TQ6000 GEN2 Wireless Access Points
Version 8.0.4-1.1 Software Release Notes

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

Supported Platforms

The following access points support version 8.0.4-1.1:

- ❒ TQ6702 GEN2
- ❒ TQm6702 GEN2
- ❒ TQ6602 GEN2
- ❒ TQm6602 GEN2

For instructions on how to upgrade the management software on the TQ6000 GEN2 wireless access points, see the *TQ6000 GEN2 Wireless Access Points Installation Guide*, available on the Allied Telesis website at **www.alliedtelesis.com/library.**

The firmware filenames are:

- AT-TQ6702GEN2-8.0.4-1.1.img
- AT-TQm6702GEN2-8.0.4-1.1.img
- AT-TQ6602GEN2-8.0.4-1.1.img
- AT-TQm6602GEN2-8.0.4-1.1.img

New Features

Version 8.0.4-1.1 added the following new features:

- 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 assigned 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 with WPA3 Enterprise security mode.
- Support for 4 operating Spatial Streams on Radio 2 for 5GHz as well as the previous support for 8 streams. This reduces the maximum power consumption when using 5GHz.
- Support for verifying RADIUS packets. This feature prevents RADIUS protocol forgery attacks and is available in Settings > VAP/Security on the following pages:
  - Security > Mode: WAP 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

The following specification changes have been made in version 8.0.4-1.1:

- 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

The following issues have been resolved in version 8.0.4-1.1:

- The access point occasionally rebooted when a large number of log files were output.
- 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.
- A 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.
- Off-Channel CAC (Channel Availability Check) would sometimes fail to scan the second channel if Auto Channel was changed to a wide range.
- Following a target assertion, upon recovery, Zero-Wait DFS would sometimes set a channel that was not part of the Auto Channel Selection.
- Following wireless recovery, Radio 1 would stop transmitting.
- [AWC-CB] If there was a delay in an AP responding to Auth Requests, many Auth messages would be circulated. This would cause a long delay in connecting a VAP.

Note
The following resolved issues only relate to TQ6702 GEN2 and TQ6602 GEN2.

- [AWC-CB] An access point would sometimes reboot when a wireless client enabled Proxy ARP.

Known Issues

Here are the limitations for the access points version 8.0.4-1.1:

- A LAN port takes approximately 30 seconds to start communications after it links up.
- When the access point is powered with the AC adapter, a LAN port might take one minute to link up after the cable is disconnected and connected.
- The wireless client’s static IP is not supported when Proxy ARP is enabled on a VAP.

- The access point transmits the following illegal frames to other LAN ports when Cascade connection is enabled:
  - Frames with the same Source and Destination MAC addresses
  - Frames with the source MAC address as the 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.
- The Multicast to Unicast conversion feature must be enabled to use IPv6 communication with the IP Auto configuration of IPv6 Router Advertisement on a cell VAP with Dynamic VLAN enabled. Do not use IPv6 communication with the IP Auto configuration of IPv6 Router Advertisement on a Channel Blanket VAP with Dynamic VLAN enabled.
- Even when only the primary RADUIS server is specified, a following log can be issued: “RADIUS No response from Authentication server IP ADDRESS:PORT - failover.”
- When a wireless client in the power saving mode does not respond to the access point, the wireless client will be disconnected before the inactivity timer expires.
- A LAN port goes down for three seconds when Vista Manager EX applies a configuration to the access point.
- The access point occasionally fails to be managed by Vista Manager EX right after the access point boots up.
- While the access point is configured with the management VLAN tag enabled and the VLAN ID set to 1, 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 still can communicate with the access point for several minutes.
- RADIUS Authentication fails when the RADIUS key contains ″￥″.
- Fast roaming IEEE802.11r with MAC Access Control and Distributed System cannot be enabled at the same time.
- 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.
- A wireless client’s RX rate is shown as rounded down on Vista Manager EX.
- The Application Proxy feature sometimes produces duplicate copies of VLAN assignment log messages.

Note
The following issue is applied only to the TQ6702 GEN2 and TQ6602 GEN2 access points:

- (AWC-CB) The access point might report to Vista Manager EX less than the actual number of associated wireless clients.
- (AWC-CB) When both Dynamic VLAN and IEEE802.1r fast-roaming are enabled, a Dynamic VLAN user may be disconnected from the AP.

