TQ7403 Wireless Access Point
Version 10.0.6-0.1 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 10.0.6-0.1:

- ❒ TQ7403

The firmware filename is:

- ❒ AT-TQ7403-10.0.6-0.1.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 10.0.6-0.1:

- ❒ 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 then 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 the TQ7403 access point version 10.0.6-0.1:

- If clients in different VLANs connected to the same wireless AP, communication between them may have become unavailable when the following features were enabled.
  - Dynamic VLAN
  - AMF Application Proxy
  - Virtual IP address for Captive Portal
  - LAN2 Port Settings (Static LAG, Cascade, LACP)
  - WDS (Wireless Distribution System)
  - AWC-CB (Channel Blanket)

Known issues

Here are the known issues for the TQ7403 access point version 10.0.6-0.1

- 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 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.
- Fast roaming IEEE802.11r with MAC Access Control and Distributed System cannot be enabled at the same time.
- The LAN port on the access point goes down for three seconds when a configuration is being applied by either Vista Manager EX or the Device GUI.
- 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.
- 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.
- The walled garden wildcard entry is case sensitive.
- 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”.
- It may take up to one minute per wireless interface for the number of connected clients to be reflected by the MIB value atkkWiAcAPInfoNumOfSTA.
- An AP will very occasionally reboot if the power is cycled on and off several times.
- A beacon will be transmitted with maximum power even when the transmission output power on Radio1 or Radio3 is set to "Middle".
- When using IEEE802.11n or a later wireless standard, Wi-Fi Multi Media (WMM) would not be disabled, despite being set to 'disable' in its configuration.
- 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.

- 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 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. The web authentication function may then 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.

Limitations

Here are the limitations for version 10.0.6-0.1:

- 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).
- 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 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 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 disabled and cannot be enabled.
  - The Session-Timeout RADIUS attribute is disabled and cannot be enabled.
  - 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

- 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

The TQ7403 access point continues to support the following countries:

(Note: * 6GHz cannot be selected in these 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
- ❒ Philippines
- ❒ 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**.