TQ1402 Series Wireless Access Point
Version 6.0.2-0.1b Software Release Notes

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

Supported Platforms

The following access points support version 6.0.2-0.1b:

- AT-TQ1402
- AT-TQm1402

For instructions on how to upgrade the management software on wireless access points, refer to the *Management Software for TQ1402 and TQm1402 Wireless Access Points User Guide*.

Documents are available on the Allied Telesis website at **www.alliedtelesis.com/library**

The version 6.0.2-0.1b firmware filenames are listed here:

- AT-TQ1402-6.0.2-0.1b.img.zip
- AT-TQm1402-6.0.2-0.1b.img.zip

Resolved Issues

The following issues have been resolved in version 6.0.2-0.1b:

- Access Points sometimes output "Connection Success" logs even when the connection failed when wireless clients executed duplicate authentication on VAPs with MFP Enabled.
- In rare cases, if an invalid management frame was sent from a wireless client, an unintended reboot may have occurred.

- AT-Vista Manager EX sometimes showed a configuration application failure when configuration was applied to AP from the application.
- Wireless clients could not connect to the AP when they would repetitively connect and disconnect without Captive Portal authentication while Captive Portal was Enabled on a VAP.
- While applying configuration that changed the username and password of AP in AWC, when accessing the Web-GUI of the access point, the user and password changed by the AWC could be lost.
- When a RADIUS query received no response from the primary RADIUS server, the query was re-sent after 3 seconds, but failed over to the secondary RADIUS server without waiting for timeout after that re-send.
- If a large amount of debug logs were output continuously at short intervals, they could temporarily consume large amount of memory and the AP would reboot.
- When the AP's system time was advanced and time was corrected by the wireless controller's management, the wireless controller's statistics and number of connected clients were not displayed.
- Web authentication could not be completed when another wireless client with the same IP address as the IP address of another wireless client, that had previously performed web authentication, performed web authentication.
- The recovery process from a wireless module error detection sometimes failed, resulting in memory depletion and a reboot due to internal processing errors.
- When Dynamic VLAN was enabled, a reboot would sometimes occur.
- The access point occasionally rebooted when a large number of log files were output.
- When wireless clients would connect with PMKSA cache, reauthentication would not be performed as per the time set in the session-timeout section of RADIUS.
- After initially connecting using PMKSA cache, if reauthentication occurred by the RADIUS server, the log would show it was reauthenticated using the PMKSA cache.
- After initially authenticating using PMK, if the session timed out and the device was reauthenticated using RADIUS, the log would show it was reauthenticated using PMK.
- A reboot may have occurred when PS-Poll control frame was received from a wireless client that had not shifted to Power-Saving mode.

Known Issues

Here are the known issues for version 6.0.2-0.1b:

- Access points do not synchronize Hostname and SNMP System Name.
- In the Technical Support Information, a note states the 801.1x authentication log contains the user ID, but not the password. Neither user IDs nor passwords are included.
- The IP address of the secondary RADIUS server is blank, and the setting can be applied with string set to the key of the secondary RADIUS server.
- Access points might disconnect inactive clients several seconds before the expiration of the Inactivity Timer.

- Do not use the disconnect button of Associated Client page in Web-GUI to disconnect when using Wireless Distribution System (WDS) children.
- In rare instances, the hardware and software tables may develop inconsistencies that can cause access points to reset. This is entered in the log as “kernel: Rebooting due to DMA error recovery.”
- EngineBoots and EngineTime values of SNMPv3 Trap are sent with 0.
- IPv6 wireless clients with Router Advertisement enabled, do not communicate on Dynamic VLAN VAP.
- When you Enable more than 7 VAPs and set WPA Personal, the AP cannot associate over 117 wireless clients on Radio1.
- [Single Channel] Access points sometimes output a “Disassociate” log without a reason code on Single Channel VAP when the AP disassociates with a wireless client.
- [AWC-SCL] The LED behavior is not changed after the AWC-SCL Cluster setting is changed from Enabled to Disabled.
- [AWC-SCL][AWC-CB] The access point would sometimes output a “Removing STA due to association advertisement” log, even if STA Roaming has not occurred on Single Channel VAP(Channel Blanket VAP). (Log only).
- [AWC-SCL] [AWC-CB] Access points might output a "Connection" log which included the RADIUS server's IP address when a wireless client re-connects to a Single Channel VAP(Channel Blanket VAP) using PMK cache.

