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

Cassia User Manual

Release date: March 9, 2023

Contents

Version: EN-2023039-YJ

1. What is a Cassia Gateway?

The Cassia Bluetooth Gateway is a long-range enterprise Bluetooth gateway that can be used for indoor and outdoor environments. It extends the range of Bluetooth connectivity up to 1 kilometer and enables remote control of up to 40 Bluetooth low energy devices without requiring any changes to Bluetooth end devices.

The Cassia Bluetooth gateway acts as a protocol gateway, which translates between the Bluetooth protocol and the Internet Protocol (IP) protocol. This enables your Bluetooth low energy devices to be remotely accessible and controllable via an Internet application.

From firmware 1.3 onwards, Cassia provides container support for the Cassia Bluetooth Gateway E1000, X1000, and X2000 where users can run custom applications.

1.1. Cassia X2000

Cassia launches the new X2000 Bluetooth gateway to deliver secure, long-range, multiple device connectivity for enterprise-grade IoT applications. It is designed to further improve the performance and reduce the complexity and cost of large-scale Industrial IoT deployments. X2000 features Bluetooth Low Energy 5.0 support, a ruggedized IP66 enclosure, integrated TPM chip, more power/Wi-Fi/antenna options, larger memory, and various enhancements.

Cassia X2000 Bluetooth Gateway

The X2000 extends Bluetooth connectivity up to 400 meters for Bluetooth 4.x and 1 kilometer for Bluetooth 5.0 in open space using a patented filtering and smart antenna array. Furthermore, the range extension does not require replacing existing Bluetooth Low Energy end devices, nor is it dependent on Bluetooth Mesh. In bi-directional mode, the X2000 can pair and connect up to 40 end devices. In broadcast/advertising mode, it can listen to hundreds of end devices.

X2000 supports the full functionality of Bluetooth Low Energy 5.0, including higher data rates (2M PHY), advertising extensions, and long range. X2000 also offers flexible Bluetooth

configuration and two state-of-the-art Bluetooth modes: pure scan and high speed multiple connection modes. Pure scan offers the best scan performance in high noise floor and situations with a large number of Bluetooth devices. High speed multiple connection mode optimizes the connection performance when receiving data from multiple Bluetooth devices simultaneously.

X2000 supports edge computing, which can improve response time, reduce the cost of data transmission & cloud service, improve reliability, security, and scalability. X2000 can run large custom applications in its Ubuntu container. The container and APP can use up to 700 MB memory in X2000, which is much larger than X1000 & E1000 (128 MB).

X2000 has a TPM (Trusted Platform Module) chip embedded. It can support secure boot, trusted boot, secure storage, and other crypto-chip-based security functions. TPM can further enhance X2000's security level.

Cassia's X2000 can be used as a protocol gateway, which translates between Bluetooth protocol and IP protocol. The X2000 Internet Protocol (IP) backhaul options include Ethernet, 2.4GHz/5GHz Wi-Fi, and USB cellular modem. As a result, Bluetooth end devices are remotely accessible and controllable via an Internet application.

X2000 has eight LEDs, including Bluetooth Low Energy, AC, 4G, Wi-Fi, Ethernet, system, and power. They are very useful during gateway installation and troubleshooting. Please check Appendix F for more information.

X2000 supports Power over Ethernet (PoE) and a 12V DC power source. It can easily attach to a pole or wall with an included mounting kit or can be placed on a flat space with an optional desktop stand kit.

X2000 has passed below environmental tests. It can be used both indoor and outdoor.

Tests Items	Standard and Test Scope
Transport vibration test	ISTA 2A-2011 packaged-products 150 lb (68 kg) or less: vibration test part
IP66 International protection rating test	Standard is GB/T 4208-2017 外壳防护等级 (IP代码) which is same as IEC 60529:2013 degree of protection provided by enclosures (IP Code). IP66 means no ingress of dust and water projected in powerful jets against the enclosure from any direction shall have no harmful effects
Salt fog test	Test in salt fog chamber with 36°C and 5% sodium chloride solution for 7 days (168 hours)
Humidity test	Test at humidity chamber operated at 49°C and 95% relative humidity for 10 days (250 hours)
Thermal cycle test	Test with cycling the temperature from -45°C to 70°C at a rate of 1°C per minute for 7 days (168 hours)

Processor & Memory

- CPU: 4 core ARM Cortex-A5, up to 1.5GHz
- RAM: 1GB DDR3 (approximately 700MB for the container)
- Storage: 4GB eMMC

Bluetooth

- Bluetooth Low Energy chip: 2x nRF52840
- Bluetooth Low Energy version: 4.0/4.1/4.2/5.0
- Connections: up to 40 co-existing connections
- Frequency: 2.400 to 2.483 GHz
- Data rates: up to 2x2 Mbps
- Tx power: configurable in 3~19dBm (limited by local regulatory requirements)
- Rx sensitivity: -105dBm
- Antenna Gain: 5.7dbi vertical polarized
- External Bluetooth antenna (optional): 50 Ohm N type female connector. The antenna and cable should have N type male connector

Wi-Fi (802.11 a/b/g/n/ac)

- Frequency: 2.4GHz and 5GHz ISM band
- Working Mode: Wi-Fi client or hotspot (for setup only)
- Tx power: 12.5 to 17.5dBm for 2.4GHz, 8.5 to 15.5dBm for 5GHz
- Rx sensitivity: -96 to -71dBm for 2.4GHz band, -91 to -71dBm for 5GHz band depending on the modulation
- Antenna: Integrated dual-band

For full features and specifications, please see the X2000 datasheet here:
https://www.cassianetworks.com/resources/x2000-bluetooth-edge-gateway/

1.2. Cassia X1000

The Cassia X1000 enterprise Bluetooth gateway has an IP65-rated enclosure and may be deployed in indoor and outdoor environments. The X1000 can be attached to a pole or wall (a mounting kit is included) or placed on a surface like a desk or counter space. It receives power from Power-over-Ethernet (PoE) via the uplink Ethernet port.

Cassia X1000 Bluetooth Gateway

The X1000 has a built-in smart antenna array designed specifically for Bluetooth. It also supports Ethernet, 2.4 GHz Wi-Fi, or USB cellular modem as IP uplink. The X1000 is capable

of extending Bluetooth's range up to 1000 feet (300 meters).

The X1000 increases the number of devices that can be simultaneously paired and connected to 22 Bluetooth low energy devices. It can also listen to potentially hundreds of devices at the same time when operating in broadcast mode.

Processor & Memory

- CPU: 4 core ARM Cortex-A5, up to 1.5GHz
- 256MB RAM DDR3, 4GB eMMC storage

Bluetooth

- Bluetooth Low Energy chip: 2x CSR8811
- Bluetooth Low Energy version: 4.0/4.1
- Connections: Up to 22 co-existing connections
- Frequency: 2.400 to 2.483 GHz
- Data rates: up to 2x1Mbps
- Tx power: Configurable in 5~20dBm (limited by local regulatory requirements)
- Rx sensitivity: -105dBm
- Antenna Gain: 5.7dbi vertical polarized

Wi-Fi (802.11 b/g/n)

- Frequency: 2.4 GHz
- Working Mode: Wi-Fi client or hotspot (for setup only)
- Tx power: 12.5 to 17.5dBm
- Rx sensitivity: -96 to -71dBm
- Antenna: Omnidirectional

For full features and specifications, please see the X1000 datasheet here:
https://www.cassianetworks.com/resources/x1000-enterprise-bluetooth-router-en/

1.3. Cassia E1000

The Cassia E1000 is an enterprise Bluetooth gateway with edge computing capabilities specifically designed for deployments in industrial, hospitals, senior centers, schools, gyms, and other indoor locations. The Cassia E1000 can be attached to the ceiling or wall (a mounting kit is included) or may be placed on a desktop or counter space. The E1000 is powered via a Micro-USB adapter or from a switch using Power over Ethernet via the uplink Ethernet port.

The E1000 increases the number of devices that can be paired and controlled for up to 40 Bluetooth low energy devices. In broadcast mode, the E1000 can listen to several hundred Bluetooth low energy end devices. Its patented smart antenna is optimized for horizontal use. The E1000 supports Ethernet, 2.4Ghz, and 5Ghz Wi-Fi, or USB cellular modem as an IP uplink. This enables your Bluetooth low energy devices to be remotely accessible and controllable remotely via an Internet application.

Processor & Memory

- CPU: 4 core ARM Cortex-A5, up to 1.5GHz
- 256MB RAM DDR3, 4GB eMMC storage

Bluetooth

- Bluetooth Low Energy chip: 2x Nordic nRF52832
- Bluetooth Low Energy version: 4.0/4.1/4.2, 5 compliant
- Connections: Up to 40 co-existing connections
- Frequency: 2.400 to 2.483 GHz
- Data rates: up to 2x1Mbps
- Tx power: Configurable in 3~19dBm (limited by local regulatory requirements)
- Rx sensitivity: -105dBm
- Antenna Gain: 5dbi PEAK

For full features and specifications, please see the E1000 datasheet here:
https://www.cassianetworks.com/resources/e1000-bluetooth-edge-router/

1.4. Cassia S2000

The Cassia S2000 enterprise Bluetooth gateway is designed for deployments in industrial automation, health monitoring, senior safety, and other enterprise IoT applications. The Cassia S2000 can be attached to a ceiling or wall with the included mounting kit, or it can be placed on a desktop or counter space. The S2000 receives power from either a Micro-USB adapter or a switch using PoE via the uplink Ethernet port.

Cassia S2000 Bluetooth Gateway

The S2000 extends Bluetooth's range up to 1000 feet and expands the number of Bluetooth low energy devices that can be paired and controlled up to 20 devices. In broadcast mode, the S2000 can listen to several hundred Bluetooth low energy end devices. The patented smart antenna of the S2000 is optimized for horizontal use.

The S2000 is used as a protocol gateway, translating between the Bluetooth protocol and the IP protocol. It supports Ethernet, 2.4Ghz Wi-Fi, and USB cellular modem for IP uplink. You can easily access and control your Bluetooth low energy devices remotely via an Internet application or a mobile app.

For S2000, if the received advertising packets are more than 200 per second, it is recommended to use scan filters to reduce S2000's CPU load.

