



TQ7403 Wireless Access Point Version 10.0.4-1.1 Software Release Notes

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

- “Supported Platform,” next
- “New Features” on page 1
- “Specification Changes” on page 3
- “Resolved Issues” on page 3
- “Known Issues” on page 5
- “Limitations” on page 6
- “Supported Countries” on page 6
- “Contacting Allied Telesis” on page 8

Supported Platform

The following access point supports version 10.0.4-1.1:

- TQ7403

The firmware filename is:

- AT-TQ7403-10.0.4-1.1.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 10.0.4-1.1:

Support for new SNMP MIB, including:

- Standard MIB
 - Support HOST-RESOURCES-MIB
 - Support ENTITIY-MIB
 - Support ENTITIY-SENSOR-MIB
- Private MIB
 - IP address of associated wireless client.

- NetBIOS name of associated wireless client.
- The total number of associated wireless client
- Radio interface information
- A unique index for each Radio interface
- The radio channel
- The total number of associated wireless client for each radio
- ❑ New Radio mode options:
 - Radio1:
 - IEEE 802.11b/g/n
 - Radio2:
 - IEEE 802.11a/n
 - IEEE 802.11a/n/ac
- ❑ Support for Client Isolation per VAP
- ❑ Support for AMF auto recovery
 - AMF auto recovery is taken from the AMF master. See the *AMF Plus Feature Overview and Configuration Guide* for more information about configuring auto recovery and AMF Plus.
- ❑ Support Wi-F Scheduler
 - This feature allows you to change the status of Radios and VAPs relating to a schedule that you create. In Notice point, the wireless restart will be done on the wireless AP when the schedule is running.
- ❑ Support for Authentication Page Language for Captive Portal Click Through
- ❑ Support Two-step authentication for MAC Access Control and Captive Portal
 - This field shows on the MAC Access Control page only if Captive Portal is enabled.
- ❑ A new RFScan method when Neighbor AP Detection is enabled, allowing the scanning method and scan time to be configured. One of the following scan methods can be selected:
 - All Channel (Default setting)
 - One Channel
- ❑ 'All Channel' scans the entire band. The scan interval is every 5 minutes.
- ❑ 'One Channel' scans one selected channel.
- ❑ When 'One Channel' is selected, the user can configure:
 - Scan interval:
 - Scan duration:
 - Data keep time
- ❑ Added the following fields for timeout processing for RADIUS requests on the Security > WPA Enterprise and MAC Access Control > External RADIUS pages:
 - RADIUS Timeout
 - RADIUS Retransmit
 - Retry interval for Primary

- ❑ The Syslog buffer size has been changed from 64kb to 4MB.
- ❑ Improvements to configuring Passpoint settings via the GUI.
- ❑ Frequency information has been added to both the Associated Client page, and the Neighbor AP page of the web-based Device GUI.
- ❑ DHCP request packets are sent when an AP reconnects to update its address.

Specification Changes

The following specification changes were added to version 10.0.4-1.1 for the TQ7403 wireless access point:

- ❑ The Syslog buffer size has been changed from 64kb to 4MB
- ❑ Improvements to configuring Passpoint settings via the GUI.
- ❑ Frequency information has been added to both the Associated Client page, and the Neighbor AP page of the web-based Device GUI.
- ❑ DHCP request packets are sent when an AP reconnects to update its address.

Resolved Issues

Here are the limitations for the TQ7403 access point version 10.0.4-1.1:

- ❑ When an access point's system time was corrected by the wireless controller's management, the wireless controller's statistics and the number of connected clients were not displayed.
- ❑ To use the Passpoint feature, you must set required fields; however, the following required fields could be saved without any values:
 - NAI Realm information
 - Operator Friendly Name
 - OSU SSID
 - OSU Providers Server

Even though the access point issues the error message "One or more fields contain invalid values!," it still saves the settings without values.

- ❑ Sometimes, when enabling Radio 1 and/or Radio 3 on the AP, beacons would sometimes be lost.
- ❑ VAP1's setting did not return to default when VAP0's security settings changed from Enhanced Open Transition Mode to Other Security.
- ❑ When multicast to unicast conversion was enabled, APs would block multicast frames that were received over a wired connection.
- ❑ The access point occasionally rebooted when a large number of log files were output.
- ❑ When Management VLAN Tag was enabled, VLAN-related interface information would incorrectly be included in the Interface MIB.
- ❑ When accessing a neighbor AP list with a private MIB, an SNMP process would sometimes restart.

- ❑ MAC Address Filtering did not work after an AP reboot.
- ❑ In rare cases, an AP may have unexpectedly rebooted repeatedly.
- ❑ The access point would occasionally fail to move channels when a radar was detected on channels that are generally reserved for radar.
- ❑ Beacons that included AC parameters were showing with no value for WMM Information Element.
- ❑ QR Code information would not display if the "View QR code" button was clicked repeatedly.
- ❑ A wireless client would fail to connect to the access point using PMKSA cache.
- ❑ Abnormal memory usage may have occurred when Dynamic VLAN was enabled.
- ❑ On APs, Samba would work unintentionally.
- ❑ The access point may have rebooted when wireless client disconnected while transmitting DELBA frames.
- ❑ The cipher suite became empty when both Passpoint was Enabled, and WPA and WPA2 were used.
- ❑ Occasionally, the access point could not get an IP address from the DHCP server after applying configuration.
- ❑ The maximum number of Realm Names than can be assigned is 10. It was possible to add more than 10 Realm Names and the VAP would then become unavailable.
- ❑ In passpoint settings, when NAI realm entries were 10 or more, the access point would reboot.
- ❑ After initially connecting using PMKSA cache, if reauthentication occurred by the RADIUS server, the log would show it was reauthenticated using the PMKSA cache.

Known Issues

Here are the known issues for the TQ7403 access points version 10.0.4-1.1:

- ❑ 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.
- ❑ 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 RADIUS 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 IEEE802.11k is enabled, for some access points with Hidden SSID enabled, information is not shared correctly.
- ❑ Invalid numbers for VLAN ID starting with "0" are allowed to be saved & applied instead of rejected.
- ❑ 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.

Limitations

Here are the limitations for version 10.0.4-1.1:

- 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 Radio3 (6GHz) is not supported.

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
- 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 © 2024 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.