TQ1402 and TQm1402 Wireless Access Points Version 6.0.2-0.1 Software Release Notes

Please read this document before using the management software. Listed here are the document sections:

Supported Platforms

The following wireless access points support Version 6.0.2-0.1:

- TQ1402
- TQm1402

Firmware Files

The firmware filenames are listed here:

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

Instructions for upgrading the management software are in the *TQ1402 Series Wireless Access Points Management Software User's Guide*, available from the Allied Telesis Inc. web site at **www.alliedtelesis.com/us/en/services-support.**

New Features

The following new features are added to the TQ1402 and TQm1402 Version 6.0.2-0.1 access points:

- Session Key Refresh Rate
- Session Key Refresh Action
- User ID is added as an 802.1x authentication log entry
- Captive Portal: Virtual IP address
- Captive Portal: RADIUS accounting
- Captive Portal: Walled garden
- Captive Portal: Authentication page redirection
- Captive Portal: Centralized authentication

Resolved Issues

The following issues were resolved in the Version 6.0.2-0.1 for the TQ1402 and TQm1402 access points:

- The access point had 802.11 Frame Aggregation and Fragmentation vulnerability issues.
- The access point did not share the authentication result for Captive Portal under AWC plug-in management.
- When the Captive Portal setting was changed from External RADIUS to Click-through via AWC plug-in, the access point might have been rebooted unexpectedly.
- Enabling Fast Roaming with Dynamic VLAN was enabled changed the VLAN ID of wireless clients.
- When Captive Portal was enabled or WPA Enterprise security was selected, the access point re-authenticated wireless clients every one hour even though the session key refresh rate was set to zero.
- When WPA Enterprise security was selected, the access point re-authenticated wireless clients every one hour even though RADIUS session timeout was set to longer than one hour.
- Even when Management Frame Protection was enabled, Duplicate AUTH Received functioned.
- The access point might have replied an incorrect value to an OID 1.3.6.1.2.1.17.4.3.1.1 request.
- Neighbor AP Detection (SyncScan) might not have worked when Radio 2.4GHz was disabled.
- Reset Button was not able to be disabled via AWC with Vista Manger Mini.
- Setting different IP Addresses and Secret values to AMF Application Proxy Server for VAPs via AWC Plug-in might have caused the access point to reboot unexpectedly.
- AWC Plug-in might not have been able to manage the access point after it was disconnected from AWC Plug-in.

- The quarantine log messages sent by AMF Application Proxy included unexpected characters.
- The access point might have shut down when wireless clients connected and disconnected repeatedly.
- When the access point with Channel Blanket received a packet from a wireless client at the same time as a Radio disconnection process run, the access point might have been rebooted. (only TQ1402)
- When firmware was upgraded, the access point issued an unnecessary log message: Division by zero in kernel. (only TQ1402)
- The access point might not have communicated to a wireless client when the wireless client using more than one TID repeated handover. (only TQ1402)
- The access point issued an unintended log message when Channel Blanket was used. (only TQ1402)
- When the access point with its maximum number of wireless clients opened the Associated Client page, the access point might have been rebooted unexpectedly. (only TQ1402)
- When trying to collect technical support information, the access point might have been rebooted unexpectedly. (only TQ1402)
- When a wireless client using WPA-PSK (TKIP) connected to the access point with Channel Blanket, after handover, the wireless client was not able to communicate to access points. (only TQ1402)
- When Radio 2 was changed to Single Channel Mode, the access point might have dropped its throughput. (only TQ1402)

Specification Changes

The following changes are made to the specifications in the TQ1402 and TQm1402 Version 6.0.2-0.1 management software:

- The default value of the RSSI threshold for AWC-SCL was changed from 0dBmto 30dBm. (TQ1402 only)
- The Tx power displayed on the Status page was changed from a dBm value to max, high, middle, low, or min.
- Issuing an SA timeout query log

  When a valid SA Query Response is received from a wireless client within the SA Query timeout, the access point issues a an SA timeout query log entry.
- Association advertisement is supported when Channel Blanket or AWC-SCL is selected. (TQ1402 only)
- The session timeout values are shared among the access points when Fast Roaming is used.

Limitations

Here are the limitations for the TQ1402 and TQm1402 Version 6.0.2-0.1 management software:

- ❐ LLDP is not supported.
- ❐ OpenFlow is not supported.
- ❐ The maximum number of wireless clients that Radio1 supports is 120 clients. (200 clients for Radio2)
- ❐ WPA3 is not an option when WPA Enterprise is selected on Radio1.
- ❐ The WPA3 and WPA2 option can be selected only when WPA Personal is selected.
- ❐ Proxy ARP is not supported.
- ❐ A link on the Ethernet port goes up and down when the access point is rebooting.

Limitations on Single Channel Type

- ❐ Changing Radio settings is not supported.

  Before setting a Radio to the Single Channel type, set the Radio as default.
- ❐ Changing the Radio2 VAP0 settings is not supported from the Settings > VAP/Security page.

  Before setting Radio2 VAP0 to the Single Channel type, Radio2 VAP0 must be in the default settings except the parameters listed in “Specifications and Limitations on AWC-SCL Cluster” on page 6.
- ❐ Using the same Single Channel Group ID as access points using in different networks in the near wireless spatial is not supported.
- ❐ Management VLAN ID and Control VLAN ID 1 are not supported.
- ❐ Establishing more than six access points in Single Channel Mode is not supported.
- ❐ The BSSID of the Single Channel Type VAP with the largest MAC address among the members of AWC-SCL Cluster is used for the BSSID for all members.