Processor & Memory

- CPU: MIPS processor, up to 535MHz
- 64MB RAM DDR2, 16MB flash

Bluetooth

- Bluetooth Low Energy chip: Nordic nRF52832
- Bluetooth Low Energy version: 4.0/4.1/4.2, 5 compliant
- Connections: Up to 20 co-existing connections
- Frequency: 2.400 to 2.483 GHz
- Data rates: up to 1Mbps
- Tx power: Configurable in 3~19dBm (limited by local regulatory requirements)
- Rx sensitivity: -105dBm
- Antenna Gain: 5dbi PEAK

For full features and specifications, please see the S2000 datasheet here:
https://www.cassianetworks.com/resources/s2000-enterprise-bluetooth-router/

1.5. Certified Country List

Country/Region	Certificate	X2000	X1000	E1000	S2000	Local Representation
China	SRRC	Y	Y	Y	Y	
China	China RoHS	Y	Y	Y	Y	
US	FCC	Y	Y	Y	Y	
Canada	IC	Y	Y	Y	Y	Cassia provides local rep
Europe	CE	Y	Y	Y	Y	
Europe	REACH	Y	Y	Y	Y	
Europe	RoHS	Y	Y	Y	Y	
Japan	TELEC	Y	Y	Y	Y	
Taiwan	NCC & BSMI	Y	Y			Cassia provides local rep
Australia	RCM	Y	Y	Y		
New Zealand	RCM	Y	Y	Y		
Singapore	IMDA	2023		Y		Cassia provides local rep
Malaysia	SIRIM	2023		Y		One certification for one customer
Thailand	NBTC	2023/2024		Y		
Brazil	ANATEL	Y				Cassia provides local rep
South Africa	ICASA & NRCS	Y				One certification for one customer
Chile	SUBTEL	Y	Y			
Colombia	CRC	Y	Y			
Mexico	IFT & NYCE	2023/2024				One certification for one customer

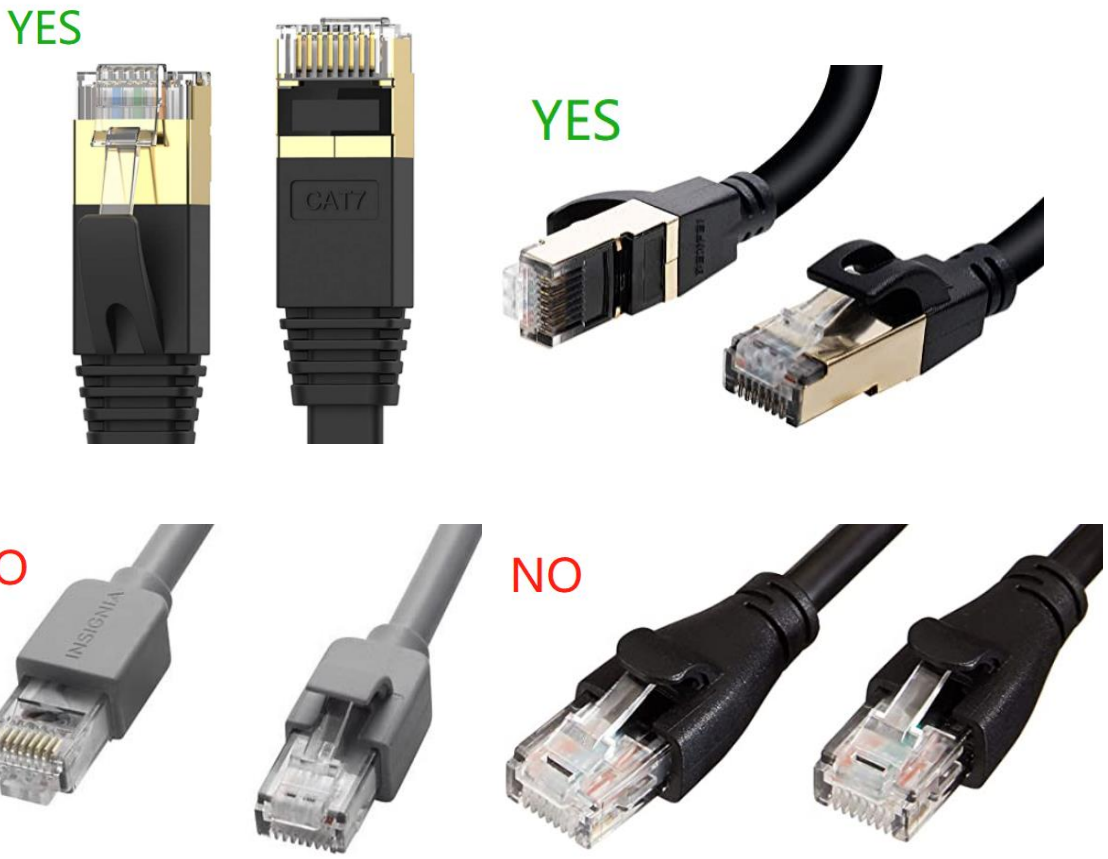
India	WPC	2023/2024		Y		Cassia provides local rep
Indonesia	SDPPI	2023/2024		Y		One certification for one customer
Philippines	NTC			Y		
Pakistan	PTA	2023/2024				Cassia provides local rep
Global	CB	Y	Y	Y	Y	
Global	BQB	Y	Y	Y	Y	

2. Installation

2.1. X2000

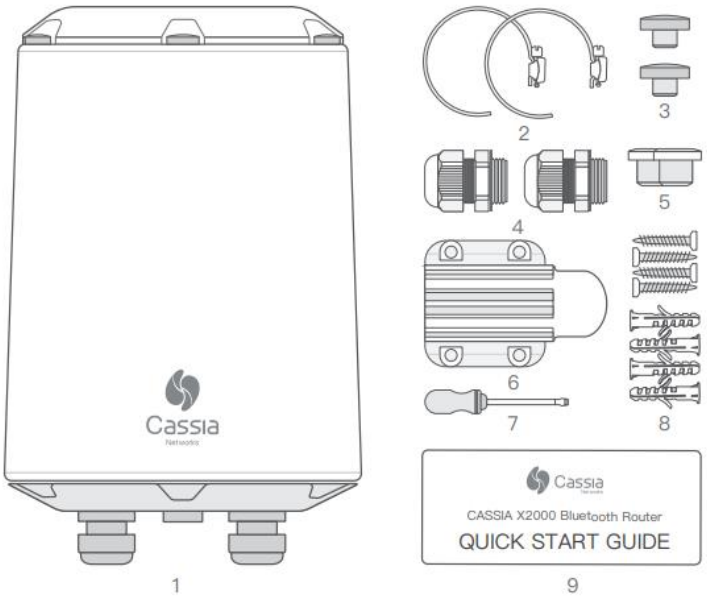
Hardware

- Cassia X2000 Gateway
- Power-over-Ethernet (POE) 802.3af/at compliant source, or PoE injector if PoE network is not available
- CAT5 Ethernet cable with standard RJ45 connector (Patch cord): 1 unit if PoE available, or 2 units if used with PoE injector. Only the Ethernet connector without the outer PVC jacket can fit X2000's cable glands.



- 12V DC power source or AC/DC power adapter (if not using PoE). The DC connector type should be interior diameter 2.5 mm, outside diameter 5.5 mm, center +v, and outer –v. The output voltage should be 12V. The output power should be equal to or larger than 12 W. Please don't use PoE and 12V DC at the same time.
- Optional external Bluetooth antennas. The connector on X2000 is a 50 Ohm N type female connector. The antenna and cable should have N type male connector.
- Computer System (Desktop/Laptop/Tablet/Smart Phone) with Wi-Fi connectivity
- USB cellular modem: Required only if set up over a SIM-based Internet connection

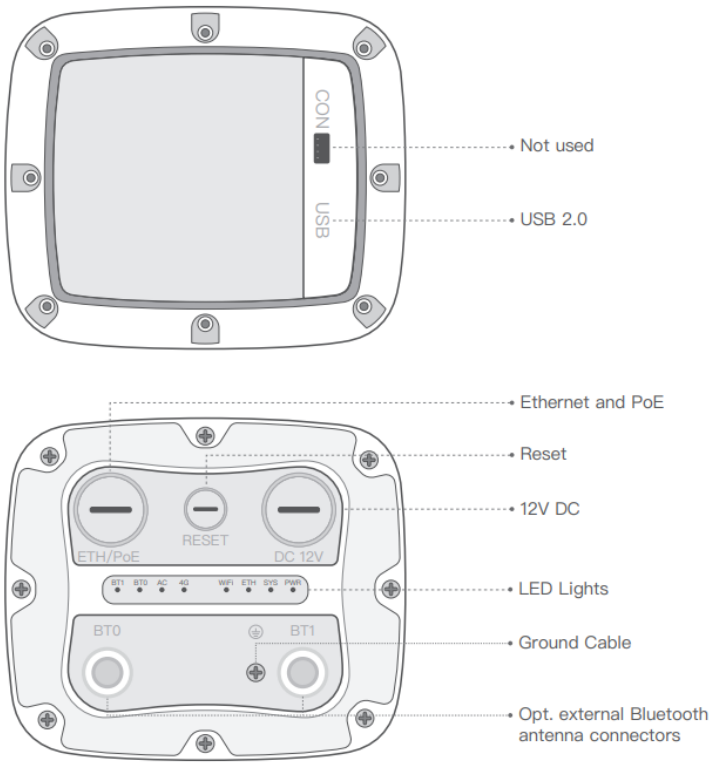
Included in Package



1. X2000 Router (1)
2. Pole Mounting Straps (2)
3. Extra Top Screw Covers (2)
4. Cable Glands (2)
5. USB Hole Silicone Plug (1)
6. Mounting Bracket (1)
7. Slotted Screwdriver (1)
8. Anchors with Screws (2*4)
9. Quick Start Guide (1)

The screws in the X2000 package are ST4.2×25. The user can use longer ST4.2 screws or ST5 screws too. If the user uses bigger screws, e.g. ST6, it will be difficult to install X2000's mounting bracket.

Head and base



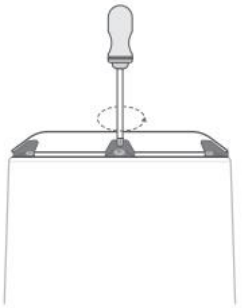
Mounting and installation

Please select the corresponding steps according to your gateway configurations.

1. Install USB Cellular modem inside X2000

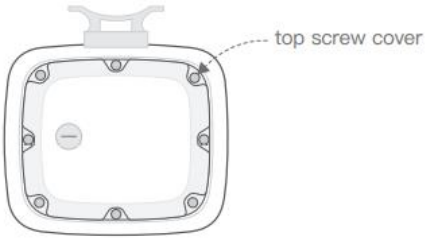
Step 1: Remove the top screw cover

Step 2: Use cross screwdriver to open the top cap



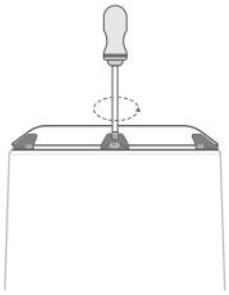
Step 3: Connect USB cellular modem to USB port

Step 4: Install the top cap, tighten the screws and insert the top screw cover



2. Install USB Cellular modem outside X2000

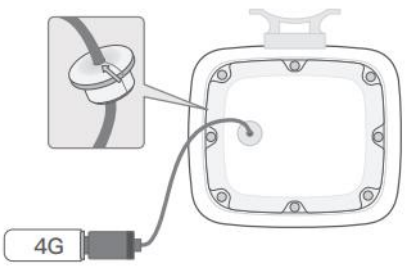
Step 1: Open the top cap



Step 2: Use slotted screwdriver to remove the USB hole plug (M20X1.5. Please don't mix with the ETH/PoE plug)

Step 3: Connect USB cable to USB port

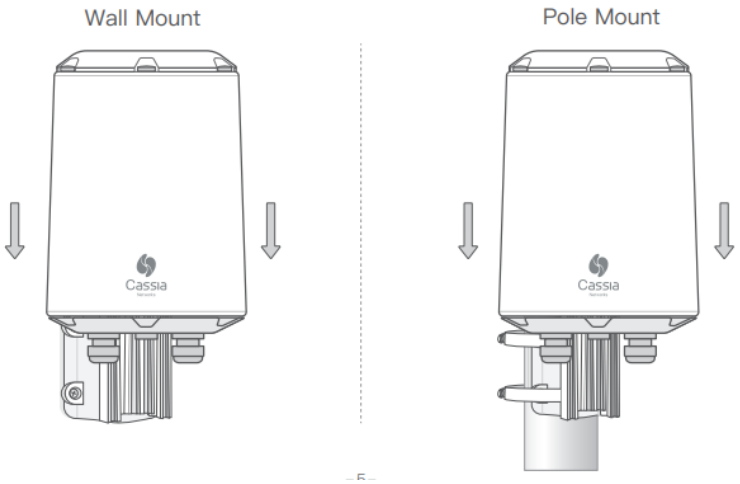
Step 4: Pass the USB cable through the USB hole, install the top cap, install the silicone plug in USB hole, and then connect the USB cellular modem to USB cable



3. Mount the X2000 mounting bracket in a vertical orientation onto a wall or pole with the supplied mounting kit

   NOTE: The side of the mounting bracket facing the wall and pole is sharp. Please don't hurt your hands.

