



TQ6000 GEN2 Wireless Access Points Version 8.0.3-0.2 Software Release Notes

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

- “Supported Platforms,” next
- “New Features” on page 2
- “Enhancements” on page 3
- “Resolved Issues” on page 3
- “Specifications Changed” on page 5
- “Specifications Changed for the Access Point with Channel Blanket” on page 5
- “Specifications for the Access Point with Smart Connect” on page 5
- “Specifications for the Access Point with Smart Cluster” on page 6
- “Specifications for Easy Setup” on page 7
- “Limitations” on page 8
- “Limitations for the Access Point with Channel Blanket” on page 8
- “Limitations for the Access Point with Smart Connect (AWC-SC)” on page 9
- “Limitations for the Access Point with Smart Cluster (AWC-SCL)” on page 9
- “Limitation for Configurations Using Easy Setup” on page 10
- “Known Issues” on page 10
- “Contacting Allied Telesis” on page 12

Supported Platforms

The following access points support version 8.0.3-0.2:

- TQ6702 GEN2
- TQm6702 GEN2
- TQ6602 GEN2
- TQm6602 GEN2

For instructions on how to upgrade the management software on the TQ6000 GEN2 wireless access point, see the *TQ6000 GEN2 Wireless Access Point Management Software User's Guide*, available on the Allied Telesis Inc. website at www.alliedtelesis.com/support.

The firmware filenames are:

- ❑ AT-TQ6702GEN2-8.0.3-0.2.img
- ❑ AT-TQm6702GEN2-8.0.3-0.2.img
- ❑ AT-TQ6602GEN2-8.0.3-0.2.img
- ❑ AT-TQm6602GEN2-8.0.3-0.2.img

New Features

Version 8.0.3-0.2 added the following new features:

- ❑ Passpoint
- ❑ AMF Auto-Recovery
 - AMF Auto-Recovery can be configured only via AMF Master controller.
- ❑ Inter VAP wireless client isolation
 - This security feature blocks wireless clients in different VAPs from communicating each other even when the VAPs have the same VLAN ID setting on the same radio.
- ❑ AWC-Smart Connect (SC)
 - AWC-SC is available only to the TQ6702 GEN2 and TQ6602 GEN2 access points.
 - AWC-SC can be configured only via Vista Manager EX or Vista Manager Mini.
- ❑ AWC-Smart Cluster (SCL)
 - AWC-SCL is available only to the TQm6702 GEN2 and TQm6602 GEN2 access points.
 - AWC-SCL is enabled by default.
 - The Single-channel function on Radio 1 and Radio 2 can be enabled at the same time.
 - Configuration can be done from the Easy Setup page.
 - SSID and password are initially generated.
 - The AWC-SCL channel is automatically selected.
- ❑ Wildcard entries in Walled Garden
 - When the DNS Proxy for Walled Garden is enabled, the access point performs as a DNS proxy upon receiving DNS frames from wireless clients.
- ❑ Channel Blanket and MU-MIMO can be enabled at the same time.
- ❑ Channel Blanket and OFMDA can be enabled at the same time.
- ❑ Channel Blanket and Dynamic VLAN can be enabled at the same time.
- ❑ The Two-step authentication for MAC Access Control with Captive Portal
 - This feature can be configured even when Captive Portal is enabled.
 - This feature is disabled, either MAC Access Control or Captive Portal continues to allow wireless clients to communicate.
 - This feature is enabled.
- ❑ AWC-Sky Defender (SDF)

- ❑ Airtime Fairness percentage control per VAP
 - The “Manual” option is added to the Airtime Fairness configuration, which can be set on a Radio page.
 - Setting the Airtime Fairness with the “Manual” option lets you specify the Pre-allocated Airtime Percentage value in the Advanced Settings page for each VAP.
- ❑ WPA Enterprise WPA2/WPA3 Transition mode
 - This transition mode is available only to the VAPs with Channel Blanket disabled.

Enhancements

Version 8.0.3-0.2 added the following enhancements:

- ❑ Wireless clients with the static IP address can connect to Proxy ARP-enabled VAPs.
- ❑ Wireless clients with the static IP address can connect to VAPs with both Channel Blanket and Proxy ARP enabled.

