AT-TQ v3.4.0 Series Wireless Access Points Software Release Notes

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

- ❒ “Supported Platforms” on page 1
- ❒ “Limitation” on page 1
- ❒ “Management Software Filenames” on page 2
- ❒ “New and Enhanced Features” on page 2
- ❒ “Resolved Issues” on page 2
- ❒ “Known Issues” on page 3
- ❒ “Contacting Allied Telesis” on page 5

Note:
The firmware passed the testing program for Global Availability and is approved for use in live or production environments.

Supported Platforms

Version 3.4.0 of the AT-TQ Series Management Software is supported on the following AT-TQ Series access points:

- ❒ AT-TQ2450 (P/N: 990-003821-00)
- ❒ AT-TQ2450-60 (P/N: 990-003821-60)
- ❒ AT-TQ3600 (P/N: 990-003881-00)
- ❒ AT-TQ4400e (P/N: 990-004879-00)
- ❒ AT-TQ4400e-01 (P/N: 990-004879-01)
- ❒ AT-TQ4600 (P/N: 990-004633-00)
- ❒ AT-TQ4600-01 (P/N: 990-004633-01)

For instructions on how to upgrade the management software on the access points, see the latest version of the AT-TQ Series Management Software User’s Guide, available on the Allied Telesis web site at www.alliedtelesis.com.

Limitation

Version 3.4.0 of the AT-TQ Series Management Software complies to the CE and AS/NZS certificates for using the optional antennas and cables supported for the AT-TQ4400e model; however, it is *not* designed to comply to FCC/IC certificates for the optional antennas and cables for the AT-TQ4400e model.

Management Software Filenames

See the table for the filenames of the management software for your access points.

Table 1: Management Software Filenames

AT-TQ2450	AT-TQ2450-3.4.0.b03.img
AT-TQ2450-60	AT-TQ2450-3.4.0.b03.img
AT-TQ3600	AT-TQ3600-3.4.0.b03.img
AT-TQ4400e	AT-TQ4400e-3.4.0.b03.img
AT-TQ4400e-01	AT-TQ4400e-3.4.0.b03.img
AT-TQ4600	AT-TQ4600-3.4.0.b03.img
AT-TQ4600-01	AT-TQ4600-3.4.0.b03.img

New and Enhanced Features

This release adds the following enhanced features:

- Airtime Fairness (ATF) - ATF gives the same amount of airtime to each client regardless of the communication speed.
- Fast multicast transmit rate - The option Fast is added. When you select Fast, the system uses the lowest rate among the rates in which the associated clients send frames to the VAP.
- RSSI indication - The system displays RSSI for each associated client.
- Disabling sending RTS frames - When the RTS threshold value 65535 is selected, sending RTS frames is disabled. The threshold value 65535 is added.
- WDS and AT-UWC controller - The access point's WDS configuration is effective even after the AT-UWC controller manges the access point.
- The country code Taiwan - The country code Taiwan is added for the wireless setting; however, the country code is preset and cannot be changed for the US model.
- PoE+ and LLDP-MED - The AT-TQ4400e and AT-TQ4600 models is able to negotiate PoE+ power using LLDP-MED.

Resolved Issues

The following issues are resolved in this release:

- Transmit counters - The access point incremented the transmit counters during boot-up. This issue is resolved.
- Client in the power saving mode - The AT-TQ4400e and AT-TQ4600 models failed to send wireless frames to an associated client in the power saving mode. This issue is resolved.
- Clustering system - The clustering system failed to use eligible channel settings. This issue is resolved.
- Automatic channel assignments for the access points of the cluster - This function did not work properly. This issue is resolved.
- Untagged frames and VLAN ID - The access point forwarded untagged frames from the LAN port to VAPs when the VLAN ID is the same as the management VLAN ID. This issue is resolved.

- Language setting - When the display language setting is changed, the access point did not automatically refresh to display the page in the selected language. This issue is resolved.
- 802.11ac client with MFP (Management Frame Protection) - The access point failed to send MFP-enabled de-authentication frames to 802.11ac clients with MFP. This issue is resolved.
- Inactivity timer for a client - The inactivity time for a client failed when the client is in the power saving mode. This issue is resolved.
- Access point abnormal shutdown - The access point shut down unexpectedly when managed by the AT-UWC controller. This issue is resolved.
- IGMP packets - IGMP general query packets were sent out from the LAN port periodically. This issue is resolved.
- Wireless to wireless communications - Continuous wireless to wireless communications over long time periods failed. This issue is resolved.
- De-authentication frame - The access point transmitted de-authentication frames during wireless interface initialization. This issue is resolved.
- Pre-authentication - Pre-authentication failed when using a specific RADIUS server. This issue is resolved.
- Pre-authentication - Pre-authentication stopped working after the security mode is changed from WPA-Personal to WPA-Enterprise. This issue is resolved.