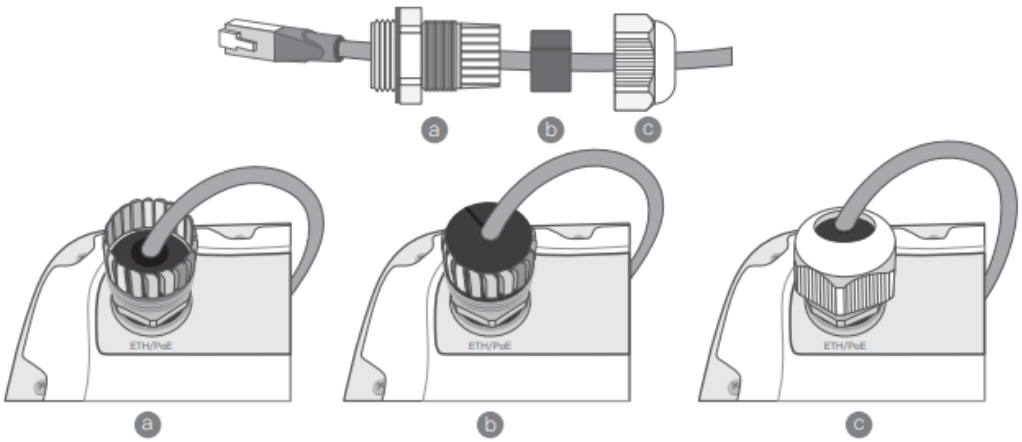
4. Slide X2000 down on the X2000 mounting bracket



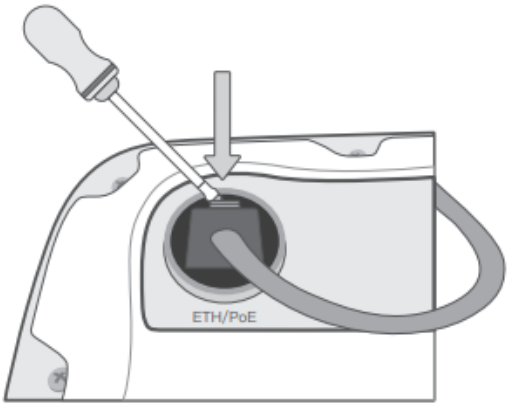
5. Connect Ethernet cable and PoE

   Remove the ETH/PoE plug (M22X1.5. Please don't mix with the USB hole plug), pass the Ethernet cable through the cable gland, insert the RJ-45 connector into the Ethernet port of X2000, and tighten the cable gland in the order of a, b, c. The torque of step c should be less than the torque of step a.

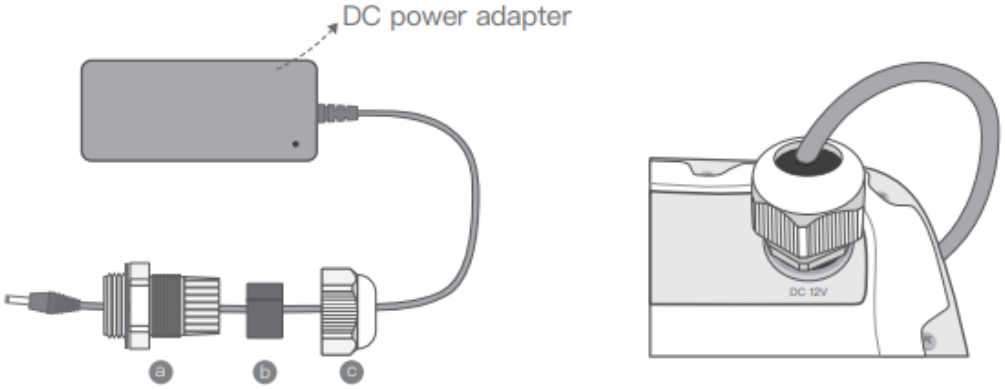
   NOTE: When removing the cable gland, please follow the order of c, b, a. Otherwise X2000 will be damaged.



To remove the Ethernet cable once it's been installed, please use the supplied screwdriver in the X2000 box or a small pointed tool of your choosing to depress the plastic release tab on the cable. See the image below.



6. Connect 12V DC power cable and cable gland to X2000 in the same way as step 5



7. For outdoor X2000 installations, please connect the ground cable to ensure X2000’s safety

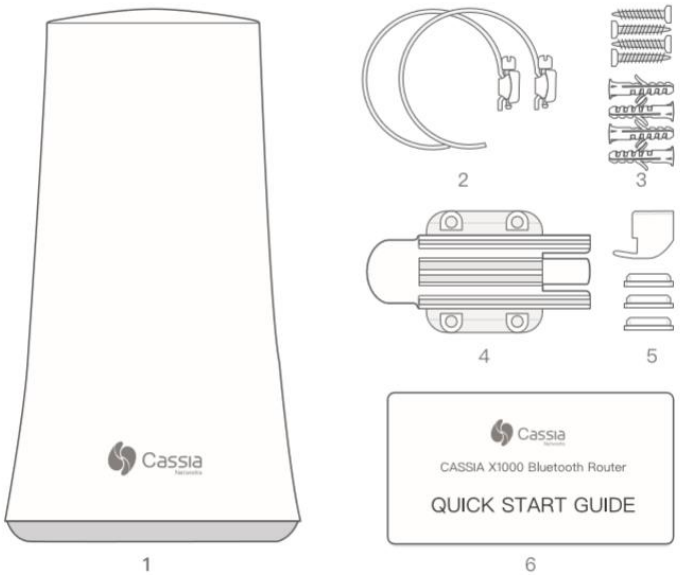
2.2. X1000

Hardware

- Cassia X1000 Gateway
- Power-over-Ethernet (POE) 802.3af/at compliant source, or PoE injector if PoE network is not available. The Cassia X1000 is only powered via Power-over-Ethernet (PoE)
- CAT5 Ethernet cable with standard RJ45 connector (Patch cord): 1 unit if PoE available, or 2 units if used with PoE injector. The user can choose an Ethernet cable with an L connector on one side to avoid stress when installing the bottom cap.

- Computer System (Desktop/Laptop/Tablet/Smart Phone) with Wi-Fi connectivity
- USB cellular modem: Required only if set up over a SIM-based Internet connection

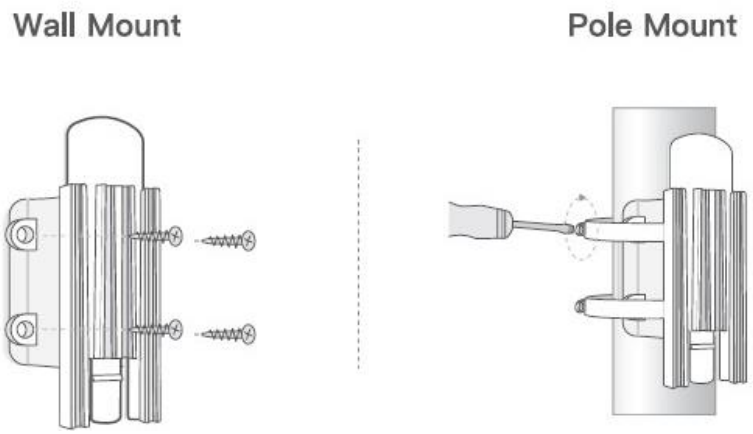
Included in Package



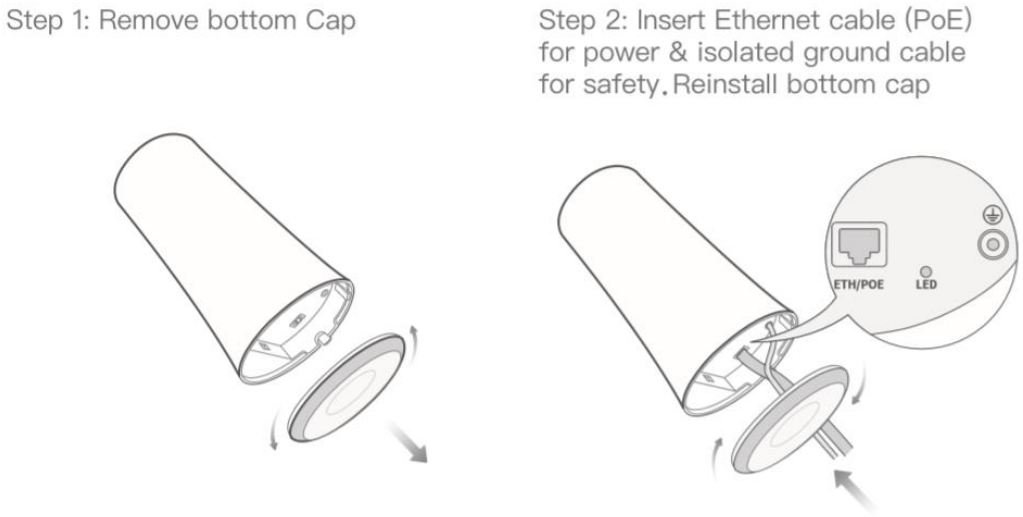
1. X1000 Router	(1)	3. Anchors with Screws	(2*4)	5. Silicon Plugs	(4)
2. Pole Mounting Straps	(2)	4. Mounting Bracket	(1)	6. Quick Start Guide	(1)