Resolved Issues

Here are resolved issues in version 8.0.3-0.2:

- ❑ The access point with one of the following country codes was not able to be managed through Vista Manager EX:
 - Dynamic VLAN
 - China
 - Hong Kong
 - India
 - Malaysia
 - Singapore
 - Thailand
 - Vietnam

Note

The access point with an unsupported country code, such as Colombia or Brazil, cannot be managed through Vista Manager EX. Contact Allied Telesis Customer Support for further information.

- ❑ The access point did not change the WDS setting when Vista Manager EX applied the WDS setting on Radio2.
- ❑ The access point stopped sending beacons for Radio2 when the LAN2 configuration was changed while Radio2 was enabled and the Radio2 channel was set to “Auto.”
- ❑ The access point sent SNMPv3 traps with an extra “0” in OID.
- ❑ The access point occasionally shut down when learning the IP address of a wireless client from Proxy ARP.
- ❑ The access point accepted more than 50 items in Walled Garden.

- ❑ The access point occasionally failed to broadcast frames when one or more of the following functions were enabled on the access point:
 - Dynamic VLAN
 - Virtual IP Address for Captive portal
 - AMF Application Proxy
 - WDS
- ❑ LLDP requested an invalid maximum power consumption to the access point.
- ❑ A Radio was turned on and off continuously after the access point enabled the VAP ID 10.
- ❑ Enabling Static LAG increased the access point's CPU usage when the LAN1 and LAN2 ports received broadcast and/or multicast frames simultaneously.
- ❑ The user password might have been lost when the access point's Web User Interface was accessed while AWC Plug-in was applying settings.
- ❑ A RADIUS server failover log was issued on the access point with no Secondary RADIUS Server defined when the RADIUS request timeout expired.
- ❑ The access point occasionally failed on RADIUS Server failover for MAC Authentication.
- ❑ The access point occasionally disconnected wireless clients when detecting abnormalities in the wireless chip.
- ❑ The access point did not issue RADIUS request timeout logs for MAC Authentication when the access point defined only Primary RADIUS Server for MAC Authentication.
- ❑ The SNMP system name was reset to the default value when the access point restored the configuration.
- ❑ The access point occasionally shut down when a wireless client connected to the access point with RADIUS Accounting enabled.
- ❑ [AWC-CB] The access point with Channel Blanket enabled might have issued unnecessary disconnect logs.
- ❑ The access point occasionally shut down when the access point with a Proxy ARP-enabled VAP received an ARP request frame in which the source IP address was 0.0.0.0 and the destination IP was 0.0.0.0.

Here are resolved issues applied only for the TQ6702 GEN2 and TQ6602 GEN2 access points:

- ❑ [AWC-CB] Fast Roaming IEEE802.11r failed on the Channel Blanket VAP when a wireless client roamed between Channel Blanket Groups, which have a different Channel Blanket Control VLAN.
- ❑ [AWC-CB] Wireless clients occasionally were not able to communicate if some of wireless clients connected to the Channel Blanket access point at the same time.
- ❑ [AWC-CB] The Channel Blanket access point occasionally disconnected wireless clients when more than 200 wireless clients were connected to the access point.
- ❑ [AWC-CB] The Channel Blanket access point occasionally failed to send broadcast and/or multicast frames to wireless clients.
- ❑ [AWC-CB] Association Advertisement did not function correctly on a VAP with the access point mode when the access point enabled a Channel Blanket VAP.
- ❑ [AWC-CB] Hand-over occasionally failed when both Channel Blanket and Mac Access Control were enabled.

Specifications Changed

Here is the specification changed in version 8.0.3-0.2:

- ❑ On Airtime Fairness, Enabled is changed to Evenly.

Specifications Changed for the Access Point with Channel Blanket

Here are specifications changed on the access point with Channel Blanket (AWC-CB):

- ❑ The access point is specified to reboot when Vista Manager EX applies configurations on Channel blanket to the access point. The access point reboots when:
 - Vista Manager EX applies the Channel Blanket profile settings to the access point for the first time.
 - Vista Manager EX applies the Channel Blanket profile settings to the access point in standalone.
 - Vista Manager EX removes the access point from Channel Blanket.