Known Issues

Here are the known issues in this release.

- SNMP walk - Performing an SNMP walk on an access point in a heavy traffic environment.might cause the unit to stop forwarding traffic.
- RADIUS accounting - The access point assigns the same RADIUS accounting session ID number to a client that leaves and reconnects within three seconds.
- View Neighboring Access Points windows - The Neighbor Details window for cluster members does not display the VAP1-15 SSID numbers. The Neighbor Details window for non-cluster members does include the SSID numbers.
- Dynamic VLANs and IEEE 802.1x authentication - Wireless clients who are assigned their VIDs from a RADIUS server and are authenticated with IEEE 802.1x might require two attempts to successfully connect to the network.
- Maximum frame size - The access point can handle packets up to 1549 bytes. The access point discards packets equal to or larger than 1550 bytes.
- LAN port - The access point might drop packets on the radios when the LAN port is operating at 100% capacity.
- UWC and channel lists - The access point does not validate channel lists from a UWC. An access point might operate in an unpredictable manner if it receives an incompatible channel list from a UWC.
- Network Time Protocol (NTP) client - When the NTP client is enabled, the access point synchronizes its time with the server whenever its IP address lease on a DHCP server expires, even when it is assigned the same IP address.
- Error packet counter - The error packet counter does not work correctly.

- Wireless Distribution System (WDS) bridge and MAC address filter - Do not use the MAC address filter on an access point that is part of a WDS bridge. The filter might not work correctly.
- Legacy Rate Sets - It might not be possible to ping an access point that has four enabled Legacy Rate Sets. This issue does not occur when an access point has greater or less than four enabled Legacy Rate Sets.
- WDS bridge and VAP0 encryption - Access points of a WDS bridge that have different encryption settings on their VAP0 VLANs might transmit unnecessary packets.
- Cluster feature - All the access points of a cluster should be the same model and have the same version of operating system. Otherwise, the cluster might not operate correctly.
- IEEE 802.11a/n/ac - You must reset the AT-TQ4400e or AT-TQ4600 access point when you change the 5 GHz radio from IEEE 802.11a to IEEE 802.11a/n/ac.
- Country setting - You must reset the access point after changing the country setting. A new country setting does not take effect until the unit is reset.
- Cluster feature - Clusters should not have more than sixteen units. Clusters with more than sixteen units may experience problems.
- WPA/WPA2 Enterprise - Authentications of wireless clients who roam across different VLANs might fail if the VLAN security is WPA or WPA2 Enterprise and the RADIUS server is using the Network Access Protection facility.
- Primary and secondary images - If the primary operating system image on the access point is v1.2.0 or earlier and the secondary image is v2.0.1 or later, switching the images with the Switch button in the Manage Firmware window automatically disables the following features:
  - Modulation and Coding Scheme (MCS) data rate setting in the Modify Radio Settings window.
  - WDS Managed Mode setting in the Configure Managed Access Point Parameters window
  - WDS Managed Ethernet Port setting in the Configure Managed Access Point Parameters window
- Management Framework (AMF) v5.4.6-01 - AT-TQ Series access points with management software v3.3.0 or later are not fully compatible as guest nodes with AMF v5.4.6-01.

Contacting Allied Telesis

If you need assistance with this product, you can contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- 24/7 Online Support — Enter our interactive support center to search for answers to your product questions in our knowledge database, to check support tickets, to learn about RMAs, and to contact Allied Telesis technical experts.
- USA and EMEA phone support — Select the phone number that best fits your location and customer type.
- Hardware warranty information — Learn about Allied Telesis warranties and register your product online.
- Replacement Services — Submit a Return Merchandise Authorization (RMA) request via our interactive support center.
- Documentation — View the most recent installation and user guides, software release notes, white papers, and data sheets for your products.
- Software Downloads — Download the latest software releases for your managed products.

For sales or corporate information, go to **www.alliedtelesis.com/purchase** and select your region.