Mounting

1. Mount the X1000 mounting bracket in a vertical orientation onto a wall or pole with the supplied mounting kit;

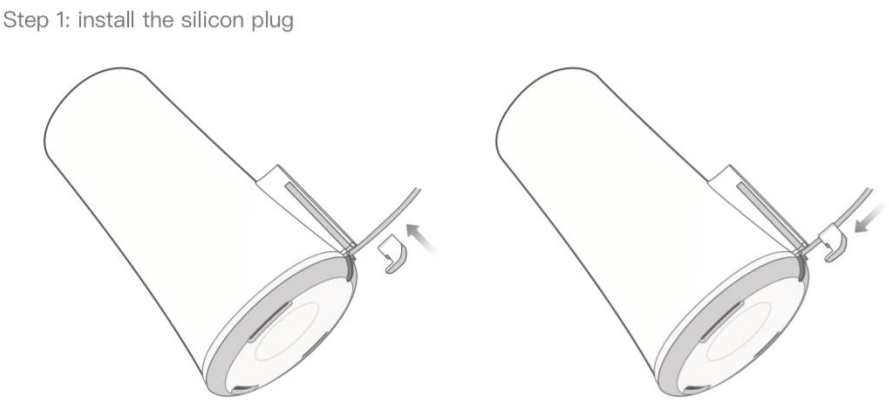


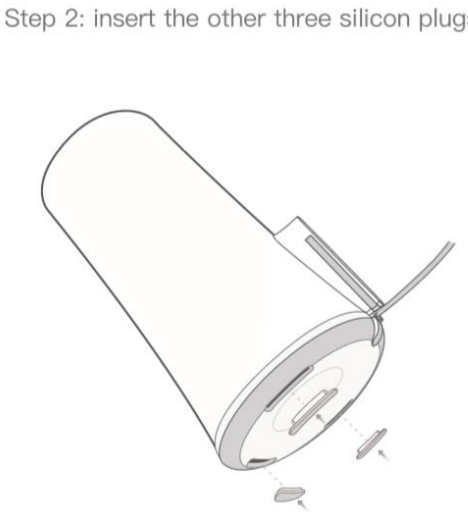
2. Connect the X1000 to Ethernet cable and ground cable;



Grounding is suggested, especially when X1000 is installed outdoors.

3. Install silicon plugs (please skip this step if the ground cable is installed);

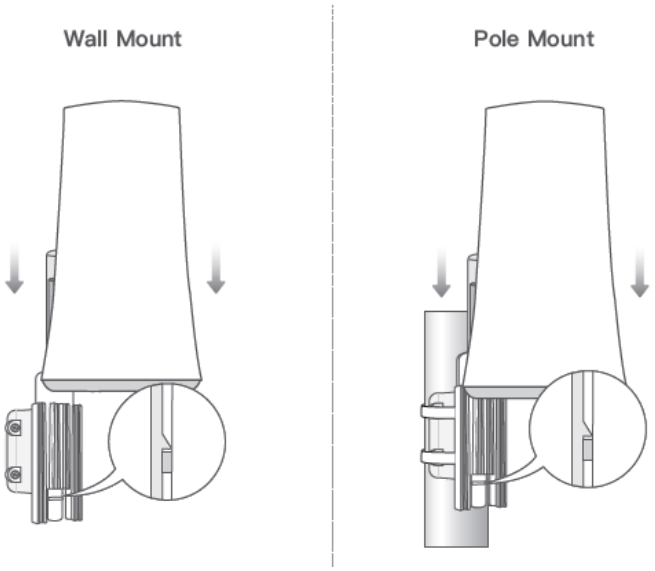




If the user wants to ground the gateway, there are many different types of cable diameters and cable hardness levels. When a grounding cable and Ethernet cable are used together, the resulting thickness might prevent silicone plug from sealing 100%.

When the silicon plugs are installed, the X1000 will be IP65. When the silicone plugs are not installed, the IP level of X1000 will be IP33. In this case, the three rainwater holes at the bottom of X1000 will avoid rainwater to stay in X1000, the user can seal up space with putty or silicone gel to ensure IP65.

4. Slide X1000 down on wall or pole mount;



5. Connect the X1000 Gateway to the PoE injector or a PoE switch.

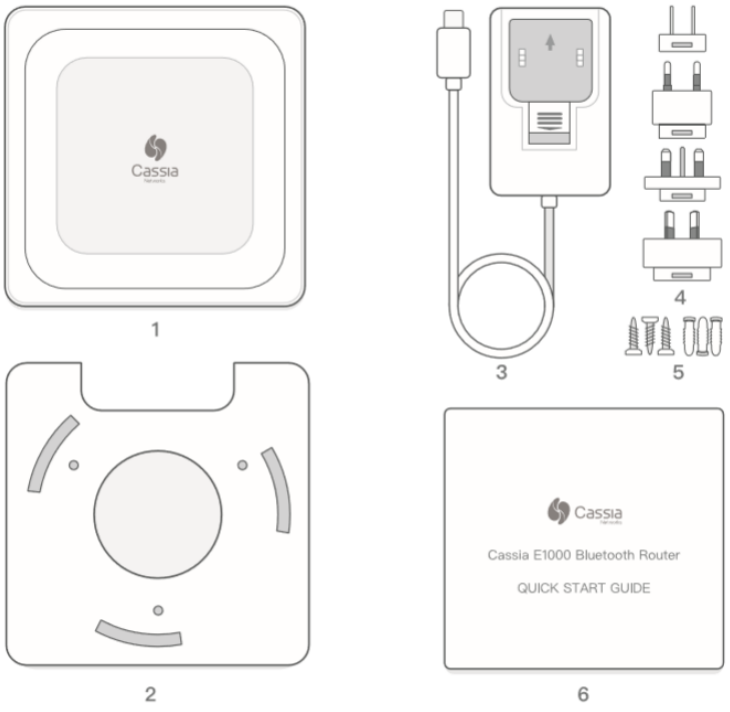
2.3. E1000

Hardware

- Cassia E1000 Gateway
- Power-over-Ethernet (PoE) 802.3af/at compliant source, or PoE injector if PoE network is not available

- CAT5 Ethernet cable with standard RJ45 connector (Patch cord): 1 unit if PoE available, or 2 units if used with PoE injector
- Micro USB power cable and universal plugs (if not using PoE)
- Computer System (Desktop/Laptop/Smart Phone/Tablet) with Wi-Fi connectivity
- USB cellular modem: required only if set up over a SIM-based Internet connection is required

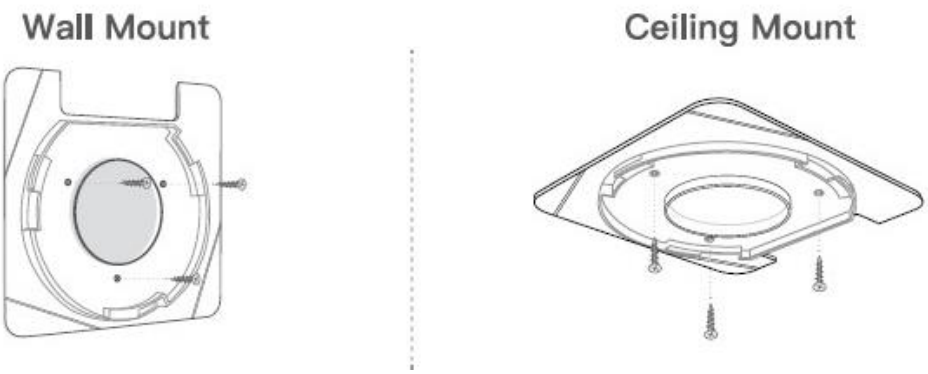
Included in Package



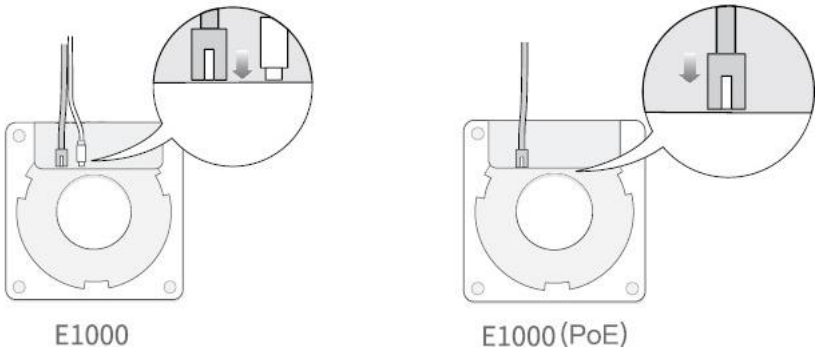
1. E1000 Router (1)	3. Micro USB Power (1)	5. Anchors with Screws (2*3)
2. Mounting Plate (1)	4. USB Power Plugs (4)	6. Quick Start Guide (1)

Mounting

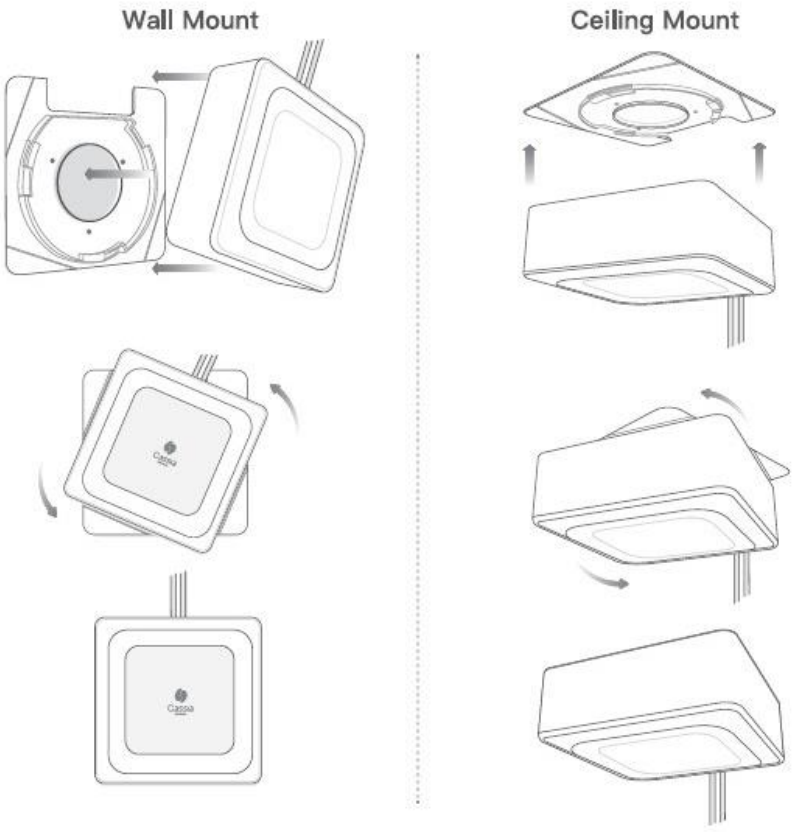
1. Place the E1000 on a flat, unobstructed surface or mount it using the supplied mounting kit in a vertical or horizontal orientation;
2. If mounting, first screw the mounting plate onto wall or ceiling;



3. Connect the E1000 to power with the supplied Micro USB cable and power adapter and to a Wi-Fi Access Point via Ethernet or Wi-Fi (2.4GHz or 5GHz). The E1000 can also connect to a Power-over-Ethernet (PoE) connection;



4. Place the E1000 gateway at a slight angle against the mounting plate and twist into place (turn clockwise);



IMPORTANT: For best range results, we recommend mounting the E1000 on the ceiling in an unobstructed location.

