TQ7403 Wireless Access Point
Version 10.0.4-3.1 Software Release Notes

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

Supported Platform

The following access point supports version 10.0.4-3.1:

- ❒ TQ7403

The firmware filename is:

- ❒ AT-TQ7403-10.0.4-3.1.img

For instructions on how to upgrade the management software on the TQ7403 wireless access points, see the *TQ7403 Wireless Access Point Installation Guide*, available on the Allied Telesis Inc. website at **www.alliedtelesis.com/library.**

New Features

Here are the new features for the TQ7403 access point version 10.0.4-3.1:

- ❒ 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.
- Support for using Radio 3 in Taiwan (TW)

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: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

Here are the resolved issues for the TQ7403 access point version 10.0.4-3.1:

- 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.
- Following a reboot, an AP could take up to 130 seconds to join as an AMF Guest node.
- When the Captive Portal page was viewed over HTTPS, the Captive Portal page would sometimes become inaccessible.
- A managed AP was not sending Association List information to Vista Manager EX.

- 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.

Known issues

Here are the known issues for the TQ7403 access point version 10.0.4-3.1

- 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.
- The LAN port on the access point that is powered from the AC adapter takes approximately one minute to link up when the Ethernet cable is disconnected and connected.
- The access point transmits the following illegal frames to the Ethernet port on the link partner when PORT2 is in the Cascade mode:
  - The Source MAC address and Destination MAC addresses are the same.
  - The 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 is displayed as WEP even when the security is set to OSEN. OSEN is a security option and can be selected when Passpoint is enabled.
- Communications via IPv6 fail on VAPs with Dynamic VLAN enabled when IP auto-configuration of IPv6 Router Advertisement is enabled.
- Even when only the primary RADUIS server is specified, a following log might 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 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 in the URL field for Captive Portal.
- 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.
- If an IP address is assigned from a DHCP server with a DHCP lease time of 1 minute or less, the AMF guest node feature will not work.
- [AWC-CB] The AP may reboot when a network loop occurs.

- [AWC-CB] When the AP disconnects a wireless client by “Disconnection No ACK” after hand-over, the AP does not send deauth frame to Radio3’s VAP.
- [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.

Limitations

Here are the limitations for version 10.0.4-3.1:

- 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).
- Fast Roaming with Enabling Over the DS on Radio3 (6GHz) 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 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.

Specifications with Channel Blanket (AWC-CB)

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

Note
The following specifications do not apply to TQ5403, TQ5403e and TQ6602 using Channel Blanket

- 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
```

Supported Countries

The TQ7403 access point continues to support the following countries:

- ❒ Australia
- ❒ Austria
- ❒ Belgium
- ❒ Bulgaria
- ❒ Canada
- ❒ Croatia
- ❒ Cyprus
- ❒ Czech Republic
- ❒ Denmark
- ❒ Estonia
- ❒ Finland
- ❒ France
- ❒ Germany

- ❒ Greece
- ❒ Hong Kong
- ❒ Hungary
- ❒ 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**.