



TQ1402 Series Wireless Access Point Version 6.0.2-1.1 Software Release Notes

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

- ☐ “Supported Platforms,” next
- ☐ “New Features” on page 1
- ☐ “Specification Changes” on page 2
- ☐ “Resolved Issues” on page 1
- ☐ “Known Issues” on page 3
- ☐ “Limitations” on page 3
- ☐ “Limitations for Combination with Easy Setup” on page 4
- ☐ “Specifications for AWC-SCL Cluster” on page 4
- ☐ “Supported Countries” on page 6
- ☐ “Contacting Allied Telesis” on page 7

Supported Platforms

The following access points support version 6.0.2-1.1:

- ☐ 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 6.0.2-1.1 firmware filenames are listed here:

- ☐ AT-TQ1402-6.0.2-1.1.img.zip
- ☐ AT-TQm1402-6.0.2-1.1.img.zip

New Features

Support for the following new features has been added:

- ☐ Support for verifying RADIUS packets. This feature prevents RADIUS protocol forgery attacks and is available in Settings > VAP/Security on the following pages:
Settings > VAP/Security:

- Security > Mode: WPA Enterprise
- MAC Access Control > MAC Access Control:

- External RADIUS
- MAC Address List + External RADIUS

Captive Portal > Captive Portal:

- External RADIUS
- External Page Redirect

If you are using a local RADIUS server on an AlliedWare Plus router or switch, the AlliedWare Plus device must be running version 5.5.4-2.1 or later.

Specification Changes

The following specification changes have been made:

- ☐ To increase security, the device GUI and Captive Portal authentication page cannot be accessed using:
 - 3DES encryption
 - TLSv1.0, TLSv1.1 or TLSv1.2.

Resolved Issues

The following issues have been resolved in version 6.0.2-1.1:

- ☐ A user could obtain a SNMP MIB with an invalid community name.
- ☐ When Neighbor AP Detection was enabled, unnecessary Notice logs for ieee80211_rcv_beacon_ap_nnn from the kernel would be output.
- ☐ When accessing a neighbor AP list with a private MIB, an SNMP process would sometimes restart.
- ☐ When an AP Profile with security WEP and Key Type "ASCII" was applied, the radio wave output of the access point would stop and wireless clients would be disconnected.
- ☐ When the Captive Portal page was viewed over HTTPS, the Captive Portal page would sometimes become inaccessible.
- ☐ When specifying an encryption key to download a Technical Support file, sometimes the retrieval would fail.
- ☐ A reboot could be observed when a device was roaming between different wireless interfaces within the same access point.
- ☐ If the radio wave output stopped after detecting radar on all DFS target channels, and the radio setting was disabled, the AP would sometimes reboot.
- ☐ An internal program would sometimes fail to release memory which would lead to insufficient memory and an automatic reboot.

Known Issues

Here are the known issues for version 6.0.2-1.1:

- ❑ 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 6.0.2-1.1 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 6.0.2-1.1 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**.

Copyright © 2025 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc. Allied Telesis and the Allied Telesis logo are trademarks of Allied Telesis, 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. 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. 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. has been advised of, known, or should have known, the possibility of such damages.