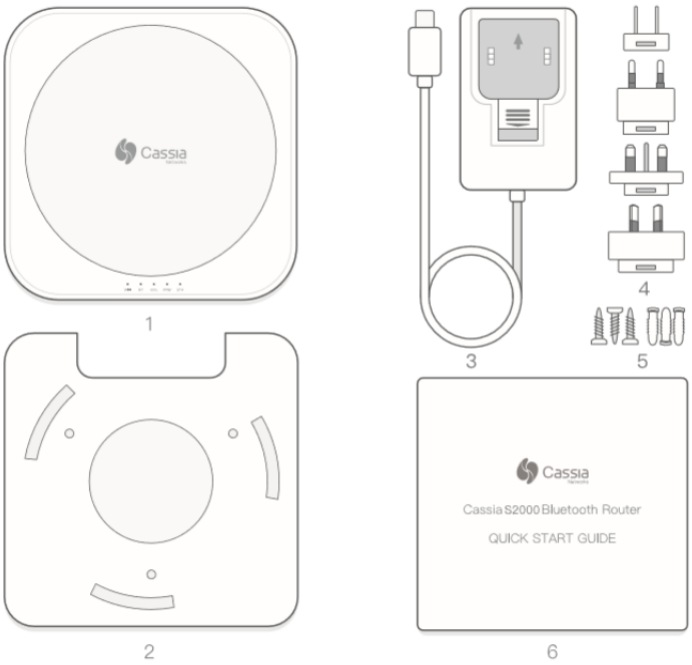
2.4. S2000

Hardware

- Cassia S2000 Gateway
- Power-over-Ethernet (PoE) 802.3af/at compliant source, or PoE injector if PoE network is not available
- CAT5 Ethernet cable with standard RJ45 connector (Patch cord): 1 unit if PoE available, or 2 units if used with PoE injector

- Micro USB power cable and universal plugs (if not using PoE)
- Computer System (Desktop/Laptop/Smart Phone/Tablet) with Wi-Fi connectivity
- USB cellular modem. This is only required if set up is over a SIM-based Internet connection

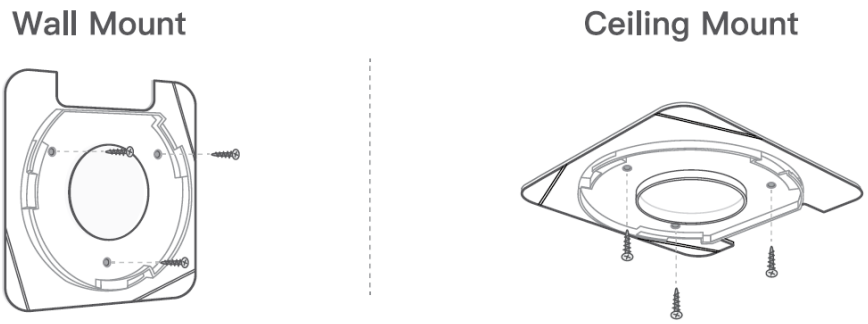
Included in Package



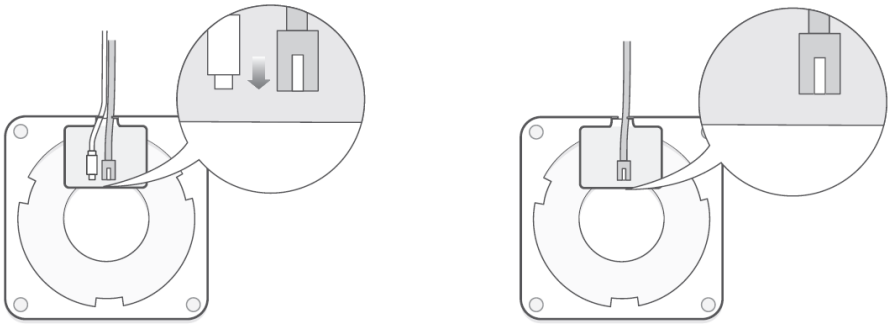
1. S2000 Router (1)
2. Mounting Plate (1)
3. Micro USB Power (1)
4. USB Power Plugs (4)
5. Anchors with Screws (2*3)
6. Quick Start Guide (1)

Mounting

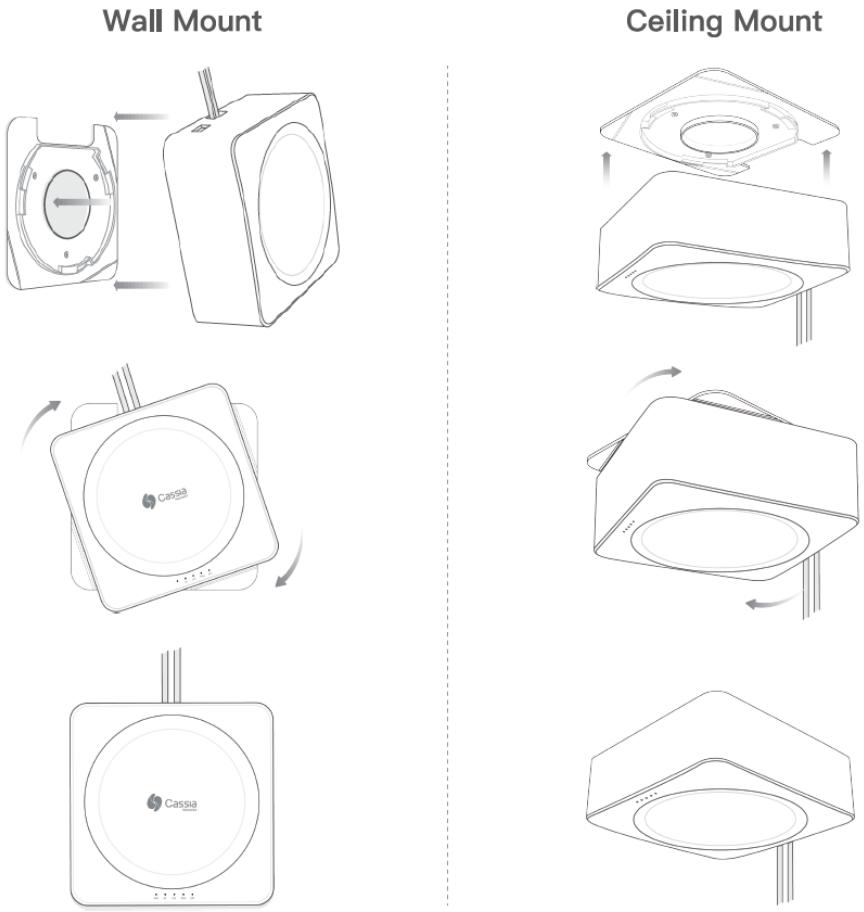
1. Place the S2000 on a flat, unobstructed surface or mount it using the supplied mounting kit in a vertical or horizontal orientation.
2. If mounting, first screw mounting plate into wall or ceiling.



3. Connect the S2000 to power with the supplied Micro USB cable and power adapter and to a Wi-Fi Access Point via Ethernet or Wi-Fi (2.4GHz only). For your network setting information, please contact your IT administrator.



4. Place the S2000 gateway at a slight angle against the mounting plate and twist it into place (turn clockwise).



IMPORTANT: For best range results, we recommend mounting the S2000 on the ceiling in an unobstructed location.

3. Deployment

3.1. X1000 and X2000

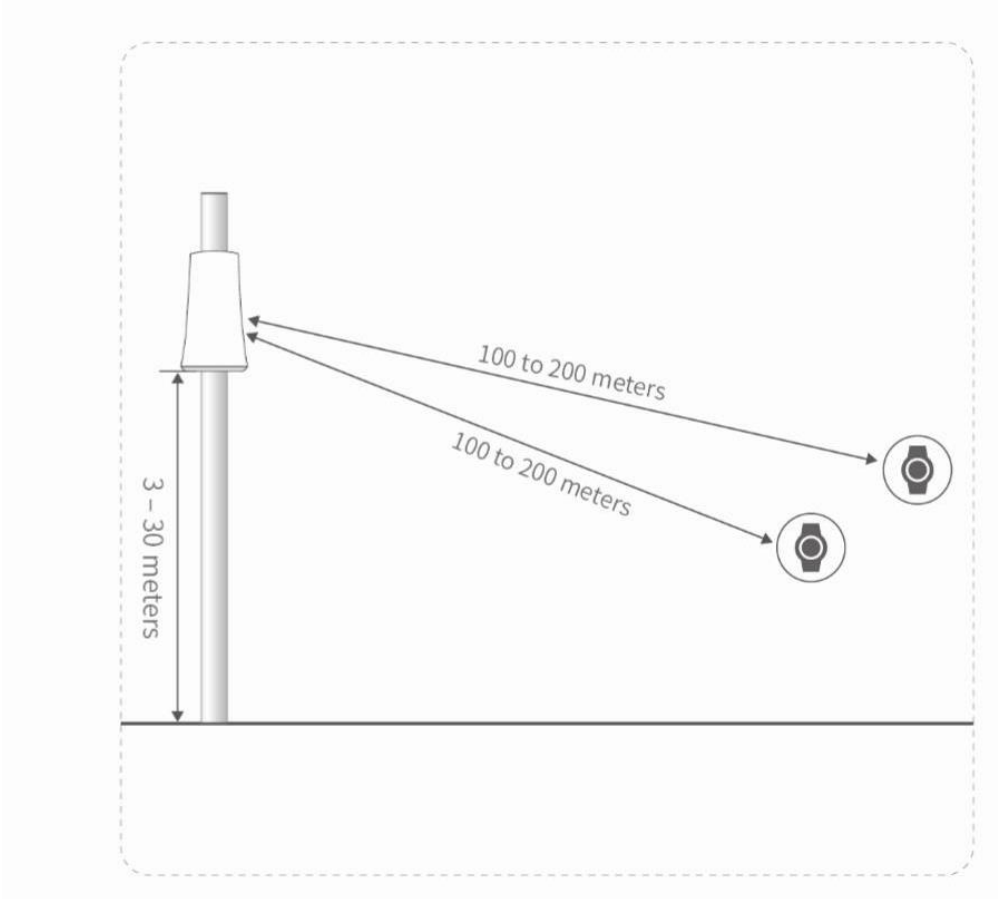
Cassia's Bluetooth gateway coverage varies based on conditions. In outdoor "open-air" locations with no obstructions, the coverage radius of Cassia's Bluetooth gateways is greater than indoor locations with walls and obstructions.

In general, the radius of outdoor coverage may vary from 100 meters to 400 meters with Bluetooth 4.x or even to 1 kilometer with Bluetooth 5.0, depending on the wireless interference, obstructions, and line of sight. A rule of thumb for deployment is to ensure that the Bluetooth device has a consistent connection and that the Bluetooth signal strength is strong.