The following log is issued when the access point reboots for the above reasons:

```

cwmmd[xxx]: CWM: APMgr[xxx]: AP XX:XX:XX:XX:XX:XX reboots for applying
configuration
  
```

Specifications for the Access Point with Smart Connect

Here are specifications on the access point with Smart Connect (AWC-SC):

Note

The specifications in this section are applied only to the TQ6702 GEN2 and TQ6602 GEN2 access points.

- ❑ The access point is specified to reboot when Vista Manager EX applies configurations on Smart Connect to the access point. The access point reboots when:
 - Vista Manager EX applies the Smart Connect profile settings to the access point for the first time.
 - Vista Manager EX applies the Smart Connect profile settings to the access point in standalone.
 - Vista Manager EX removes the access point from Smart Connect.

The following log is issued when the access point reboots for the above reasons:

```

cwmmd[xxx]: CWM: APMgr[xxx]: AP XX:XX:XX:XX:XX:XX reboots for applying
configuration
  
```

Specifications for the Access Point with Smart Cluster

Here are specifications on the access point with Smart Cluster (AWC-SCL):

Note

The specifications in this section are applied only to the TQm6702 GEN2 and TQm6602 GEN2 access points.

- ❑ The AWC-SCL cluster can be established among the same models only. No clusters can be established in combination of the TQm6702GEN2 and TQm6602GEN2 models.
- ❑ The access point reboots with an exception when the Radio setting is changed from the Single Channel mode to the Cell mode or from the Cell mode to the Single Channel mode.

The access point reboots in the following cases:

- Case1: Radio1 is changed from the Single Channel mode to the Cell mode.
Radio2 is changed from the Single Channel mode to the Cell mode.
- Case2: Radio1 is changed from the Cell mode to the Single Channel mode.
Radio2 is changed from the Cell mode to the Single Channel mode.
- Case3: Radio1 is in the Cell mode.
Radio2 is changed from the Cell mode to the Single Channel mode

The access point does not reboot in the following case:

- Case4: Radio1 is changed from the Single Channel mode to the Cell mode.
Radio2 is in the Single Channel mode.

- ❑ One AWC-SCL cluster can have up to ten access points.
- ❑ The frames that the access point in the Single Channel mode controls depends upon the management VLAN tag setting:
 - When Management VLAN is disabled, the controlled frames are untagged frames.
 - When Management VLA is enabled, the controlled frames are tagged frames with the same VLAN ID as the Management VLAN ID.
- ❑ The access points in the AWC-SCL cluster do not share the following values:
 - Host Name
 - Mac Address
 - IP Address settings
 - SNMP system location (SNMP > System Name/System Contact/System Location)
 - Channel and Transmission Power when VAP0 is in the Cell mode
 - Transmission Power when VAP0 is in the Single Channel mode
- ❑ When Radio1 is in the Single Channel mode, the BSSID value of the Radio1 VAP15 is considered as the MAC address of Radio1 VAP0. Do not enable Radio1 VAP15 or use Radio1 VAP15 for wireless communication.

- ❑ The BSSID value of a VAP in the Single Channel mode is considered as the MAC address and used to determine which VAP has the largest MAC address among the AWC-SCL Cluster's members.
- ❑ Automatic Channel Selection functions only when Radios in the access points are in the Single Channel mode. Channel Coordination runs among the access points in clusters in the same Layer 2 network. Channel Coordination does not run on the access points in other than the Single Channel mode. Rebooting the access point does not always re-activate Automatic Channel Selection.
- ❑ By default, in the access point with AWC-SCL:
 - Client Isolation: Disabled
 - RSSI Threshold: 30

Specifications for Easy Setup

The following specifications are for Easy Setup:

- ❑ The access point can be configured using either Easy Setup or Vista Manager EX (AWC Lite), but not both of them.
- ❑ The Radios and VAP0 must have the following settings for the access point to select the VAP Mode: Cell Type on the Ease Setup page:
 - Radio1 Radio: Basic Settings > Mode: IEEE802.11 b/g/n/ax
 - Radio2 Radio: Basic Settings > Mode: IEEE 802.11 a/n/ac/ax
Advance Settings > Maximum Client: 200
 - Radio1/Radio2 VAP0: 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
Advanced Settings > Association Advertisement: Disabled
- ❑ The Radios and VAP0 must have the following settings for the access point to select the VAP Mode: Single Channel Type on the Ease Setup page:
 - Radio1 Radio: Basic Settings > Mode: IEEE802.11 b/g/n/ax
 - Radio2 Radio: Basic Settings > Mode: IEEE 802.11 a/n/ac/ax
Advance Settings > Maximum Client: 200
 - 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

Limitations

Here are the limitations for the TQ6000 GEN2 access points version 8.0.3-0.2:

- ❑ Changing value of the RTS threshold is not supported.
- ❑ Wireless Distribution System (WDS) and MU-MIMO / OFDMA cannot be enabled at the same time.
- ❑ AWC-SC and NU-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).

