TQ7403 Wireless Access Point
Version 10.0.5-0.1 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 10.0.5-0.1:

- TQ7403

The firmware filename is:

- AT-TQ7403-10.0.5-0.1.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 10.0.5-0.1:

- Support for allowing different MAC Address lists to be set for each VAP.
  - Create Multiple MAC address lists from the Settings > MAC Address List page.
  - Select MAC address lists for each VAP on the Settings > VAP/Security > MAC Access Control page.

- Register up to a maximum of 3072 wireless clients from the Settings > MAC Address List page.
- Support for 'Transmit unlearned ARP packet'. Enable this on the Settings > VAP/Security page, when Proxy ARP is enabled.
- Support for 'Client Packet Analysis' with AWC plugin for Vista Manager EX.

  When enabled on the plugin, the AP will share logs containing wireless client information such as when the following has occurred:

  - a DHCP Discovery packet has been sent.
  - a DHCP Acknowledge packet has been sent.
  - an IP address has been received via DHCP.
  - an ARP resolution has been completed with the default gateway.
  - a DNS resolution with the DNS server has been completed.

  Note:

  - This function applies only when a wireless client has received an IP address from DHCP.
  - This function does not apply when the wireless client uses fixed IP addresses.
  - This function is not supported for Channel Blanket VAPs.

  When enabled, the following wireless information will be sent from the AP to the AWC plugin:

  - OS name
  - Host name
- Support for sharing the following wireless client information with the wireless LAN controller:
  - VLAN ID
  - Security
  - WPA version
  - Channel noise
  - SNR (Signal-to-Noise Ratio)

Specification Changes

- Radio 3 channel selection has the following changes:

  When you use the AP's Device GUI to configure channel settings:

  The channel drop-down list displays "PSC" in brackets next to each Preferred Scanning Channel (PSC). This applies to all bandwidths (20, 40, 80 or 160 MHz).

  If you select 40, 80, or 160 MHz as the bandwidth, then the AP decides which channel to use as the operating channel in the following way:

  - If you select a non-PSC channel from the channel list, a pop-up message recommends you use a PSC channel. This is only a recommendation; you can still choose the non-PSC.
  - If the Channel setting is Auto, the AP prioritizes using a PSC channel.

- If the Channel setting is Auto and Auto Channel Selection contains a channel bonding group with a PSC channel, then the AP uses the PSC channel.
- If the Channel setting is Auto and Auto Channel Selection does not contain a channel bonding group with a PSC channel, then the AP uses the non-PSC channel.

When you use Vista Manager's AWC Plug-in to configure channel settings:

If:

- You select 40, 80, or 160 MHz as the bandwidth (from the AWC Plug-in's AP Profile page), and
- The channel setting is Auto in the Wireless AP Individual Configuration (from the AWC Plug-in's AP Settings page)

Then the AP chooses the operating channel as follows:

- If the AP's channel setting in the AlliedWare Wireless GUI is Auto, then the AP prioritizes using a PSC channel as the operating channel.
- If the AP's channel setting in the AlliedWare Wireless GUI is fixed, the AP does not change the operating channel.

Note that if the AP Profile channel section doesn't include the AP's current operational channel, then the AP chooses the operating channel in the following way:

- If a PSC channel is included in the AP profile, the AP prioritizes the lowest-numbered PSC channel.
- If a PSC channel is not included in the AP profile, the AP prioritizes the lowest-numbered non-PSC channel.

How AWC auto-configuration selects the channel:

When the bandwidth in the AP profile is 40, 80, or 160 MHz, AWC auto-configuration chooses the operating channel as follows:

- If the configured channel is from a channel bonding group with a PSC channel, then the AP uses the PSC channel.
- If the configured channel is from a channel bonding group with no PSC channel, then the AP uses the non-PSC channel.

❒ When Band Steering is enabled, IEEE802.11v and IEEE802.11k are forcibly enabled on all VAPs. There will not be any visible change of settings in the configuration.