Deployment principles:

- Avoid installations near radio transmitters such as radio towers, cellular base stations, and Wi-Fi access points (APs)
- Pole or wall mounting is required
- Power-over-Ethernet (PoE) or 12V DC (for X2000 only) is required
- Installation height is recommended between 10 and 100 feet (3 and 30 meters)
- Grounding cable and lightning protection is suggested, especially when X1000 and X2000 are installed outdoors

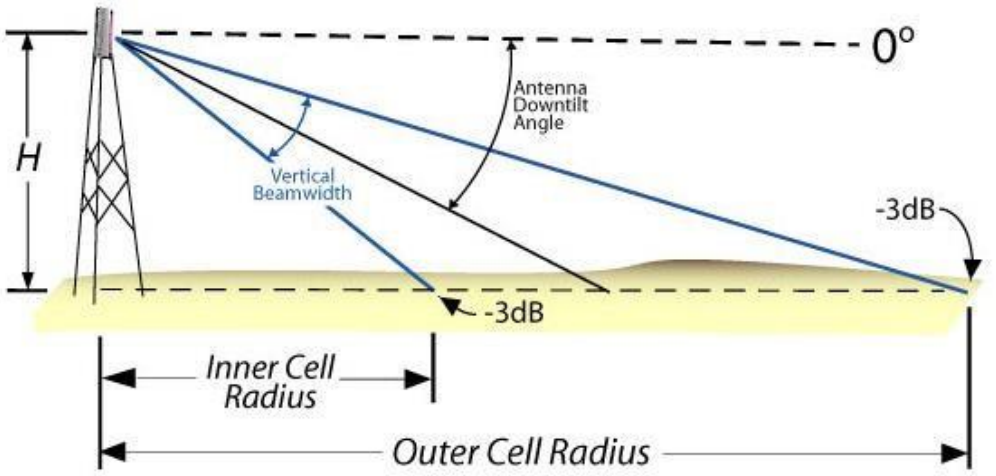
Below is an example of X1000 outdoor line of sight deployment.



Cassia X1000 outdoor deployment

Down-tilt Angle

When installation height is more than 30 feet (10 meters), an antenna down-tilt angle is required.



$$\text{Inner Radius Distance} = \frac{H/\text{Tan}\,(A + \frac{BW}{2})}{5280} \qquad \text{Outer Radius Distance} = \frac{H/\text{Tan}\,(A - \frac{BW}{2})}{5280}$$

According to the above formula, the following tilt angles are highly recommended:

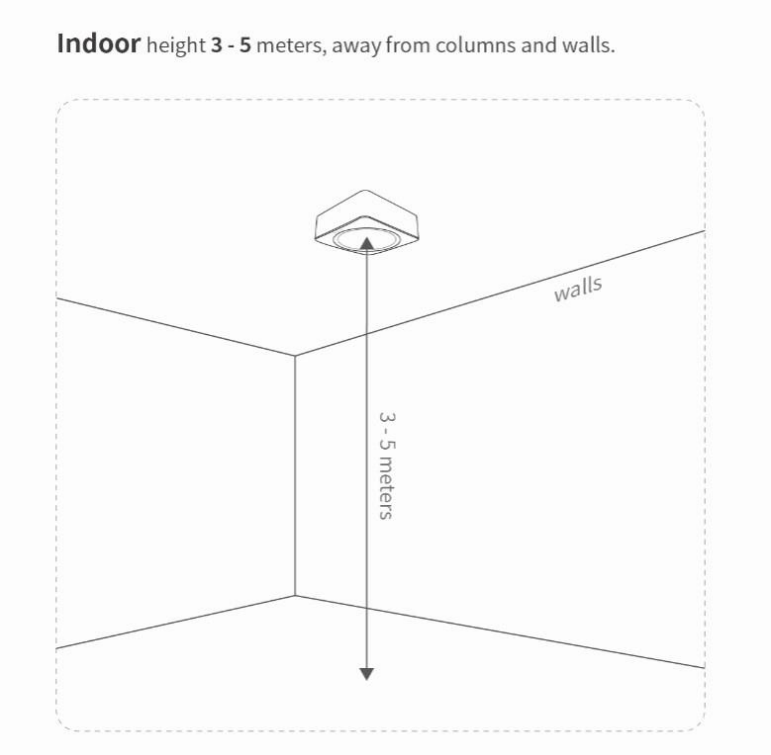
- At a height of 10-30 feet (3-10 meters), no tilting is needed
- At a height of 30-60 feet (10-20 meters), 5°-10° tilt is required
- At a height of more than 60 feet (20 meters), please calculate the inclination angle according to the formula provided above

3.2. E1000 and S2000

The optimal placement for the Cassia E1000 and S2000 should be located above ground at a height of 10 to 15 feet (3-5 meters), in direct line of sight of the Bluetooth Low Energy device, and within 180 to 1000 feet (60-300 meters) range of the device. Ceiling installations should be 6 feet (2 meters) away from nearby walls or columns. Obstacles, like walls, as well as Wi-Fi interference, will reduce the range of Cassia's Bluetooth gateways.

Deployment principles:

- Keep at least 3 feet (1 meter) away from cellular antennas and Wi-Fi access points.
- Installation should be far from microwaves, wireless keyboard/mouse, and other devices that also use the 2.4 GHz band.
- Avoid installations near air conditioners, heating pipes, water supply pipes, transformer boxes, an elevator operation room, etc.

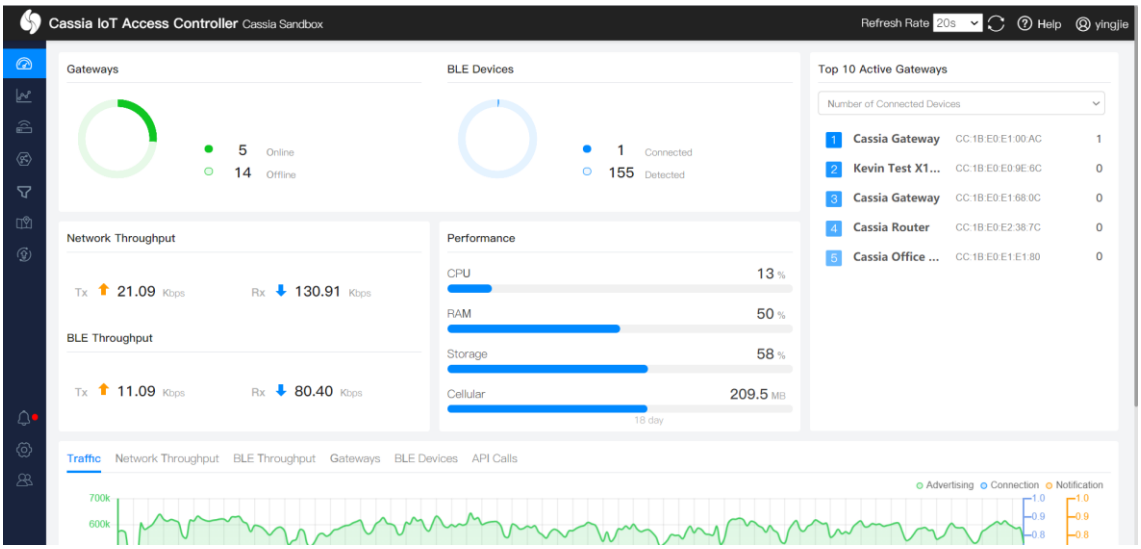


E1000 and S2000 Indoor Deployment

4. Getting Started

4.1. Understanding the Cassia Access Controller

The Cassia IoT Access Controller (AC) is a powerful IoT network management solution. Using the Cassia AC, organizations have access, control, and monitor over IoT environments. The Cassia AC solution enables the deployment and management of hundreds of Bluetooth gateways, as well as the monitoring of thousands of detected/connected devices in an enterprise environment from one centralized interface.



Cassia IoT Access Controller

Why use the AC?

- Provisioning and managing Bluetooth gateways individually is time-consuming and error-prone
- Version management for hundreds of gateways individually is a manual and inefficient process
- Gateway alone cannot support Bluetooth roaming
- Gateway alone cannot track a Bluetooth Low Energy device's location

For more details, please see the Cassia IoT Access Controller Server Data Sheets here: https://www.cassianetworks.com/resources/cassia-iot-access-controller/

The user may use a Cassia-hosted AC or install their own AC server. It is strongly recommended that new users use a Cassia-hosted AC to expedite the evaluation process. The evaluation process of a Cassia Bluetooth Gateway with a Cassia-hosted AC is available for purchase with Cassia Starter Kits. Please contact the Cassia sales team for more information.

4.2. AC Server Resource Requirements

Below table shows the server resource requirements for Cassia IoT AC in production

deployment.

Number of Gateways	CPU	RAM	Storage
Less than 50	3Ghz * 2 core	4GB	8GB
50 to 100	3Ghz * 4 core	4GB	16GB
100 to 500	3Ghz * 4 core	8GB	32GB
500 to 5000	3Ghz * 8 core	32GB	50GB

NOTE: The AC server Resource requirements may vary depending on the way the user's application controls the Bluetooth devices, number of Bluetooth devices, the frequency of the connection setup requests, etc.

If you plan to use AWS EC2 to host your Cassia IoT AC, please select instance type T2 or M4, which uses intel CPU. For example, you can use t2.medium for an AC that manages less than 50 gateways. Please check https://aws.amazon.com/ec2/instance-types/ for all the AWS instance types.

4.3. Licenses Key and Developer Key/Secret

a) Server License Key

If you want to manage more than three Cassia Bluetooth gateways by one Cassia IoT AC, please send below information to **support@cassianetworks.com** to apply License Key. The AC license key governs the number of Bluetooth gateways that can be managed by the AC and the valid time.

- AC information (customer name, AC URL, etc.)
- Number of managed gateways (4 to 9999 gateways)
- Device ID (please copy from AC setting page)

Below is an example of AC License Key:

```
v002-0128-20180427052110-0012-p52y-zunk-rqbe-pqlw
```

b) Developer Account Credentials

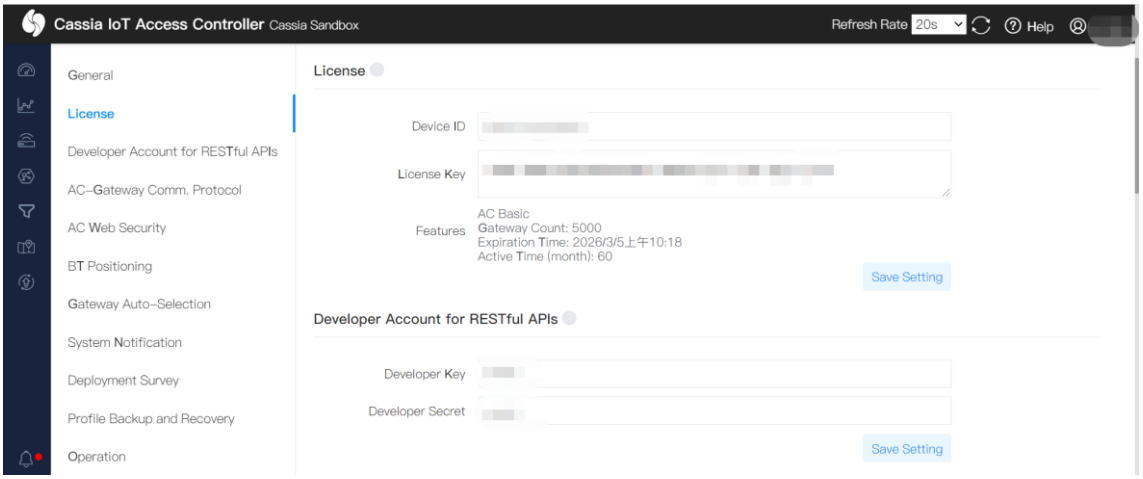
Before using Cassia's RESTful API through the AC, end-users will now have to generate their own Developer Key and Developer Secret. These credentials are also intended for the end user's IoT application for OAuth 2.0 authentication towards Cassia's AC.

