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

Cassia AC and Bluetooth Gateways 2.1.1 GA Release Notes

Release date: 2021/11/15

Contents

Release Notes

A. About this Release

This is the 2.1.1 GA release that applies to the Cassia IoT Access Controller (AC) and Cassia's Bluetooth gateways. 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-2.1.1.2111121656.zip.gpg
- X2000 firmware: X2000_2.1.1.2111122257.gz.gpg
- X1000 firmware: XC1000_2.1.1.2108111233.gz.gpg
- E1000 firmware: E1000_2.1.1.2108111233.gz.gpg
- S2000 firmware: S2000_2.1.1.2108171640.tar.gz.gpg

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

- In order to upgrade the Cassia Bluetooth gateway to 2.1.1 firmware, the user must use a 2.1.1 version of the AC software. **2.1.1 AC and gateways will use 'unique port' feature, so make sure TCP port 8883 is opened on firewall for both AC and gateway side before upgrade.**

- The 2.1.1 version of the AC server software is backward compatible with previous gateway firmware versions 2.1.0, 2.0.3, 2.0.2, 1.4.3. **An old version AC will not work properly with the latest 2.1.1 gateway.**
- When upgrading the gateway firmware in the gateway's local console, please use the local install file *.gz and turn off the "Verify File Encryption" option.
- When upgrading AC software, please ensure the host server has **a minimum of 2GB of free storage available**.
- From version 2.0.3, a newly installed AC image will support MQTT only. CAPWAP will be disabled by default. If you need to connect a v1.4.x gateway which only supports CAPWAP as an AC-gateway protocol with a v2.0.3 AC instance, please enable the CAPWAP protocol in the AC settings.
- For AC software upgrades from a 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 the AC**.
- From v2.0.3, CORS is disabled by default. Client-side scripts (e.g., JavaScript) are prevented from accessing the AC or gateway webpages due to security reasons, unless 'Access Control Allow Origin' in the AC settings or gateway configuration tab is set. For example, if using the Bluetooth debugger in http://www.bluetooth.tech/debugger/, please set 'Access Control Allow Origin' in the AC settings and gateway configuration to * or the exact URL of the requesting page http://www.bluetooth.tech .
- From v2.1.0, in return message of scan API through AC, parameter name ('event type') has been changed from 'evt_type' to 'evtType'. This is to keep consistence with local API in which 'evtType' is used. For example, {"bdaddrs":[{"bdaddr":"E1:D2:F8:F9:82:E0","bdaddrType":"random"}],"adData":"02010000000000000000000000","name":"(unknown)","rssi":-29,"**evtType**":0}
- Container 2.0.0 can only be installed on gateway firmware 2.1.1 and later version. Previous container versions (1.1.1, 1.2.0) can still be installed on gateway firmware 2.1.1. and later version.

C. New Features and Enhancements

Description	Affected Software
Consolidated AC Management port – Only TCP port 8883 is needed for v2.1.1 gateways, CAPWAP is supported	**AC/All Gateways**
AC event log– add user name for each operation	**AC**
AC statistic– 5 mins sampling granularity for last 1 day, and 1 hour granularity for the last 3 months	**AC**
AC device history – extend historical device connection logs to 7 days	**AC**
Multiple AC server viewer	**AC**

Gateway is automatically configured when connected to AC during initial setup process	**AC**
Allow user to configure gateway name in the local console	**AC/All Gateways**
AC UI – allows gateway to be assigned up to 3 groups	**AC**
BLE Debug Tool upgraded to v2	**AC**
Container – sudo upgrade to version 1.9.5p2-1	**X2000/X1000/E1000**
Container– support user defined delete_app.sh script	**X2000/X1000/E1000**
Scan filter– option to add timestamp in scan result	**AC/All Gateways**
Scan filter– display connectable devices only	**AC/All Gateways**
Scan filter– Value Filter without offset	**AC/All Gateways**
Support Huawei modem 8372h-320/820 (EU)	**All Gateways**
JQuery upgrade from version 1.2.0 to 3.5.1	**All Gateways**
Dropbear upgrade from version 2016.74 to 2017.75	**All Gateways**
Suspend console login after 5 failed attempts, auto release after 15 minutes	**AC/All Gateways**
Support web console password expiration	**AC/All Gateways**
BLE– support data length extension (DLE)	**E1000/S2000**
Cellular enhancement – when auto recovery option is ON and gateway is in AC managed mode, gateway will be rebooted if cellular connection can not be recovered in 1 hour.	**All Gateways**
Filter enhancement – AC combine SSE support scan filters (name, mac, value, duplicate filters)	**AC**

