



TQ6403 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,” next
- ❑ “Specifications for Easy Setup” on page 2
- ❑ “New Features” on page 2
- ❑ “Resolved Issues” on page 2
- ❑ “Known Issues” on page 3
- ❑ “Limitations” on page 5
- ❑ “Limitations When Using Channel Blanket (AWC-CB)” on page 5
- ❑ “Specifications with Channel Blanket (AWC-CB)” on page 6
- ❑ “Supported Countries” on page 6
- ❑ “Contacting Allied Telesis” on page 8

Supported Platforms

The following access points supports version 9.0.6-0.1:

- ❑ TQ6403 GEN2
- ❑ TQm6403 GEN2

The firmware filenames are:

- ❑ AT-TQ6403GEN2-9.0.6-0.1.img
- ❑ AT-TQm6403GEN2-9.0.6-0.1.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 9.0.6-0.1 for the TQ6403 GEN2 and TQm6403 GEN2 wireless access points 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 them 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 can be changed on the following pages:

Settings > VAP/Security > MAC Access Control

Settings > VAP/Security > Security

Resolved Issues

Here are the resolved issues for 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.
- ❑ 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.
- ❑ Single-byte spaces can be entered into the Captive Portal URL field.
- ❑ Fast Roaming does not function when Hidden SSID is enabled.

- ❑ A wireless client's RX rate is shown as rounded down on Vista Manager EX.
- ❑ 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".
- ❑ 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** on the warning screen 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, and the web authentication function may 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. When Radio1, Radio2, and Radio3 are all enabled, and there is an SSID subject to band steering on Radio1 and Radio2, a connection attempt to either Radio1 or Radio2 may be rejected once if the bands of Radio1 and Radio2 are congested. After the initial connection rejection, the wireless client is able to connect successfully.

Note

The following issues only apply to the TQ6403 GEN2 access point:

- ❑ [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] Sometimes, if an already-associated wireless client attempts to re-authenticate with the AP, the AP will disconnect that client.
- ❑ [AWC-CB] When channel blanket-related settings are applied from the wireless LAN controller, an intended reboot occurs on the affected access point. However, during this process unnecessary dump files may sometimes be generated.

The intended reboot scenarios are as follows:

 - During the initial application of common Channel Blanket (CB) settings.

- When applying settings to add common CB settings to an environment that is currently operating with only common AP settings.
- When applying settings to switch from an environment operating with common CB settings to one using only an AP profile.
- ❑ [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.

Limitations

Here are the limitations for version 9.0.6-0.1:

- ❑ 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 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:

```

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

Supported Countries

Version 9.0.6-0.1 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.

Copyright © 2026 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.