing Radio mode, the following unnecessary text was included in the popup message: “In addition, any VAP currently configured for WPA will have the CCMP (AES) cipher suite enabled.”
- Passpoint osu-providers method-list settings were not being applied correctly from Vista Manager mini.
- When Passpoint OSU Status is enabled, OSU SSID and OSU Providers Server URI are now required before the settings can be applied.
- When a large number of wireless clients were connected, and the AP requested the attWiAcClientTable MIB value, the response time would be long, and would sometimes result in a timeout.
- Passpoint settings could be applied even if the following fields were not set:
  - NAI Realm information
  - Operator Friendly Name
  - OSU SSID
  - OSU Providers Service
- When the country code was CA (Canada) and the location was switched between indoor and outdoor, sometimes the Bandwidth or Channel would be blank in the GUI.
- When Radius Accounting was enabled, certain attributes were not added to the Accounting-Request packet.
- Very occasionally, changing the settings in the AP's web GUI would cause the connection to be lost.
- If the security of a detected access point is WPA3-Personal, the Neighbor AP security is not displayed on Vista Manager EX.
- The access point would fail to reboot after a backup configuration was applied.
- The access point did not store the wireless client's transmit traffic counter correctly, and sent RADIUS accounting packets with invalid traffic counter information.
- The access point would sometimes reboot when the AP tried to restore a configuration.
- When Static LAG was enabled, a wireless client would sometimes temporarily fail to communicate after roaming to a new AP.
- One Private MIB reply was sent even when a number of wireless clients were connected.

- Channel and bandwidth settings would disappear when the location was switched to indoor 80+80 MHz.
- It was possible to load a country configuration file that did not match the country code stored on the AP.
- When the location was changed in the GUI, the correct channel list information for that location would sometimes not load.
- 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 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 is 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 the TQ6702e GEN2 access points 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.
- 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.
- 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.
- Packet losses or communication delay may occur for approximately ten seconds when Neighbor AP Detection is enabled. Leave Neighbor AP Detection disabled if you need to avoid the communication interruption.
- 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.
- Single-byte spaces can be entered into the Captive Portal URL field.
- When IEEE802.11k 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 the TQ6702e GEN2 access points version 9.0.4-1.1:

- LAG, LACP and Cascade mode for the LAN2 Port are not supported.
- The TQ6702e does not support AC Power Supply. It is powered only by PoE 802.3bt (Class 5).
- Changing value of the RTS threshold is not supported.
- Wireless Distribution System (WDS) and MU-MIMO / OFDMA cannot be enabled at the same time.
- Autonomous Wave Control-Channel Blanket (AWC-CB) is not supported.
- AWC-Smart Connect (AWC-SC) is not supported.
- 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).
- AWC-Dynamic Client Navigation (AWC-DCN) is not supported.
- Autonomous Management Framework (AMF) Application Proxy Redirect URL is not supported.

Supported Countries

The TQ6702e GEN2 access point version 9.0.4-1.1 management software supports the following countries:

- ❒ Argentina
- ❒ Australia
- ❒ Austria
- ❒ Bangladesh
- ❒ Belgium
- ❒ Bolivia
- ❒ Bosnia and Herzegovina
- ❒ Brazil
- ❒ Brunei
- ❒ Bulgaria
- ❒ Cambodia
- ❒ Canada
- ❒ Chile
- ❒ China
- ❒ Colombia
- ❒ Costa Rica
- ❒ Croatia
- ❒ Cyprus
- ❒ Czech Republic
- ❒ Denmark
- ❒ Ecuador
- ❒ Egypt
- ❒ El Salvador
- ❒ Estonia
- ❒ Finland
- ❒ France
- ❒ Germany
- ❒ Gibraltar
- ❒ Greece
- ❒ Guatemala
- ❒ Honduras
- ❒ Hong Kong
- ❒ Hungary Iceland
- ❒ India

- ❒ Indonesia
- ❒ Ireland
- ❒ Israel
- ❒ Italy
- ❒ Japan
- ❒ Korea
- ❒ Kuwait
- ❒ Latvia
- ❒ Liechtenstein
- ❒ Lithuania
- ❒ Luxembourg
- ❒ Macao
- ❒ Macedonia
- ❒ Malaysia
- ❒ Malta
- ❒ Mexico
- ❒ Monaco
- ❒ Montenegro
- ❒ Morocco
- ❒ Nepal
- ❒ Netherlands
- ❒ New Zealand
- ❒ Norway
- ❒ Pakistan
- ❒ Panama
- ❒ Paraguay
- ❒ Peru
- ❒ Phlippines
- ❒ Poland
- ❒ Portugal
- ❒ Qatar
- ❒ Romania
- ❒ Russia
- ❒ Saudi Arabia
- ❒ Serbia
- ❒ Singapore
- ❒ Slovakia Republic
- ❒ Slovenia

- ❒ Spain
- ❒ Sweden
- ❒ Switzerland
- ❒ Taiwan
- ❒ Thailand
- ❒ Turkey
- ❒ Ukraine
- ❒ United Arab Emirates
- ❒ United Kingdom
- ❒ United States
- ❒ Uruguay
- ❒ Uzbekistan
- ❒ Venezuela
- ❒ Vietnam

Contacting Allied Telesis

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