Additional updates in X2000_2.1.1.2110291527.gz.gpg

BLE– support data length extension (DLE)	**X2000**
Support for the 4G modem Soracom Onyx Dongle SC-QGLC4-C1	**X2000**

D. Fixed Bugs since the last Release

- Fixed gateway group name, allow the underscore character to be used..
- MQTT connection and API request optimization to reduce frequent gateway online/offline events in the AC console.
- Wi-Fi connectivity optimization to improved WiFi connection stability.
- Improve accuracy of AC server's CPU load calculation.
- Fixed issue of S2000 web session expires immediately after login.
- Fixed issue of Wi-Fi LED not turning off after disabling Wi-Fi.
- Fixed issue of losing email notification for gateway online status change.
- Fixed issue of supporting BLE tool bluepy in container of X2000.
- Fixed issue of losing BLE connection sporadically in v2.1.0 X2000.
- Fixed log size control issue of cellular 'auto recovery' function.
- Remove /nohup.out log of container app.
- Fixed sporadic issue of X1000 firmware upgrade failure.

Additional updates in Cassia-AC-2.1.1.211105170 and X2000_2.1.1.2111091130:

- Fixed issue that email address with '-' is not permitted in the AC.
- Fixed issue that alarm email of online/offline group is sent when AC notification is OFF.
- Fixed issue that AC gateway list page shows '{Template Error}' after upgrading to 2.1.1
- Fixed issue of AC CPU load increasing due to handling > 50K connection history records, and changed size limitation of connection history to 7 days or 100K records.
- Fixed vulnerability issue of Weak Cipher Suite (CVE-2016-2183: 64-bit block cipher 3DES vulnerable to SWEET32 attack) on the AC server.
- Fixed issue of incomplete BLE 5 extended advertise packet in X2000 scan output.
- Fixed CROS setting failure with * and character / in the local console page.

E. Known Issues and Restrictions

- If the AC and gateways are connected through the internet, and the Cassia RESTful API through the AC is called to collect device data, please **disable UDP based CAPWAP protocol in the AC settings (set CAPWAP port to Disable), which will enable all gateways to communicate with the AC through TCP based MQTT only**. Otherwise, there might be packet loss or an incorrect message sequence for device data with a CAPWAP configuration. Oftentimes the API calls might return HTTP 502 or 504 errors, depending on the connection quality of the internet.
- The maximum number of SSE connections for one gateway is 32. Cassia's local RESTful API will return '502 Bad Gateway' when this limit is exceeded. Currently, there are 4 types 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 connections by closing the HTTP connection. It is not recommended to frequently open and close combined SSE connections.
- Container status on AC gateway list webpage is updated in each 'Statistics Report Interval'. When the interval is set longer than 30 seconds, e.g., 5 mins, the container status on the AC gateway list will not be updated in a timely basis.
- For the S2000 gateway, in situations where the number of received advertising packets is greater than 200 per second, it is recommended to use "scan filter" or "pure scan filter" to reduce the CPU load.
- In order to get a prompt response for discover GATT API operation, the gateway by default will use cached GATT database which was discovered during previous connection. Connection API parameter discovergatt=0 needs to be specified when the user needs the gateway to read real-time GATT service and characteristics from the BLE device.
- In the AC settings, enabling 'Room-Based BT Positioning' or 'Gateway Auto-Selection' will consume additional CPU resource. It is recommended to enable these features only when needed.
- LED enhancement – 2 additional BT LED status indicators for scanning and connecting have been added in support of Cassia's Bluetooth stack. If using BlueZ, BT LED will not display new status behavior.

- When enabling the Wi-Fi ‘verify and save’ function during provisioning and the Wi-Fi client is set to static IP, and if the gateway does not connect to the Wi-Fi AP with the current settings, it will fall back to Wi-Fi 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 Wi-Fi hotspot mode, ‘verify and save’ button disappears after switching tabs. The button will appear again after refreshing the webpage.