TQ6403 GEN2 Wireless Access Points
Version 9.0.5-1.1 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 9.0.5-1.1:

- TQ6403 GEN2
- TQm6403 GEN2

The firmware filenames are:

- AT-TQ6403GEN2-9.0.5-1.1.img
- AT-TQm6403GEN2-9.0.5-1.1.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 configuration depends upon regions:
  - Japan, United States, Canada, and Taiwan: All Radios are enabled.
  - All other countries: All Radios are disabled.
- 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 9.0.5-1.1 for the TQ6403 GEN2 and TQm6403 GEN2 wireless access points added support for the following new features:

- Support for configuring the Key Holder List. The Key Holder List, used with 802.11r (Fast Roaming), can now be configured manually from the following page:

  Settings > VAP/Security > Fast Roaming
- Pre-authentication is now supported on VAPs 1-15 (previously this was only available on VAP0).

  When security mode is **WPA-Enterprise** or **OSEN**, pre-authentication on VAPs 0-15 can be enabled or disabled on the following page, for each VAP:

  Settings > VAP/Security > Security.

Resolved Issues

Here are the resolved issues for version 9.0.5-1.1:

- An unexpected reboot would occasionally occur when MFP(IEEE802.11w) was enabled.
- The access point would sometimes unexpectedly reboot if the chip detected an abnormality.
- QR Code information would not be displayed if the "View QR code" button was clicked repeatedly.
- An AP would sometimes unexpected reboot when Airtime Fairness was enabled.

- When WPA3 Enterprise CCMP mode was set, the message "STASHED CHANGES: NEED TO APPLY STASHED SETTINGS." would be displayed incorrectly.
- When external page redirect was set to an FQDN (not an IP address), after applying settings and rebooting, the web authentication screen would not appear for VAP0 for up to 5 minutes.
- After a wireless client logged in on the Captive Portal page, the welcome screen on the device would not display correctly.
- Wireless connection to specific VAPs would sometimes fail after the AP was startup or when applying settings.
- The AP would reboot if 13 or more VAPs, across all radios, were enabled.
- When a blank setting is saved on Captive Portal's Walled Garden, the "stash change" message would be incorrectly displayed.
- Saving Radio settings would occasionally fail.
- When changing the mode in Radio settings, the popup dialog would sometimes contain incorrect information.
- Whilst managed by an AWC Plug-in, if an AP requested a tech support file that happened to be large, memory usage would spike and communication would sometimes be lost.
- MAC address lists would not be saved correctly.
- A stack overflow, causing a reboot, could occur when receiving WNM action frames larger than 1024 bytes.
- Fixed an issue where the link speed could downgrade from 2.5G to 1000M, then from 1000M to 100M, when repeatedly linked up and then immediately linked down.
- With SNMP enabled, the AP would sometimes not send authentication failure traps when an incorrect community name was used.

The following resolved issue applies only to the TQ6403 GEN2:

- With Channel Blanket, if handover with a wireless client was performed repeatedly, it would occasionally become impossible for the AP to communicate with wireless clients.

Known Issues

Here are the known issues for version 9.0.5-1.1:

- 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.
- 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.
- The walled garden wildcard entry is case sensitive.
- 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] xx
- 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".

Limitations

Here are the limitations for version 9.0.5-1.1:

- 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).

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 can 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 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 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

Version 9.0.5-1.1 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**.