Limitations on Channel Blanket

When Channel Blanket Radio is Enabled

- ❐ Changing the RTS threshold is not supported.
- ❐ Airtime Fairness is not supported.

When Channel Blanket VAP is Enabled

- ❐ Changing the Broadcast Key Refresh Rate is not supported.
- ❐ RADIUS Accounting is not supported.
- ❐ Fast Roaming is not supported.
- ❐ Pre-authentication is automatically disabled.
- ❐ Dynamic VLAN is automatically disabled.
- ❐ The Session-Timeout RADIUS attribute is automatically disabled.

- Captive Portal is automatically disabled.
- Changing the Inactivity Timer value is not supported.

Channel Blanket Settings

- The Management VLAN ID and Control VLAN ID settings are not supported.
- The VAP VLAN ID and Control VLAN ID settings are not supported.

Wireless Clients' Behavior on Channel Blanket

- Communications of wireless clients are interrupted when the access point is turned off or reboots. It takes approximately two minutes for the wireless clients connected to the access point that was turned off or rebooted to restore communications.

Specifications and Limitations on Easy Setup

Here is a list of specifications and limitations for Easy Setup:

- When the VAP mode is set to Cell Type, the Radio and VAP0 settings must be configured as follows:
  - Radio1 setting
    Basic Settings > Mode: IEEE802.11b/g/n
  - Radio2 setting
    Basic Settings > Mode: IEEE802.11a/n/ac
  - VAP0 setting for both Radio1 and Radio2
    Security > Mode: WPA Personal
    Security > WPA Version: WPA2 and WPA3
    Security > Cipher Suites: CCMP
    Security > IEEE802.11w (MFP): Enabled
- When the VAP mode is set to Single Channel, the Radio and VAP0 settings must be configured as follows:
  - Radio2 setting
    Basic Settings > Mode: IEEE802.11a/n/ac
    Advanced Settings > Maximum Client: 500
  - VAP0 setting for both Radio1 and Radio2
    Basic Settings > Security Mode: WPA Personal
    Basic Settings > Security WPA Version: WPA2
    Basic Settings > Security Cipher Suites: CCMP
    Basic Settings > IEEE802.11w (MFP): Disabled
    Advanced Settings > Association Advertisement: Enabled
- Single Channel can be selected only when AWC-SCL Cluster is enabled.

- ❐ The Control Frame setting in the Single Channel mode is automatically changed based on the Management VALN Tag settings of the access point.
  - Management VLAN is disabled: Control Frame setting is changed to untagged frame.
  - Management VLAN is enabled: Control Frame setting is changed to tagged frame, which is the same as Management VALN ID.
- ❐ When Easy Setup is used, Vista Manager EX or Vista Manger Mini is not supported.

Specifications and Limitations on AWC-SCL Cluster

Here is a list of specifications and operational notes for AWC-SCL Cluster:

- ❐ The access points in AWC-SCL share the configuration except:
  - Host Name
  - MAC address
  - IP address settings
  - SNMP system name, system contact, and system Location
  - Transmission power when VAP0 mode is set to the Single Channel Type.
- ❐ The maximum number of AWC-SCL members is five.
- ❐ The access points in AWC-SCL cannot be managed by Vista Manager EX or Vista Manager mini.
- ❐ When the access point in AWC-SCL and the Single Channel type is added to AWC-SCL as a device replacement, the configuration re-apply process automatically runs if the access point has the largest MAC address among the cluster members. As a result, the wireless clients that had been connected to the access point are all disconnected.

Known Issues

- ❐ Access points do not synchronize Hostname and SNMP System Name.
- ❐ When only one access point with Channel Blanket enabled is up and running, wireless clients are not able to communicate with the Channel Blanket VAP correctly.
- ❐ The access point might save the Secondary RADIUS Server Key value as empty.
- ❐ Access points might disconnect inactive clients several seconds before the Inactivity Timer expires.
- ❐ Do not disconnect clients on WDS children using the Associated Client window in the web browser interface. The results may be unpredictable.
- ❐ 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.”
- ❐ When Dynamic VLAN is enabled, the access pint returns a wrong value to the OID: 1.3.1.2.1.17.4.3.1.1 (MAC address information) request.
- ❐ When Management Frame Protection (MFP) is enabled, MFP disconnects a wireless client, who requests multiple connections; however, a successful connection log message is issued incorrectly.

- Radio1 supports up to 117 wireless clients when seven VAPs are set to WPA Personal.
- The access point in Single Channel mode might issue a disassociation log message without a reason code. (TQ1402 only)
- The System LED did not correctly reflect a change to the enabled or disabled status of the AWC-SCL feature. (TQ1402 only)
- The access point in Single Chanel mode generated extraneous “Removing STA due to association advertisements” event messages in the system log. (TQ1402 only)
- When a wireless client re-connects to Single Channel VAP using PMK cache, the access point might issue a connection log message including RADIUS Server IP address. (TQ1402 only)
- The access point might issue an unnecessary log message: Removing STA due to association advertisement when a wireless client is connected to the access point. (TQ1402 only)

Contacting Allied Telesis

If you need assistance with this product, the Services & Support section of the Allied Telesis web site at **www.alliedtelesis.com/services-support** 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**.

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.