TQ6702e GEN2 Wireless Access Points
Version 9.0.6-0.1 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 9.0.6-0.1:

- ❒ TQ6702e GEN2

The firmware filename for the TQ6702e GEN2 version 9.0.6-0.1 access point is:

- ❒ AT-TQ6702eGEN2-9.0.6-0.1.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 9.0.6-0.1 for the TQ6702e GEN2 wireless access point added support for the following new features:

- ❒ Support for wireless client connection management based on RSSI values. This feature allows APs to disconnect wireless clients whose RSSI falls below a configurable threshold and prevent then from reconnecting until signal strength improves using the Disconnect Low-Signal Client setting.

  Disconnect Low-Signal Client can be enabled on the following page:

  Settings > VAP/Security > Advanced Settings

- Support for the customization of the MAC address used in the Calling-Station-ID. This is an attribute that the AP sends to a RADIUS server.

  The format can be changed to one of the following:

  1. Lowercase only (e.g., 00-10-a4-23-19-c0)
  2. No octet separators (e.g., 0010A42319C0)
  3. Lowercase with no octet separators (e.g., 0010a42319c0)

  The Calling-Station-ID format cna be changed on the following pages:

  Settings > VAP/Security > MAC Access Control

  Settings > VAP/Security > Security

Resolved Issues

Here are the resolved issues for the TQ6702e GEN2 access point version 9.0.6-0.1:

- When a wireless client connects to or disconnects from the network, the wireless chipset may occasionally detect an abnormal condition and perform a recovery process.
- If an access point receives IEEE 802.11ax related packets from a wireless client that is connected using IEEE 802.11a/b/g, an unintended reboot of the access point may occur.

Known Issues

Here are the known issues for version 9.0.6-0.1:

- 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. 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.
- While the access point is configured with the management VLAN tag enabled and the VLAN ID set to 1, and the VLAN setting of the LAN port of the switch connected to the access point is changed from tagged 1 setting to untagged 1, the switch is still able to communicate with the access point for several minutes.
- Single-byte spaces can be entered into the Captive Portal URL field.
- The walled garden wildcard entry is case sensitive.
- When IEEE802.11k is enabled, for some access points with Hidden SSID enabled, information is not shared correctly.
- 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".
- The Application Proxy feature sometimes produces duplicate copies of VLAN assignment log messages.
- It may take up to one minute per wireless interface for the number of connected clients to be reflected by the MIB value atkkWiAcAPInfoNumOfSTA.
- A beacon will be transmitted with maximum power even when the transmission output power on Radio1 is set to "Medium".
- 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.
- (AWC-CB) On a channel blanket AP with Proxy ARP enabled, when an ARP announcement packet is transmitted by another device that has the same IP address as a wireless client is received, the packet may be forwarded to the wireless VAP from all APs.
- When external page redirection is enabled for web authentication, a wireless client that has not yet completed web authentication may occasionally experience communication interruption from the AP when accessing an HTTPS page registered in the walled garden. This results in a certificate warning being displayed.

  If the warning screen appears, click Continue or refresh the page.
- Pre-authentication does not work when the following features are enabled:
  - LAN2 settings (Static LAG / LACP / Cascade)
  - WDS
  - Dynamic VLAN
  - Virtual IP address for web authentication
  - AMF Application Proxy

  The features operate normally otherwise.
- In environments where a total of 60 or more FQDN entries are registered in the web authentication walled garden, if communication failures or excessive latency occur between the AP and the DNS server, processing related to web authentication on the AP is delayed. The web authentication function may then fail to operate correctly.

This issue is automatically resolved once communication between the AP and the DNS server is restored or improved.

Enabling the DNS proxy for the walled garden can be used as a workaround to avoid this issue.

Limitations

Here are the limitations for the TQ6702e GEN2 access point version 9.0.6-0.1:

- 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.
- 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.

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 and 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 only apply to the TQ6702e GEN2 access points using Channel Blanket. These specifications do not apply to other Allied Telesis 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

The TQ6702e GEN2 access point version 9.0.6-0.1 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**.