TQ3403 Wireless Access Point
Version 11.0.5-1.1 Software Release Notes

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

Supported Platform

The following access points support version 11.0.5-1.1:

- ❒ TQ3403
- ❒ TQm3403

The firmware filename is:

- ❒ AT-TQ3403-11.0.5-1.1.img
- ❒ AT-TQm3403-11.0.5-0.1.img

For instructions on how to upgrade the firmware on the TQ3403 access point, see the TQ3403 *Access Point Installation Guide* at **www.alliedtelesis.com/library**.

New Features

Here are the new features for the TQ3403 access point version 11.0.5-1.1:

- ❒ 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

- Support for disabling IEEE802.11b Legacy Rates "1, 2, 5.5, 11"on the Radio settings page.
- Support for allowing the selection of Multicast Rates in addition to IEEE802.11b.

Resolved Issues

Here are the resolved issues for the TQ3403 access point version 11.0.5-1.1:

- 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.
- 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.
- 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.
- Fixed an issue where the link speed could downgrade from 2.5G to 1000M, then from 1000M to 100M, when repeatedly linked up and then immediately linked down.
- With SNMP enabled, the AP would sometimes not send authentication failure traps when an incorrect community name was used.
- After a Wi-Fi Schedule Profile was assigned to a radio, further configuration on that radio would result in an incorrect error message appearing and GUI functionality would be affected.
- When sending a request to a switch with LLDP, the AP would request an incorrect power consumption value.

Known issues

Here are the known issues for the TQ3403 access points version 11.0.5-1.1

- 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.
- 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.
- 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 Vista Manager EX applies a configuration to the access point, the LAN port on the access point goes down for three seconds.
- 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.
- 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.
- A beacon will be transmitted with maximum power even when the transmission output power on Radio 1 is set to "Medium".
- IEEE802.11r fast roaming is not supported with the following:
  - WPA Enterprise > Dynamic VLAN
  - AMF Application Proxy
- With Management Frame Protection (MFP) enabled on a VAP, if a duplicate AUTH packet is received, negotiation between the MFP and client will fail. The client will be disconnected, however sometimes a disconnection log will not be output.

Limitations

Here are the limitations for version 11.0.5-1.1:

- 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 Radio 3 (6GHz) is not supported.

Limitations on Performance

Here are the performance limitations for version 11.0.5-1.1:

- Communication sessions between the AP and wireless clients are registered in a high-speed communication table. However, if the table exceeds the maximum of 4096 entries, communication will then be performed by the CPU resulting in a drop in performance.

  The sessions will then be registered using the following information:

  - Source IP address
  - Source port number
  - Destination IP address
  - Destination port number
  - Transport protocol (UDP/TCP)

  When the table maximum is exceeded, the following log will be output:

  kernel notice:ECM connection count exceeds 4096.

  When this occurs, it is recommended to either:

  - reduce the number of wireless clients connected; or
  - place the APs closer together.

Supported Countries

The TQ3403 access point continues to support the following countries:

- Australia
- Austria
- Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia

- ❒ Finland
- ❒ France
- ❒ Germany
- ❒ Greece
- ❒ Hungary
- ❒ Ireland
- ❒ Italy
- ❒ Japan
- ❒ Latvia
- ❒ Lithuania
- ❒ Luxembourg
- ❒ Malta
- ❒ Netherlands
- ❒ New Zealand
- ❒ Poland
- ❒ Portugal
- ❒ Romania
- ❒ Singapore
- ❒ Slovakia Republic
- ❒ Slovenia
- ❒ Spain
- ❒ Sweden
- ❒ Taiwan
- ❒ United Kingdom
- ❒ United States

Contacting Allied Telesis

If you need assistance with this product, visit the Allied Telesis website at **www.alliedtelesis.com/services**.