Note
The following issues are applied only to the TQm6702 GEN2 and TQm6602 GEN2 access points:

- (AWC-SCL) The cluster is occasionally deconstructed temporarily when a change is made on the settings on the VAP page of the AWC-SCL cluster constructed access point. The cluster is automatically reconstructed after deconstructed.
- (AWS-SCL) When an AWC-SCL cluster is built for the first time, the "Synchronize settings from" status might show to an access point as "Not Synchronized." When the status is displayed, you need to restart the access point with the "Not Synchronized" status.

Limitations

- 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-SC and NU-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.
  - Changing the LAN2 port configuration is not supported.
  - 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 Broadcast Key Refresh Rate is not supported.
  - Changing Session Key Refresh Rate is not supported.
  - Changing the Session Key Refresh Action setting 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 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 takes approximately two minutes to restore the communications of wireless terminals connected to the access point that is powered off.

Specifications with Channel Blanket (AWC-CB)

Here are specifications on the access point with Channel Blanket (AWC-CB):

Note
The following specifications only apply to the TQ6000 GEN2 access points using Channel Blanket. These specifications do not apply to other Allied Telesis access points using Channel Blanket.

❒ The access point is specified to reboot when Vista Manager EX applies configurations on Channel blanket to the access point. The access point reboots when:
- 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
```

Limitations When Using Smart Connect (AWC-SC)

Here are the limitations when using Smart Connect (AWC-SC):

❒ Limitations on the access point:
- Enabling Management VLAN on the access point is not supported.
- Enabling WDS is not supported.
- Changing the Static LAG/LACP/Cascade configuration on LAN2 port is not supported.
- Enabling Channel Blanket is not supported.

- Limitations on enabling the Smart Connect Radio Interface:
  - Enabling the Neighbor AP Detection feature is not supported.
  - Enabling MU-MIMO is not supported.
  - Enabling OFDMA is not supported.
  - Changing the Client Isolation settings is not supported.
- Limitations on the other items except the access point and Smart Connect Radio Interface:
  - The Smart Connect feature and AMF guest cannot be used at the same time.
  - The Smart Connect feature on the access point and DHCP Snooping feature on the switch cannot be used at the same time.

Specifications for Combination with Smart Connect

Here are specifications on access points with Smart Connect (AWC-SC):

Note
The specifications in this section are applied only to the TQ6702 GEN2 and TQ6602 GEN2 access points. These specifications are not applied to other Allied Telesis access points using Smart Connect.

- The access point is specified to reboot when Vista Manager EX applies configurations on Smart Connect to the access point. The access point reboots when:
  - Vista Manager EX applies the Smart Connect profile settings to the access point for the first time.
  - Vista Manager EX applies the Smart Connect profile settings to the access point in standalone.
  - Vista Manager EX removes the access point from Smart Connect.

  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
  ```

Limitations for Combination with Smart Cluster (AWC-SCL)

Here are the limitations when using the Smart Cluster feature:

- Limitation on the access point:
  - If a Single Channel Group ID has been already used on access points in another network in your near wireless spatial, the access point with the same Single Channel Group ID in your network is not supported.
- Limitations on enabling the AWC-SCL Single-Channel Radio Interface:
  - The Radio must be in the default settings. Reset the Radio to the default settings before setting the Radio to the Single Channel type.

- Changing the VAP0 setting from “Settings > VAP / Security” page is not supported when the VAP0 mode is Single-Channel Type. Reset VAP0 to the default settings before setting the Radio to the Single Channel type.
- Changing configurations from the Easy Setup page is not supported when the Bandwidth has other than 20 MHz on the Radio settings.
- To configure the Radios as the single channel mode from the Easy Setup page, the Radio settings on the access point must be the default settings.
- When the access point is configured as the Single-Channel mode in Radio 1, changing the settings from the Settings > VAP/Security > Radio 1 > VAP0 and VAP15 pages is not supported.
- When the access point is configured as the Single-Channel mode in Radio2, changing the setting from the Settings > VAP/Security > Radio 2 > VAP0 page is not supported.
- When the access point is configured as Single-Channel mode, changing configurations from the Easy Setup page is not supported if VAP0 is not in the default settings.

❒ Limitations on the other items:

- AWC Plug-in cannot manage the access point during building an SCL cluster. AWC Plug-in can manage the access point after it has built an SCL cluster; however, the SCL feature is not available for the access point under the AWC Plug-in management. The configurations made from the Easy Setup page on the access point is overwritten with configurations by AWC Plug-in. Therefore, the Cluster status on the access point is disabled when AWC Plug-in accesses the access point.
- DHCP option 43 is not supported. The AWC-SCL Cluster is disabled when the access point receives an IP address via DHCP with the option 43.
- AMF Auto-Recovery is not supported with AWC-SCL. When AMF Auto-Recovery tries to restores configurations on the access point, which AWC-SCL operates on, the AMF Auto-Recovery sequence might fail.