Limitations for the Access Point with Channel Blanket

Here are the limitations when using Channel Blanket (AWC-CB):

Note

All Allied Telesis firmware including Channel Blanket have the same limitations as the firmware version 8.0.3-0.2 for TQ6000 GEN2 access points.

- ❑ Limitations on the access point:
 - Enabling Band steer on the access point is not supported.
 - The Change Duplicate AUTH received setting is not supported.
 - Only Duplicate AUTH:ignore is supported.
 - The same radio settings are required on all access points under Channel Blanket.
 - Changing the LAN2 port configuration is not supported.
 - Enabling WDS is not supported.
 - Enabling AMF Application Proxy is not supported.
 - Enabling AWC-SC VAP is not supported.
- ❑ Limitations on enabling Blanket Radio Interface:
 - Changing the RTS setting is not supported.
 - Enabling Airtime Fairness is not supported.
- ❑ Limitations on Enabling Channel Blanket VAP:
 - Changing Broadcast Key Refresh Rate is not supported.
 - Changing Session Key Refresh Rate is not supported.
 - Changing the Session Key Refresh Action setting is not supported.
 - Enabling RADIUS Accounting is not supported.
 - Pre-authentication is forced to be disabled.
 - The Session-Timeout RADIUS attribute is forced to be disabled.
 - Changing Inactivity Timer is not supported.
 - IEEE802.11w (MFP) should be disabled.
- ❑ Limitations on the Channel Blanket settings:

- Setting Management VLAN ID and Control VLAN ID is not supported.
- Setting VAP VLAN ID and Control VLAN ID is not supported.
- ❑ Limitations on Channel Blanket behavior
 - Communications of wireless clients are affected when the access point is turned off or rebooted.
 - It takes approximately two minutes to restore the communications of wireless terminals connected to the access point that is powered off.

Limitations for the Access Point with Smart Connect (AWC-SC)

Here are the limitations when using Smart Connect (AWC-SC):

- ❑ Limitations on the access point:
 - Enabling Management VLAN on the access point is not supported.
 - Enabling WDS is not supported.
 - Changing the Static LAG/LACP/Cascade configuration on LAN2 port is not supported.
 - Enabling Channel Blanket is not supported.
 - Enabling Dynamic VLAN is not supported.
- ❑ Limitations on enabling the Smart Connect Radio Interface:
 - Enabling the Neighbor AP Detection feature is not supported.
 - Enabling MU-MIMO is not supported.
 - Enabling OFDMA is not supported.
 - Changing the Client Isolation settings is not supported.
- ❑ Limitations on the other items except the access point and Smart Connect Radio Interface:
 - The Smart Connect feature and AMF guest cannot be used at the same time.
 - The Smart Connect feature on the access point and DHCP Snooping feature on the switch cannot be used at the same time.

Limitations for the Access Point with Smart Cluster (AWC-SCL)

Here are the limitations when using the Smart Cluster feature:

- ❑ Limitation on the access point:
 - If a Single Channel Group ID has been already used on access points in another network in your near wireless spatial, the access point with the same Single Channel Group ID in your network is not supported.
- ❑ Limitations on enabling the AWC-SCL Single-Channel Radio Interface:
 - The Radio must be in the default settings. Reset the Radio to the default settings before setting the Radio to the Single Channel type.
 - Changing the VAP0 setting from “Settings > VAP/Security” page is not supported when the VAP0 mode is Single-Channel Type. Reset VAP0 to the default settings before setting the Radio to the Single Channel type.

