Cassia Networks Inc.
97 East Brokaw Road, Suite 130
San Jose, CA 95112
support@cassianetworks.com

Cassia AC and Bluetooth Routers 2.0.3

Release Notes

Release date: 11/05/2020

Contents

Release Notes

A. About this Release

This is the 2.0.3 release that applies to the Cassia IoT Access Controller (AC) and Cassia Bluetooth routers. This document provides detailed information on the following: upgrade instructions, notes, fixed bugs, and known issues.

Below is the list of firmware and software versions for this release:

- AC Server software: Cassia-AC-2.0.3.2009022156.zip.gpg
- X1000 firmware: XC1000_2.0.3.2011021146.gz.gpg
- E1000 firmware: E1000_2.0.3.2011021145.gz.gpg
- S2000 firmware: S2000_2.0.3.2011021146.tar.gz

B. Upgrade Notice (Please read this section carefully before upgrading your AC server & router firmware)

- In order to upgrade the Cassia Bluetooth router to 2.0.3 firmware, the user must use a 2.0.3 version of the AC server software.
- The 2.0.3 version of the AC server software is backward compatible with 2.0.2 and 1.4.3

router firmware.

- When upgrading the router firmware in the router's local console, please use the local install file *.gz and turn off the "Verify File Encryption" option.
- When upgrading AC software from version 1.4.3 to version 2.0.2 and above, please make sure the host server has **at least 2GB of free storage available**.
- For container user, if the app uses BlueZ with Gatttool and Bluetoothd (e.g. noble or python Bluetooth lib) instead of the Cassia Bluetooth stack and Cassia RESTful API, please **change 'Cassia Bluetooth Stack' to Close** (default is set to Open) in Bluetooth Setting section of router webpage Config Tab (after upgrading router to version 2.0.2 and above). Otherwise, Bluetooth operations in the app may return a failure.
- For container user, an option to enable and disable container local ssh login is added in Container Tab from 2.0.2 forward. **Container local ssh login was disabled by default** for security reasons. Resetting the router will change this option to the default value.
- For container user, the RESTful API to obtain router configuration from AC (GET http://{your AC domain}/api/cassia/info?mac=<hubmac>) is changed in 2.0.2, **container status will be removed from default API output**, in order to avoid oversized UDP packet problem. Container status can be obtained separately by the same API by setting the following parameter value: 'fields=container'. Please refer to the SDK document for details.
- For container user, from 2.0.2 onward, the **DNS name server in the router will be propagated into container /etc/resolv.conf**. Besides having two default DNS name servers (8.8.8.8 and 114.114.114), the Container will use DNS settings in the Network section of the Router webpage's Config Tab as an additional DNS name server. This is to resolve the issue where two default DNS servers are blocked by a firewall.
- From version 2.0.3, newly installed AC will support MQTT only. CAPWAP will be disabled by default. If you need to connect v1.4.x router which only supports CAPWAP as AC-router protocol with v2.0.3 AC, please enable CAPWAP protocol in the AC settings.
- For AC upgraded from previous release, both CAPWAP and MQTT will be enabled by default. Since TCP based MQTT is more reliable on internet than UDP based CAPWAP protocol, **it is highly recommended to disable CAPWAP in the AC settings if using the Cassia RESTful API to collect device data from AC**.
- From v2.0.3, CORS is disabled by default. Client-side scripts (e.g., JavaScript) are prevented from accessing webpage of AC or router due to security reasons, unless 'Access Control Allow Origin' in AC settings or router configuration tab is set. E.g., When using the Bluetooth debugger in http://www.bluetooth.tech/debugger/, please set 'Access Control Allow Origin' in AC settings and router configuration to * or the exact URL of the requesting page http://www.bluetooth.tech .

C. New Features and Enhancements

Description	Effected Software
BLE device roaming	**AC - E1000/S2000 only**
Avoid 2.4G WIFI interference	**Router**
AC statistic enhancement - API call and results	**AC**

AC retrieve router debug log	**AC**
AC integrated Bluetooth debug tool (full version)	**AC**
VMWare AC image support for Windows OS	**AC**
AC Email notification - notifications for new router online and router online/offline in customer specified group	**AC**
Container enhancement - Support for deleting APP in container	**Router**
Container enhancement - Support for calling HTTP API in container regardless of HTTPS settings on Router webpage	**Router**
Container enhancement - Support 'high speed multiple connection mode' on BlueZ	**E1000/S2000 only**
Scan filter enhancement - Added additional timer for duplicate filter	**Router**
Scan filter enhancement - Added all scan filters to auto selection API	**Router**
MQTT bypass enhancement - Support message rate control and timestamp for advertising packet	**Router**
MQTT bypass enhancement – AWS IoT Core support	**Router**
WIFI enhancement – Now supports "verify and save" for provisioning	**Router**
Cellular enhancement - Added IMEI/IMSI info and support signal strength display for more dongles	**Router**
Cellular enhancement - Integrated speed test tool for on-site debugging	**X1000/E1000 only**
Cellular enhancement - Supports 2 additional Japanese modems	**Router**
LED enhancement - Added 2 more BLE chip LED status indications for scan and connection	**E1000/S2000 only**
Security enhancements – Disabled CORS by default and set 'Access Control Allow Origin' to enable	**AC and Router**
Security enhancements – Support Oauth for Cassia local RESTful API	**Router**
Security enhancements – Mask certificate and key in AC settings	**Router**
UI enhancements – New web login interface	**AC and Router**