NOTE: For the latest version of the AC, v2.1.1, the Developer Secret Key should be between 8 to 60 characters, and must contain numbers, letters, and special characters.

For a 2.1.1 AC upgraded from older versions, the old Developer Secret key still functions, but we are strongly recommending users generate new Developer Secret Keys that match the new format stated above. Please update the Developer Secret Key used in your IoT application as well.

Please see the screenshot below for inputting the License key, Developer Key and

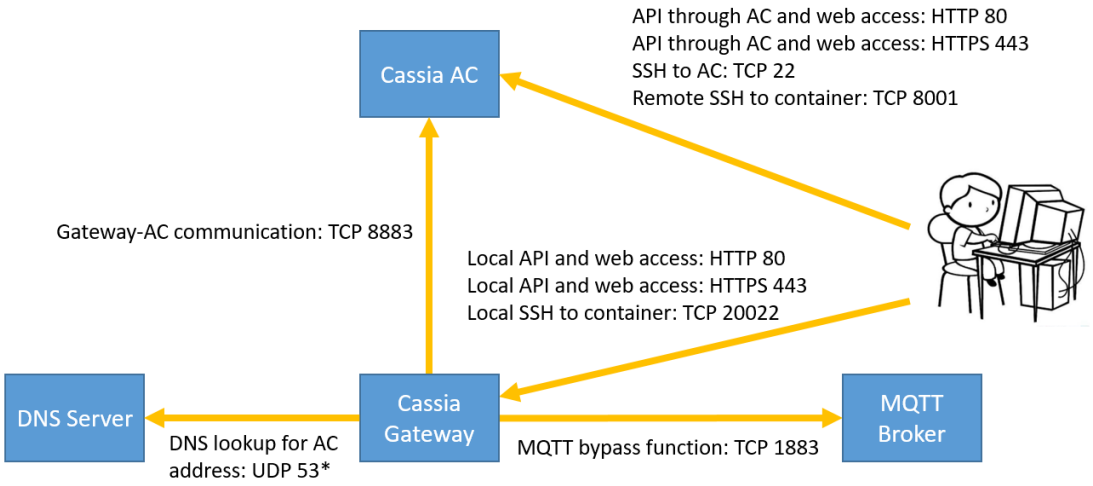
Developer Secret in AC setting page.



Input your developer key, developer secret, and license key via the AC

4.4. Network Requirement

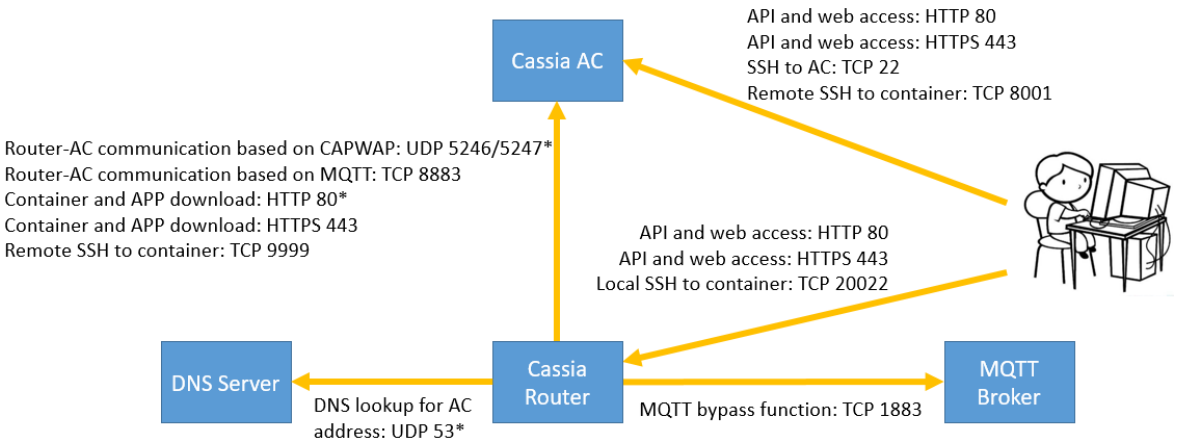
From v2.1.1, for the gateways that uses MQTT to communicate with AC (default setting), the following ports are used and required for firewall configuration. TCP ports 80, 443 and 9999 are not required anymore.



Please make sure the following ports are opened outbound on the gateway side firewall.

Type	Port	M/O	Description
TCP	8883	Mandatory	Gateway-AC communication
UDP	53	Mandatory*	DNS lookup for AC address. *Optional if internal DNS is specified in gateway network configuration
TCP	1883	Optional	For MQTT bypass function only (see chapter 5.6)

For the gateways that use CAPWAP to communicate with AC or the gateways using firmware below v2.1.1, the following ports may be used and required for firewall configuration.



Please make sure the following ports are opened outbound on the gateway side firewall. The user can check if a TCP port is opened by using Netcat in chapter 5.5.

Type	Port	M/O	Description
UDP	5246, 5247*	Mandatory	Gateway-AC communication based on CAPWAP. *Port 5246 and 5246 can be disabled after migrating gateway-AC communication to MQTT (see chapter 4.4)
TCP	8883		Gateway-AC communication based on MQTT (recommended from firmware v2.0.2)
HTTP	80*	Mandatory	Container and APP download from AC based on HTTP. *HTTP port 80 can be disabled if HTTPS is enabled
HTTPS	443		Container and APP download from AC based on HTTPS
UDP	53	Mandatory*	DNS lookup for AC address. *Optional if internal DNS is specified in gateway network configuration
TCP	9999	Mandatory	Remote SSH to container (laptop->8001->AC<-9999<-container)
TCP	1883	Optional	For MQTT bypass function only (see chapter 5.6)

4.5. CAPWAP and MQTT Setting

Before firmware 2.0.2, Cassia Bluetooth gateway communicates with AC using CAPWAP protocol. CAPWAP is based on UDP port 5246 and 5247 and always uses DTLS 1.2 to ensure security (secured CAPWAP).

From firmware 2.0.2, Cassia gateway can also use MQTT to communicate with AC. MQTT uses TCP port 8883 and always uses TLS 1.2 (secured MQTT). MQTT improves the robustness of gateway and AC communication. It brings a higher upgrade success rate and less data drop rate. What is more, sometimes the user's firewall doesn't allow UDP packets to pass. In this case, MQTT will help the packets between the gateway and AC to pass through the user's firewall.

TCP based MQTT protocol is more reliable on internet than UDP based CAPWAP protocol. If the AC and gateways are connected through the internet, and the Cassia RESTful API through the AC is used to collect Bluetooth device data, it is highly recommended to disable CAPWAP ports in AC Settings page, which will force all the gateways to connect to the AC through MQTT. Otherwise, there might be packet loss or an incorrect message sequence between the gateway and AC. The API calls might return HTTP 502 or 504 errors, depending on the internet connection quality.

One AC can use MQTT to communicate with some gateways and use CAPWAP to communicate with the other gateways at the same time. The user can enable or disable CAPWAP and MQTT ports on AC by setting “CAPWAP port” and “MQTT port” on AC setting page. The user can disable CAPWAP ports if they don’t want gateways to connect this AC by CAPWAP.

On AC or gateway’s console, the user can set the high priority gateway-AC protocol by changing parameter “AC-Gateway Protocol Priority” (default is MQTT). The gateway will try both MQTT and CAPWAP with below strategy. First, the gateway will try to use the high priority protocol to connect AC. If it doesn’t succeed in 15 minutes, the gateway will try the low priority protocol for 5 minutes automatically. If it fails again, the gateway will try the high priority protocol for another 15 minutes, and then repeat. For the gateway using USB cellular modem, the timer for high priority protocol is 60 minutes. After the gateway is online, the user can find the actually used protocol by checking “AC-Gateway Protocol” on AC or gateway’s console.

NOTE: From version 2.0.3, a newly installed AC will support MQTT only (CAPWAP disabled by default). If the user needs to connect a version 1.4.x gateway (only supports CAPWAP) to a 2.0.3 AC, please enable the CAPWAP ports in AC settings. For the AC upgraded from a lower version, both CAPWAP and MQTT will be enabled by default.

NOTE: From firmware 2.0.3, the default “AC-Gateway Protocol Priority” on the gateway is MQTT. If the gateway was upgraded from lower versions, the default value will be CAPWAP.

Please follow the below steps to migrate one gateway from CAPWAP to MQTT.

1) Open outbound TCP port 8883 on gateway side firewall.
2) Fill in AC server address in AC console gateway Config tab or gateway console Basic tab, if it is empty. **NOTE:** AC server address is mandatory if AC is in the cloud or MQTT is used for gateway and AC communication.
3) In the AC console gateway Config tab or gateway console Basic tab, please change “AC-Gateway Protocol Priority” from CAPWAP to MQTT.
4) The gateway will disconnect from AC and try to re-connect by MQTT. If the gateway can’t connect to AC by MQTT, it will try CAPWAP instead automatically.
5) After the gateway is on-line, please check if MQTT is actually used by checking “AC-Gateway Protocol” on the AC console gateway Details tab or gateway console Status tab.
6) When all the gateways managed by one AC have been migrated to MQTT, the user can disable CAPWAP ports on the AC setting page.

4.6. Connecting the Gateway to AC

You will find your Cassia Bluetooth gateway's MAC address located at the bottom of the gateway.

Cassia Bluetooth gateway's MAC address

If you are filtering MAC addresses in your security policy, please make sure to input the active MAC addresses. For example, if you are using Wi-Fi for an uplink connection, your active MAC will be Label_ MAC+1. See the table below for further details.

Model	Label MAC	Ethernet MAC	Wi-Fi MAC
X2000/X1000/E1000/S2000	MAC	MAC	MAC+1
S1000/S1100	MAC	MAC	MAC-1

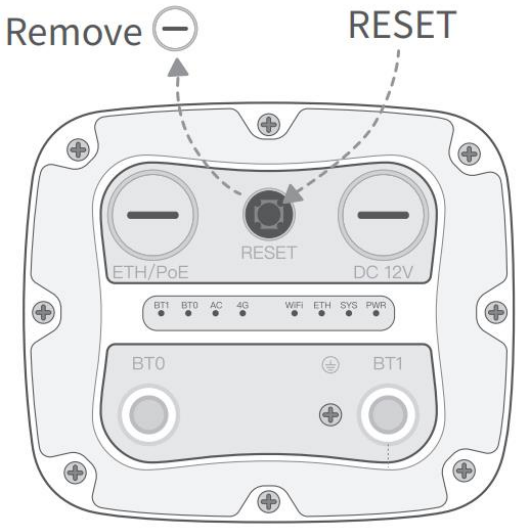
For firmware 1.2 or above, a Cassia Bluetooth gateway comes with a Wi-Fi hotspot function (2.4GHz only). The SSID is cassia-xxxxxx (the "x's" corresponds to the last 6 digits of the gateway's MAC address). The default password of the Wi-Fi hotspot is the same as the SSID.