Specifications for Access Points with Smart Cluster

Here are specifications on access points with Smart Cluster (AWC-SCL):

Note
The specifications this section are applied only to the TQm6702 GEN2 and TQm6602 GEN2 access points.

❒ The AWC-SCL cluster can be established among the same models only. No clusters can be established in combination of the TQm6702GEN2 and TQm6602GEN2 models.

❒ The access point reboots with an exception when the Radio setting is changed from the Single Channel mode to the Cell mode or from the Cell mode to the Single Channel mode.

The access point reboots in the following cases:

- Case1: Radio1 is changed from the Single Channel mode to the Cell mode.

Radio2 is changed from the Single Channel mode to the Cell mode.

- Case2: Radio1 is changed from the Cell mode to the Single Channel mode.
  Radio2 is changed from the Cell mode to the Single Channel mode.
- Case3: Radio1 is in the Cell mode.
  Radio2 is changed from the Cell mode to the Single Channel mode

The access point does not reboot in the following case:

- Case4: Radio1 is changed from the Single Channel mode to the Cell mode.
  Radio2 is in the Single Channel mode.

- One AWC-SCL cluster can have up to ten access points.
- The frames that the access point in the Single Channel mode controls depends upon the management VLAN tag setting:
  - When Management VLAN is disabled, the controlled frames are untagged frames.
  - When Management VLAN is enabled, the controlled frames are tagged frames with the same VLAN ID as the Management VLAN ID.
- The access points in the AWC-SCL cluster do not share the following values:
  - Host Name
  - Mac Address
  - IP Address settings
  - SNMP system location (SNMP > System Name/System Contact/System Location)
  - Channel and Transmission Power when VAP0 is in the Cell mode
  - Transmission Power when VAP0 is in the Single Channel mode
- When Radio1 is in the Single Channel mode, the BSSID value of the Radio1 VAP15 is considered as the MAC address of Radio1 VAP0. Do not enable Radio1 VAP15 or use Radio1 VAP15 for wireless communication.
- The BSSID value of a VAP in the Single Channel mode is considered as the MAC address and used to determine which VAP has the largest MAC address among the AWC-SCL Cluster's members.
- Automatic Channel Selection functions only when Radios in the access points are in the Single Channel mode. Channel Coordination runs among the access points in clusters in the same Layer 2 network. Channel Coordination does not run on the access points in other than the Single Channel mode. Rebooting the access point does not always re-activate Automatic Channel Selection.
- By default, in the access point with AWC-SCL:
  - Client Isolation: Disabled
  - RSSI Threshold: 30

Limitation for using Easy Setup

Here is a limitation when using the Easy Setup

- Configuring the access point with both Easy Setup and Vista Manager EX is not supported.

Specifications for Easy Setup

The following specifications are for Easy Setup:

Note
The specifications this section are applied only to the TQm6702 GEN2 and TQm6602 GEN2 access points.

- The access point can be configured using either Easy Setup or Vista Manager EX (AWC Lite), but not both of them.
- The Radios and VAP0 must have the following settings for the access point to select the VAP Mode: Cell Type on the Ease Setup page:
  - Radio1 Radio: Basic Settings > Mode: IEEE802.11 b/g/n/ax
  - Radio2 Radio: Basic Settings > Mode: IEEE 802.11 a/n/ac/ax
    Advance Settings > Maximum Client: 200
  - Radio1/Radio2 VAP0: Basic Settings > Security Mode: WPA Personal
    Basic Settings > Security WPA Version: WPA2 and WPA3
    Basic Settings > Security Cipher Suites: CCMP
    Basic Settings > Security IEEE802.11w (MFP): Enabled
    Advanced Settings > Association Advertisement: Disabled
- The Radios and VAP0 must have the following settings for the access point to select the VAP Mode: Single Channel Type on the Ease Setup page:
  - Radio1 Radio: Basic Settings > Mode: IEEE802.11 b/g/n/ax
  - Radio2 Radio: Basic Settings > Mode: IEEE 802.11 a/n/ac/ax
    Advance Settings > Maximum Client: 200
  - Radio1/Radio2 VAP0: Basic Settings > Security Mode: WPA Personal
    Basic Settings > Security WPA Version: WPA2
    Basic Settings > Security Cipher Suites: CCMP
    Basic Settings > Security IEEE802.11w (MFP): Disabled
- Advanced Settings > Association Advertisement: Enabled

Contacting Allied Telesis

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