D. Fixed Bugs since the last Release

- Fixed lost connection event or notification issue for some routers in combined SSE when AC connects to more than 50 routers.
- Fixed 'High speed multiple connection mode' setting issue for S2000 failure in v.2.0.2.
- Fixed device connection display failure issue when connection history has more than 10000 records.
- Fixed AC online time calculation error on AC router detail tab.
- Fixed container remote ssh failure when HTTPS is enabled AC in v2.0.2.
- Fixed display issue associated with setting of container APP's customized configuration

in v2.0.2.

- For container APP customized configuration, the input fields "type" in JSON changed from mandatory to optional.
- Fixed issue of email notification not being able to handle 2 email addresses in v2.0.2.
- Fixed statistic data display failure issue for local time in UTC -1:00 to UTC -11:00 (North and South America).
- Fixed MQTT router fails to go online in version 2.0.3.2009021827 when WiFi signal is weak and domain name instead of IP is used for AC address.

Additional bug fixes in router firmware version 2.0.3.2011021146:

- Fixed issue of MultiTech CAT-M1 cellular signal strength displaying as 'poor'.
- Fixed remote ssh container login sporadic failure issue due to br0 failure in container.
- Masked certificate/keys on router local webpage.
- Web session now terminated when browser is closed.
- Fixed RESTful API in container 502 issue when AC router connection is lost for 15 mins.
- Fixed BLE link disconnect issue in X1000 due to secure level setting.

E. Known Issues and Restrictions

- If AC and routers are connected through internet, and Cassia RESTful API through AC is called to collect device data, please **disable UDP based CAPWAP protocol in AC settings (set CAPWAP port to Disable)**, **which will enable all routers to communicate with AC through TCP based MQTT only.** Otherwise, there might be packet loss or an incorrect message sequence for device data with a CAPWAP configuration. Sometime API calls might return HTTP 502 or 504 errors, depending on the connection quality of the internet.
- Downgrading router from 2.0.2 to previous firmware version, such as 1.4.3, will require users to reset the router website password. When upgrading back to version 2.0.2 or above, users must login with the original (old) 2.0.2 password.
- The maximum number of SSE connections for one router is 32. Cassia's local RESTful API will return '502 Bad Gateway' when this limit is exceeded. Currently there are 4 type of SSE connections, "/gap/nodes?event=1", "/gatt/nodes?event=1", "/management/nodes/connection-state", and "/gap/rssi". It is recommended to maintain only one stable SSE connection for each type and to close unused SSE by closing HTTP connection. It is not suggested to open and close combined SSE connections very frequently.
- Container status on AC router list webpage is updated in each 'Statistics Report Interval'. When the interval is set longer than 30 seconds, e.g. 5 mins, container status on AC router list will not be updated on a timely basis.
- For the S2000 router, in a situation where the number of received advertising packets is more than 200 per second, it is recommended to use scan filter or pure scan filter to reduce CPU load.
- For the E1000 router, when both BLE chips need to handle an uplink throughput data rate over 10KBps simultaneously, it is recommended to contact Cassia's support team and provide the BLE parameters of the device in order to fine tune performance.
- In order to get a prompt response for discover GATT API operation, router by default will

use cached GATT database which was discovered during previous connection. Connection API parameter discovergatt=0 needs to be specified when user needs the router to read real time GATT service and characteristics from BLE device.

- In AC settings, enabling 'Room-based BT Positioning' or 'Router Auto-selection' will consume additional CPU resource. It is recommended to only enable these features when needed.
- LED enhancement - 2 more BT LED status to indicate scanning and connecting is just for Cassia Bluetooth stack, if customer uses BlueZ, BT LED does not have new status.
- When enabling WIFI 'verify and save' function during provisioning and the WIFI client is set to static IP, if the router does not connect to the WIFI AP with the current settings, it will fall back to WIFI hotspot mode. In this case, the hotspot IP address will have already been changed from the default IP (192.168.40.1) to the new static IP address.
- In Wifi hotspot mode, 'verify and save' button disappears after switching tabs. The button will appear again after refreshing webpage.
- Remote login to container from AC webpage might get failure if AC router connection is very slow in which establishing the ssh connection might need 10~15 seconds. Refreshing Webssh screen or run ssh command 'ssh -p 8001 cassia@abb.cassia.pro' a few seconds later will resolve the problem.
- For Huawei dongle E8372h, subtype 320 is not supported in v2.0.3, only Huawei E8372h-153 or 155 is supported. Other subtypes will be supported in 2.1.0.