



## TQ6702e GEN2 Wireless Access Points Version 9.0.4-3.1 Software Release Notes

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

- ❑ “Supported Platforms,” next
- ❑ “New Features” on page 1
- ❑ “Specification Changes” on page 2
- ❑ “Resolved Issues” on page 2
- ❑ “Known Issues” on page 3
- ❑ “Limitations” on page 4
- ❑ “Limitations When Using Channel Blanket (AWC-CB)” on page 4
- ❑ “Specifications with Channel Blanket (AWC-CB)” on page 5
- ❑ “Supported Countries” on page 6
- ❑ “Contacting Allied Telesis” on page 9

### Supported Platforms

---

The following access point supports version 9.0.4-3.1:

- ❑ TQ6702e GEN2

The firmware filename for the TQ6702e GEN2 version 9.0.4-3.1 access point is:

- ❑ AT-TQ6702eGEN2-9.0.4-3.1.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](http://www.alliedtelesis.com/library).

### New Features

---

Version 9.0.4-3.1 for the TQ6702e GEN2 wireless access point added support for 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 for WPA3 Enterprise security mode.
  - ❑ Support for wildcard entry in Walled Garden.
  - ❑ Support for DNS Proxy for Walled Garden. When DNS Proxy for Walled Garden is enabled, DNS frames from the wireless client will be managed by the DNS Proxy.
  - ❑ Support for verifying RADIUS packets. This feature prevents RADIUS protocol forgery attacks and is available in Settings > VAP/Security on the following pages:
    - Settings > VAP/Security:
      - Security > Mode: WPA 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

---

- ❑ 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: 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: disassociated from CB-BSSID zz:zz:zz:zz:zz:zz (EEE) for reason NNN by YYY (YYY: AP or STA)

## Resolved Issues

---

Here are the resolved issues for the TQ6702e GEN2 access point version 9.0.4-3.1:

- ❑ The access point was sometimes unable to output all log files after the network had recovered from a network loop.
- ❑ 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.
- ❑ Firmware upgrade would sometimes fail if Application Proxy had been configured on more than one VAP.

- ❑ [AWC-CB] AP would sometimes reboot when multiple wireless clients connected and disconnected at the same time.
- ❑ 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.
- ❑ When "One channel mode" was used, the Scan data keep time would be incorrectly set on disabled radios.
- ❑ An AP would sometimes reboot when a profile was applied then the host name changed.

## Known Issues

---

Here are the known issues for version 9.0.4-3.1:

- ❑ 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.
- ❑ [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] When both Dynamic VLAN and IEEE802.1r fast-roaming are enabled, a Dynamic VLAN user may be disconnected from the AP.
- ❑ The Application Proxy feature sometimes produces duplicate copies of VLAN assignment log messages.

## Limitations

---

Here are the limitations for the TQ6702e GEN2 access point version 9.0.4-3.1:

- ❑ 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.

## 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 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 forced to be disabled.
  - The Session-Timeout RADIUS attribute is forced to be disabled.
  - 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 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:

```

cwmmd[xxx]: CWM: APMgr[xxx]: AP XX:XX:XX:XX:XX:XX reboots for applying
configuration
  
```

## Supported Countries

---

The TQ6702e GEN2 access point version 9.0.4-3.1 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
- Philippines
- 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](http://www.alliedtelesis.com/services).

Copyright © 2025 Allied Telesis Inc., Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis Inc., Inc. Allied Telesis Inc. and the Allied Telesis Inc. logo are trademarks of Allied Telesis Inc., Incorporated. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners. Allied Telesis Inc., Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis Inc., Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis Inc., Inc. has been advised of, known, or should have known, the possibility of such damages.