❒ Changes to the following log outputs:

1. When a connection is rejected by the MAC access control function, the reason for the rejection is added to the end of the log. The reasons for the rejection are displayed as one of the following:
   - Allow List
   - Deny List
   - RADIUS
   - Allow List + RADIUS
   - Deny List + RADIUS
2. When a wireless client is connected, the VLAN ID it is assigned to is added to the log output.

Resolved Issues

Here are the resolved issues for the TQ7403 access point version 10.0.5-0.1:

- [AWC-CB] When both Dynamic VLAN and IEEE802.1r fast-roaming were enabled, a Dynamic VLAN user may have been disconnected from the AP.
- When an AP was managed by a wireless LAN controller using DHCP option 43, sometimes management of the AP by the AWC controller would be lost and regained repeatedly.
- During MAC Authentication, an AP would sometimes send a RADIUS Request packet with an incorrect attribute resulting in RADIUS Accounting not working correctly.
- When an AP received an IP address from DHCP server, an unnecessary "Start HTTP service" log would be displayed on the console.
- When specifying an encryption key to download a Technical Support file, sometimes the retrieval would fail.
- When WDS was established with Radio3, FDB table entries of more than the maximum (1,025) would be allowed and the AP would reboot.
- When 'Enhanced Open transition mode' was selected for security on VAP0 other than Radio3, 'WPA Enterprise' would incorrectly show as selectable for security on VAP1 of the same Radio.
- [AWC-CB] Restoring a configuration with AWC-CB would fail.
- [AWC-CB] When a wireless client tried to reconnect to an AP, the AP would incorrectly detect an issue and start the recovery operation.
- For firmware 10.0.4-1.1 and later:

  Captive Portal authentication would fail when the following two conditions were met:

  - The AP was registered with a STATIC IP address on the wireless LAN controller.
  - The AP received an IP address from a DHCP server with option 43 that was different to the wireless LAN controller.

  For firmware 10.0.4-2.1 and later:

  - Captive Portal authentication would not work correctly with a Channel Blanket VAP.
- Band Steering would stop working when updates to the steering candidate list failed.
- When the mode was set to IEEE 802.11b/g/n and the bandwidth set to 40Mhz on Radio 1, 1Mbps could not be disabled from the Legacy Rate Set.
- Band steering would not work correctly on Radio 3 if the AP was rebooted with Band Steering enabled.
- When a wireless client was connecting to an AP, band steering functions would be performed unintentionally before the connection was completed. This would result in Band Steering (using IEEE802.11v) not functioning for a while.
- When Radio 3 was enabled, if Band Steering was set to enable, the AP would reboot.
- With Band Steering enabled, steering functions to Radio 3 were not performing correctly.
- [AWC-CB] When a wireless client attempted to connect to an AP while the AP is applying a configuration, occasionally the AP would reboot.

- When Vista Manager mini was used to apply a Passpoint OSU icon file, the process would not finish and the AP configuration would not be completed.
- When the AP was managed by an AWC plugin, the channel setting was Auto instead of Static.
- If the Radio 3 channel was set to Auto, the FILS Discovery frame would not be transmitted.
- Following a FW upgrade, an AP would continuously reboot when applying a CB Profile.
- The Black List would not be deleted when a 6GHz-capable client connected to Radio 2 VAP.
- When Neighbor AP detection is changed from 'Enabled' to 'Disabled', the Neighbor AP list would not be cleared.
- When upgrading from v10.0.4-0.1 or earlier to v10.0.4-1.1, v10.0.4-2.1 or v10.0.4-3.1, the LAN2 port would not link up.
- When Band Steering was enabled, unnecessary functions would be performed.

Known issues

Here are the known issues for the TQ7403 access point version 10.0.5-0.1

- 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.

- 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".
- 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.

Limitations

Here are the limitations for version 10.0.5-0.1:

- 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
- ❒ 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**.