Limitations

Here are the limitations for the TQ1402 Series Access Points version 6.0.2-0.1b management software:

- LLDP is not supported.
- OpenFlow is not supported, but GUI has OpenFlow tab.
- Maximum Client is limited to 120 on Radio1. (Radio2 is 200)
- Radio1 cannot select WPA3 when set WPA Enterprise.
- “WPA3 and WPA2” can only be selected with WPA Personal.
- Proxy ARP is not supported, but GUI has Proxy ARP contents on Advanced Settings tab.
- Ethernet Link sometimes up/down occurred during AP booting.

Limitations for Combination with Easy Setup

The following specifications are for Easy Setup:

- Radio and VAP0 must have following settings when AP selects VAP Mode: Cell Type
  - Radio1 Radio: Basic Settings > Mode: IEEE 802.11 b/g/n
  - Radio2 Radio: Basic Settings > Mode: IEEE 802.11 a/n/ac
- Radio1/Radio2 VAP0 settings:
  - Basic Settings > Security > Mode: WPA Personal

  - Basic Settings > Security > WPA Version: WPA2 and WPA3
  - Basic Settings > Security > Cipher Suites: CCMP
  - Basic Settings > Security > IEEE802.11w (MFP): Enabled
- Radio and VAP0 must have following settings when AP selects VAP Mode: Single Channel Type
  - Radio2 Radio: Basic Settings > Mode: IEEE 802.11 a/n/ac
  - Advanced Settings > Maximum Client: 500
  - Radio1/Radio2 VAP0: Basic Settings > Security Mode: WPA Personal
  - Basic Settings > Security WPA Version: WPA2
  - Basic Settings > Security Cipher Suites: CCMP
  - Basic Settings > Security IEEE802.11w (MFP): Disabled
  - Advanced Settings > Association Advertisement: Enabled
- Single Channel Type can only be selected when AWC-SCL Cluster setting is enabled
  - Control frame for Single Channel Mode changes according to the management VLAN tag setting of the AP.
  - Management VLAN is disabled: Control frame is untagged frame.
  - Management VLAN is enabled: Control frame is tagged frame which is the same as Management VLAN ID.

Specifications for AWC-SCL Cluster

The following specifications are for AWC-SCL:

- AWC-SCL Cluster does not share following configurations:
  - Host Name.
  - Mac Address
  - IP Address setting
  - SNMP > System Name/System Contact/System Location
  - Channel and Transmission Power when VAP0 mode is “Cell Type”.
  - Transmission Power when VAP0 mode is “Single Channel Type”.
- The number of supported established AWC-SCL Cluster members is 5.
- The AP cannot be managed from AT-Vista Manager EX/(Vista mini) when AWC-SCL Cluster is enabled.
- When using AWC-SCL Cluster and Single Channel, when an AP is replaced by another AP with a new MAC address, configuration will be reapplied for all cluster APs. If a wireless client is already connected to the AP, the AP will disconnect all clients to perform this.
- Limitation for AP setting using Easy Setup:
  - Combination with Easy Setup and AT-Vista Manager EX/(AWC Lite) is not supported
- Limitation for AP setting using Single Channel Type: The Change Radio setting is not supported.

- If the Radio setting is not default value, change Radio setting to default value before setting the Single Channel Type.
- The Change Radio2VAP0 setting is not supported from “Settings > VAP/Security” page.
- If Radio2VAP0 setting is not default value, change Radio2VAP0 setting to default value before setting the Single Channel Type.
- * However, the parameters described in the Specification are excluded.
- Use APs with the same “Single Channel group ID” on APs on different networks in the near wireless spatial is not supported
- Setting to Management VLAN ID and Control VLAN ID 1 is not supported.
- Establish Single Channel Mode AP with over 6 APs is not supported.
- It is possible to establish Single Channel, however it is not supported.
- Single Channel Type VAP’s BSSID is used largest Mac address of AWC-SCL Cluster’s member.

Supported Countries

Version 6.0.2-0.1b management software supports the following countries:

- Australia
- Austria
- Belgium
- Bulgaria
- Canada
- China
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hong Kong
- Hungary
- India
- 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, the Services & Support section of the Allied Telesis website at **www.alliedtelesis.com/services** has links to the following technical services:

- Helpdesk (Support Portal) - Log onto Allied Telesis interactive support center to search for answers to your questions in our knowledge database, check support tickets, learn about Return Merchandise Authorizations (RMAs), and contact Allied Telesis technical experts.
- Software Downloads - Download the latest software releases for your product.
- Licensing - Register and obtain your License key to activate your product.
- Product Documents - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.
- Warranty - View a list of products to see if Allied Telesis warranty applies to the product you purchased and register your warranty.
- Allied Telesis Helpdesk - Contact a support representative.

To contact a sales representative or find Allied Telesis office locations, go to **www.alliedtelesis.com/contact**.