AT-UWC v3.4.0
Software Release Notes

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

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 Series management software is supported on the following AT-UWC Series products:

- ❒ AT-UWC-BaseST (P/N: 990-000232)
- ❒ AT-UWC-60-APL-10 (P/N: 990-003883-10)
- ❒ AT-UWC-60-APL-30 (P/N: 990-003883-30)
- ❒ AT-UWC-60-APL-40 (P/N: 990-003883-40)
- ❒ AT-UWC-60-APL-50 (P/N: 990-003883-51)

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

Management Software Filename

The management software filename is given here;

at-uwc-3.4.0-B03.i386.rpm

Supported Access Points

You can use the AT-UWC v3.4.0 controller to manage 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)

Note:
To ensure full compatibility, you should install AT-TQ Series v3.4.0 or v3.4.1 management software on the access points before managing them with the AT-UWC v3.4.0 controller.

New and Enhanced Features

Here are new and enhanced features:

- ❒ Airtime Fairness (ATF) - You can use the AT-UWC controller to enable/disable ATF on the wireless network.
- ❒ Fast multicast transmit rate - You can use the AT-UWC controller to specify the option Fast as the multicast transmit rate for the network. The access point in the network uses the lowest rate among the rates in which the associated clients send frames to the VAP.
- ❒ Disabling sending RTS frames - You can use the AT-UWC controller to disable the access point sending RTS frames. When the RTS threshold value 65535 is selected, the access point disables sending RTS frames. The threshold value 65535 is added.
- ❒ Captive portal syslog - The user ID is added to the syslog messages.
- ❒ Integrated OUI database - It is updated.

Resolved Issues

Here are the resolved issues in this release:

- ❒ Additional HTTP port and HTTP secure port in CP Global Configuration page - These ports were not supported. This issue is resolved. They are supported.
- ❒ The peer controller - The automatic channel and power assignment of the peer controller did not work properly when the peer controller manages more than 26 access points.

Known Issues

Here are the known issues in this release.

- ❒ Distributed tunneling and dynamic VLANs - Wireless clients who roam across multiple access points in distributed tunneling environments may experience problems. They are assigned to static VLANs in the access points rather than dynamic VLANs from a RADIUS server.
- ❒ Wireless Network Configuration - WEP page - When configuring WEP security, you must set the WEP Key Type and WEP Key Length before the WEP keys. Changing the key type or length requires reentering the WEP keys.
- ❒ Log time stamps - The log time stamps in event logs for “Idle Timeout” events for wireless clients in Captive Portals are incorrect. This issue is limited to the AT-TQ3600 Access Point.
- ❒ CP Web Customization (Authentication Page) - The “Denied Message” option in the page does not work.

- Log - The controller does not correctly update the log when it ends client sessions because of idle or session timeouts. This applies to wireless clients who are authenticated by a RADIUS server in Captive Portals.
- CP Configuration page - The User Logout Mode option in the page might not work correctly for wireless clients using a Captive Portal in a UWC cluster environment. Clients who roam to a peer controller from a cluster controller might not be able to log out using the “Logout pop-up.”
- SNMP - The controller returns no value or the wrong value for the following SNMP objects:
  knownClientDatabaseRadiusServerStatus
  wsManagedAPDistTunnelBytesReceived
- Managed Access Point Neighbor Client Status page - This page lists wireless clients that should have “Associated to this AP” in the Discovery Reason column as “RF Scan.”
- TimeZone object - The controller does not correctly update the Set/Change Time Zone log when the time zone is manually set with the TimeZone object.
- Network Visualization - The controller deletes the icons of non-managed access points from the graph when it discovers them.
- Upgrading the controller software - The controller might not be able to boot up if you try to upload new firmware to it when its storage disk is full. You should check to be sure the storage disk has adequate space before uploading new firmware.
- Managed Access Point Radio Status Detail page for the 5GHz radio - The controller does not correctly update the “Time Since Radar Last Detected” for 5GHz radios in access points that are managed by peer controllers.
- Access Point Profile List page - The UWC continues to display the message “Apply In Progress” on the screen if you apply a profile in this page to an access point that becomes unreachable or unavailable before the process is completed.
- WDS Group Status page - The controller might increment the Deleted WDS Links Count statistic in the page when you change or delete Wireless Distribution System (WDS) settings.
- Network visualization - The option “Graph located device to the detected location” does not work with access point icons.
- Network visualization - The icon of a satellite access point managed by a peer controller might be incorrectly displayed as gray (unknown).
- Associated Client Status pages - Do not use the Disassociate or Disassociate All buttons in the Associated Client Status pages across a WDS bridge to disassociate wireless clients. It might cause the WDS bridge to fail.
- HTTPS and network visualization - The controller might display the message “Web session has expired” if you log on using HTTPS and open the network visualization feature.
- SNTP Global Status page - The controller does not correctly update the Last Update Time value in the page.
- Managing wireless clients - The controller might experience problems if multiple network managers add, modify, or delete the same wireless clients at the same time.
- Network visualization and Java security - The Network Visualization feature is not compatible with “Mixed code security verification” in Java security. You must disable the security feature on your computer to use network visualization.
- Captive Portal configurations - The controller supports the following Captive Portal configurations:

- Configuration 1: If the management VLANs of the UWC and access points have the same VID number, the VAP must have the same VID number.

- Configuration 2: If the management VLANs of the UWC and access points have different VID numbers, the VAP can have any supported VID number.

- Invalid parameter values - The controller does not verify the values for many parameters. It might accept invalid values for some parameters, which can result in unpredictable operations of features. In other cases it might reject invalid values but not display error messages.
- Rogue access points - Access points that are configured not to transmit their SSIDs will be labeled as rogue units if the “AP without a SSID” option is enabled in the WIDS AP Configuration page.
- Access Point Profile QoS Configuration page - When setting the cwMin and cwMax parameters in the page, set the cwMin value first. Setting the cwMax value first might result in an error message.
- Distributed tunnels and VLANs - Wireless clients who roam in distributed tunnel environments cannot change VLANs until the Distributed Tunnel Idle Timeout value in the Distributed Tunneling Configuration page has expired. The default value for the Distributed Tunnel Idle Timeout parameter is 120 seconds.
- The AT-UWC WLAN Controller software product does not support external network adapters or 10/100Mbps adapters.
- VAPs and web browser pages - The controller might display some web browser pages incorrectly when there are sixteen defined VAPs.
- Status tab in the Associated Client Status page - The controller might not correctly update the “Detected IP address” information in the Status tab in the Associate Client Status page when you click the Refresh button.
- Centralized L2 Tunneling and UWC clustering features - Do not use the Centralized L2 Tunneling feature with UWC clustering feature. Combining the two features might cause a packet loop in the wired network.
- WIDS AP Rogue Classification page - The Unmanaged AP Detected On Wired Network field in the page does not work. It remains False even when the controller detects a rogue access point that meets the condition.
- AP De-Authentication Attack option - The AP De-Authentication Attack option, which is used to disconnect rogue access points from a network, does not work on all access points. The option is located in the WIDS AP Configuration page.
- Network visualization - Wireless node icons in network visualization might not always display the Vertex label when you position the mouse over them.
- SNMP MIB walk - The controller might experience a problem with the wsOuiTable and wsOuiEntrry objects during an SNMP MIB walk.
- WDS bridges - An access point cannot establish a WDS link if the radio channel is changed in the Managed AP Channel/Power Adjust page.
- ifInOctets object - The ifInOctets object does not count received CRCs.
- Valid Access Point Configuration page - An access point that has an authentication password will stop responding to the controller if you change its AP Mode setting. To avoid the problem, delete the authentication password before changing the AP mode setting.

- WDS bridges - This version of the management software does not support multi-hop WDS bridges. Refer to the latest AT-TQ Series User's Guide for diagrams of supported WDS bridges.
- HTTPS management - Network administrators who access the controller through a Captive Portal whose protocol mode in the CP Configuration page is set to HTTPS can manage the controller with HTTPS even when HTTPS is disabled in the Secure HTTP Configuration page.
- SNMP - The default value for community strings has changed. In v1.x, it was enabled. In v2.0 or later, it is disabled.
- Network visualization - Meter units are displayed as whole numbers. Fractions are rounded, as needed (e.g., 1.2 to 1 or 2.5 to 3).
- Country code - The default country code is JP (Japan).
- RADIUS server - If the RADIUS server is identified in the controller by a host name unknown to the DNS, all managed access points function as stand-alone units and the web browser management interface response becomes slow.
- Managed Access Point Radio Statistics page - The Fragments Received and Fragments Transmitted statistics in the page do not work.
- Network Visualization - The icon of the "RF Scan Sentry AP" changes to red (rogue) if the access point becomes unreachable.
- Multiple network administrators - The controller may experience problems if multiple network administrators configure elements of the program simultaneously.
- Listed here are the maximum numbers of wireless clients that can simultaneously use a web authentication page of a captive portal to log on to a wireless network:
  - The maximum number for the AT-UWC-60-APL product is nine clients.
  - The maximum number for the AT-UWC-BaseST product depends on the server hardware, but can be as many as 240 clients

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.