- Changing configurations from the Easy Setup page is not supported when the Bandwidth has other than 20 MHz on the Radio settings.
 - To configure the Radios as the single channel mode from the Easy Setup page, the Radio settings on the access point must be the default settings.
 - When the access point is configured as the Single-Channel mode in Radio 1, changing the settings from the Settings > VAP/Security > Radio 1 > VAP0 and VAP15 pages is not supported.
 - When the access point is configured as the Single-Channel mode in Radio2, changing the setting from the Settings > VAP/Security > Radio 2 > VAP0 page is not supported.
 - When the access point is configured as Single-Channel mode, changing configurations from the Easy Setup page is not supported if VAP0 is not in the default settings.
- Limitations on the other items except the access point and Single-Channel Radio Interface:
- AWC Plug-in cannot manage the access point during building an SCL cluster. AWC Plug-in can manage the access point after it has built an SCL cluster; however, the SCL feature is not available for the access point under the AWC Plug-in management. The configurations made from the Easy Setup page on the access point is overwritten with configurations by AWC Plug-in. Therefore, the Cluster status on the access point is disabled when AWC Plug-in accesses the access point.
 - DHCP option 43 is not supported. The AWC-SCL Cluster is disabled when the access point receives an IP address via DHCP with the option 43.
 - AMF Auto-Recovery is not supported with AWC-SCL. When AMF Auto-Recovery tries to restores configurations on the access point, which AWC-SCL operates on, the AMF Auto-Recovery sequence might fail.

Limitation for Configurations Using Easy Setup

Here is a limitation when using the Easy Setup

- Configuring the access point with both Easy Setup and Vista Manager EX is not supported.

Known Issues

Here are the known issues for the TQ6000 GEN2 access points version 8.0.3-0.2:

- The Radar Detecting Channel List is cleared when a radio setting is changed.
- A LAN port takes approximately 30 seconds to start communications after it links up.
- When the access point is powered with the AC adapter, a LAN port might take one minute to link up after the cable is connected or disconnected.
- The wireless client's static IP is not supported when Proxy ARP is enabled on a VAP.

- ❑ The access point transmits the following illegal frames to other LAN ports when Cascade connection is enabled:
 - Frames with the same Source and Destination MAC addresses
 - Frames with the source MAC address as the 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 shows WEP even when it is OSEN. OSEN is a security option, which can be used when Passpoint is enabled.
- ❑ On the VAPs where Dynamic VLAN is enabled, IPv6 communication does not function when IP Auto-configuration of IPv6 Router Advertisement is enabled.
- ❑ Even when only the primary RADIUS server is specified, a following log can be issued: "RADIUS No response from Authentication server IP ADDRESS:PORT - failover."
- ❑ When a wireless client in the power saving mode does not respond to the access point, the wireless client will be disconnected before the inactivity timer expires.
- ❑ A LAN port goes down for three seconds when a configuration is applied to the access point from Vista Manager EX.
- ❑ The access point occasionally fails to be managed by Vista Manager EX right after the access point boots up.
- ❑ While the access point is configured with the management VLAN tag enabled and the VLAN ID set to 1, the VLAN setting of the LAN port of the switch connected to the access point is changed from tagged 1 setting to untagged 1, the switch still can communicate with the access point for several minutes.

The following issues are applied only to the TQ6702 GEN2 and TQ6602 GEN2 access points:

- ❑ RADIUS Authentication fails when the RADIUS key contains "¥".
- ❑ (AWC-CB) The access point might report to Vista manage EX less than the actual number of associated wireless clients.
- ❑ When the access point is initialized with the Reset button, a log indicating "Expected Rebooting due to factory reset by reset button" is duplicated in the reboot.log of the access point.
- ❑ Fast roaming IEEE802.11r with MAC access control and Distributed System cannot be enabled at the same time.

The following issues are applied only to the TQm6702 GEN2 and TQm6602 GEN2 access points:

- ❑ (AWC-SCL) The cluster is occasionally deconstructed temporarily when a change is made on the settings on the VAP page of the AWC-SCL cluster constructed access point. The cluster is automatically reconstructed after deconstructed.
- ❑ (AWS-SCL) When an AWC-SCL cluster is built for the first time, the "Synchronize settings from" status might show to an access point as "Not Synchronized." When the status is displayed, you need to restart the access point with the "Not Synchronized" status.

Contacting Allied Telesis

If you need assistance with this product, visit the Allied Telesis web site at www.alliedtelesis.com/support.

Copyright © 2023 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.