



## TQ6702e 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,” next
- “New Features” on page 1
- “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 5
- “Contacting Allied Telesis” on page 9

### Supported Platforms

---

The following access point supports version 9.0.5-1.1:

- TQ6702e GEN2

The firmware filename for the TQ6702e GEN2 version 9.0.5-1.1 access point is:

- AT-TQ6702eGEN2-9.0.5-1.1.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](http://www.alliedtelesis.com/library).

### New Features

---

Version 9.0.5-1.1 for the TQ6702e GEN2 wireless access point 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 the TQ6702e GEN2 access point version 9.0.5-1.1:

- ❑ An unexpected reboot would occasionally occur when MFP(IEEE802.11w) was enabled.
- ❑ 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.
- ❑ 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.
- ❑ In rare instances, wireless clients could not communicate on specific VAPs following boot up of the AP.
- ❑ 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.
- ❑ The AP would reboot if 13 or more VAPs, across all radios, were enabled.
- ❑ Wireless connection to specific VAPs would sometimes fail after the AP was startup or when applying settings.
- ❑ 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.
- ❑ Even when the 5GHz radio was disabled, the following message would incorrectly appear "Selected channel is illegal for outdoor usage".
- ❑ When the channel destination was configured as a DFS channel, band steering would not work.
- ❑ With SNMP enabled, the AP would sometimes not send authentication failure traps when an incorrect community name was used.

## 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. 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 atkWiAcAPInfoNumOfSTA.
- ❑ 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 the TQ6702e GEN2 access point version 9.0.5-1.1:

- ❑ 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.
- ❑ 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:

```

cwm[d[xxx]: CWM: APMgr[xxx]: AP XX:XX:XX:XX:XX:XX reboots for applying
configuration

```

## Supported Countries

---

The TQ6702e GEN2 access point version 9.0.5-1.1 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
- 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.