For example, if the Cassia Bluetooth gateway MAC address is "CC:1B:E0:**E0:96:DC**", the SSID and its default password will be "cassia-**E096DC**". The gateway's default IP address is 192.168.40.1. The gateway's console default username is admin.

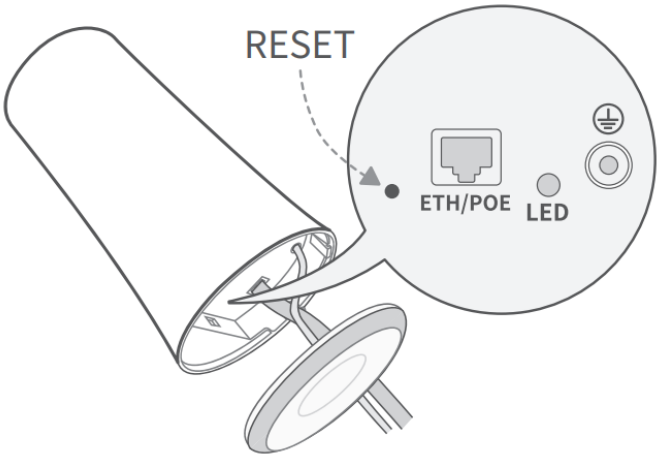
Please follow the Gateway Installation Guide to connect your laptop to the Wi-Fi hotspot and to configure the gateway and connect it to the AC. For detailed instructions, please click here: https://www.cassianetworks.com/support/knowledge-base/general-documents/

If you can't find the Wi-Fi hotspot (2.4GHz only) or forget the gateway's login password, and your firmware is 1.2 or above, you can press and hold the reset button located at the bottom of the gateway for 10 to 15 seconds while the gateway is powered on. Once reset,

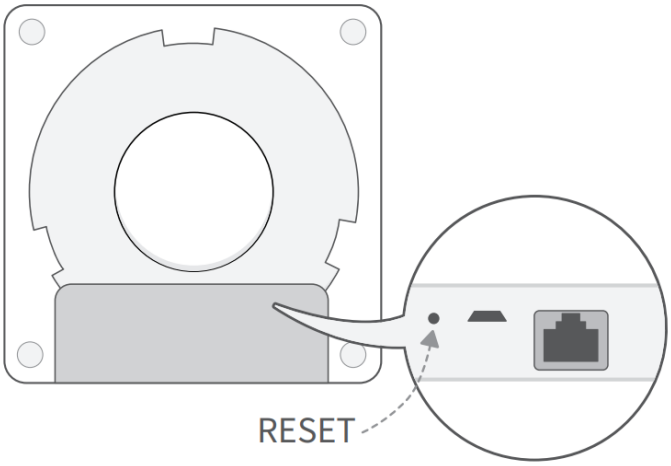
the Wi-Fi hotspot will be enabled, and the gateway login password will be reset. You can also reset gateway's login password through the AC.



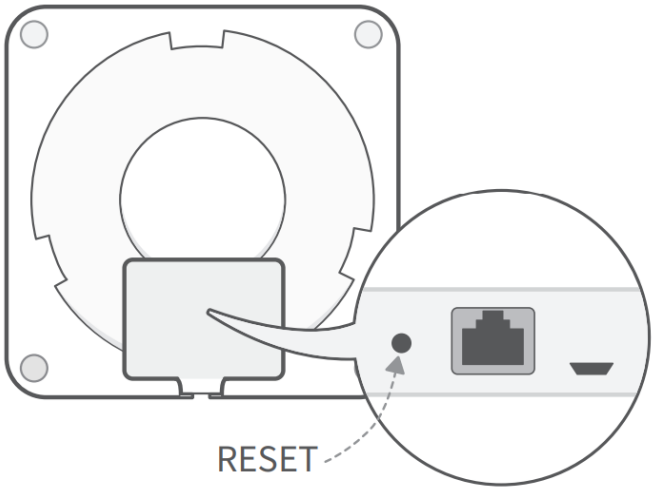
X2000 Reset Button



X1000 Reset Button



E1000 Reset Button



S2000 Reset Button

After reset, the gateway configurations in the below table will be set to the factory default profile settings. The country code, container, and customer APP will not be impacted.

Parameter	Manufacturing Default Value
Gateway Console Username	admin
Gateway Console Password	Need to set new password
AC Server Address	Empty
Local RESTful API	OFF
Remote Assistance	OFF
Connection Priority	Wired
Wi-Fi / Operating Mode	Hotspot
Wi-Fi / SSID	cassia-xxxxxx
Wi-Fi / Password	cassia-xxxxxx
Local Time Zone	UTC +08:00
Local Time	1970-01-02, 00:00:00
Enable Local SSH Login	OFF
AC-Gateway Protocol Priority	MQTT (this configuration is available from firmware 2.0.2)

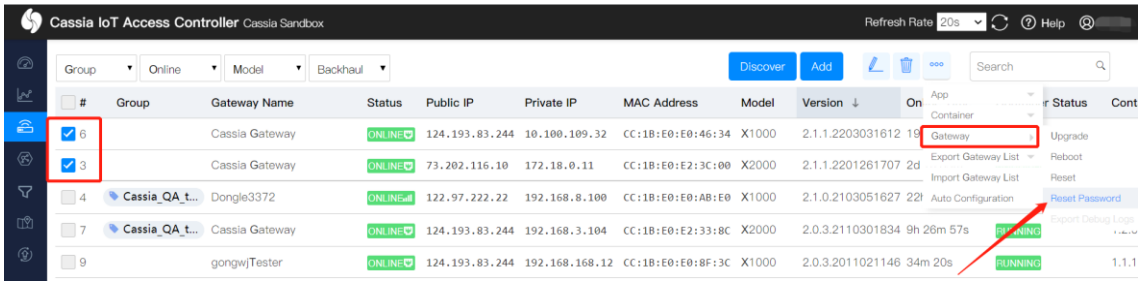
5. Cassia Bluetooth Gateway Configurations

NOTE: The Google Chrome browser is preferred as results may vary with other browsers.

To configure the gateway, please open the Cassia Bluetooth gateway's local console by entering its local IP address or access it from the gateway's Wi-Fi hotspot. The user can also configure the gateways by gateway auto configuration feature (chapter 6.6), or configure the gateways in batch from AC console (chapter 6.7).

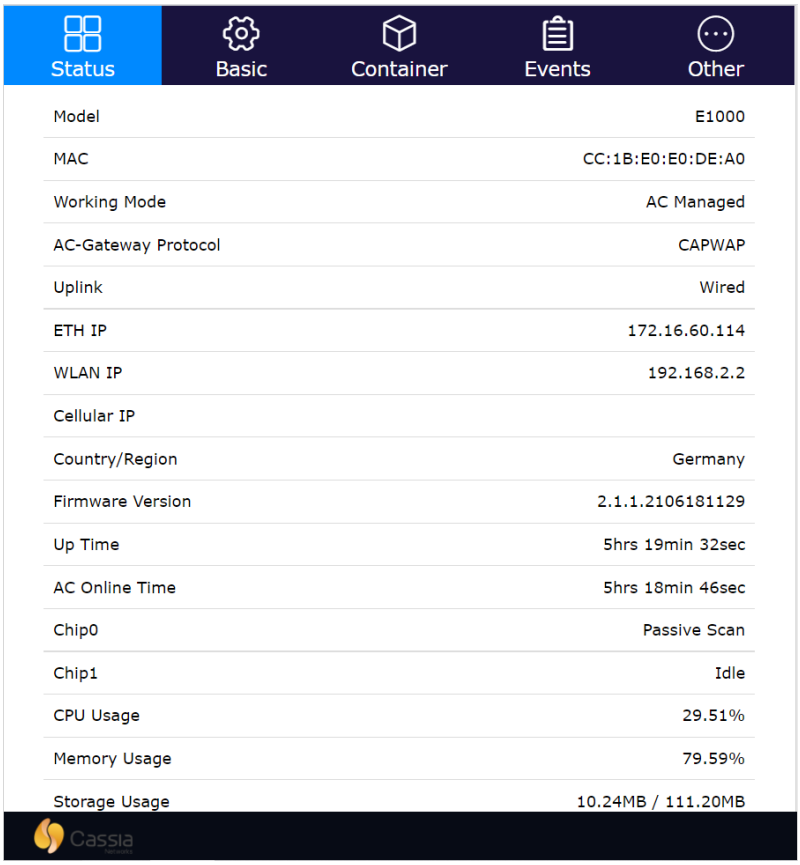
The gateway's local console account will be frozen for 1 minute after 5 failed attempts. The login password will expire in 180 days if "Change Password Every 180 days" is switched on in Other tab.

If you forget the gateway's login password, you can reset it through the AC. The read only AC account doesn't have the permission to reset the gateway's login password.



5.1. Status Tab

The Status tab displays the gateway's current configuration:



Cassia gateway configuration page – Status

Parameter	Description
Model	X2000, X1000, E1000 or S2000.
MAC	This is the MAC address printed on the bottom of the Cassia Bluetooth gateway, which is equal to the gateway's Ethernet interface MAC.
Working Mode	**AC Managed** mode means the Cassia Bluetooth Gateway is connected to the Cassia IoT Access Controller and managed by the AC. **Standalone** mode means the Cassia Bluetooth Gateway is not connected to the AC and operating locally.
AC-Gateway Protocol	CAPWAP or MQTT. It shows the actually used gateway-AC communication protocol. It may be different from the "AC-Gateway Protocol Priority" configuration, which is the high priority protocol. If the gateway connects to AC successfully, it will save the used protocol and try it first after the connection is lost or gateway reboot.
Uplink	Ethernet, Wi-Fi, or USB cellular modem
ETH IP	Ethernet IP address of the gateway
WLAN IP	WLAN IP address
Cellular IP	The IP address of the gateway when using a USB cellular modem
Country/Region	Deployment location
Firmware Version	The firmware version on the gateway
Up Time	The gateway up time in hours since the last reboot
AC Online Time	The time of the gateway connected with the AC. If not connected, it shows offline.
Chip 0	Status of Bluetooth Low Energy chip 0. It can be idle, active scan, passive scan, or advertise
Chip 1	Status of Bluetooth Low Energy chip 1. It can be idle, active scan, passive scan, or advertise
CPU Usage	Current status of CPU
Memory Usage	Current memory usage
Storage Usage	Total and current storage usage

5.2. Basic Tab

The user can configure the most common settings for the gateway, such as Gateway Mode, Tx Power, AC Server Address, Remote Assistance, Connection Priority, and Wired/Wi-Fi/Cellular configurations.

The Cassia Bluetooth Gateway supports the following networking uplinks: wired, Wi-Fi, and USB cellular modem.

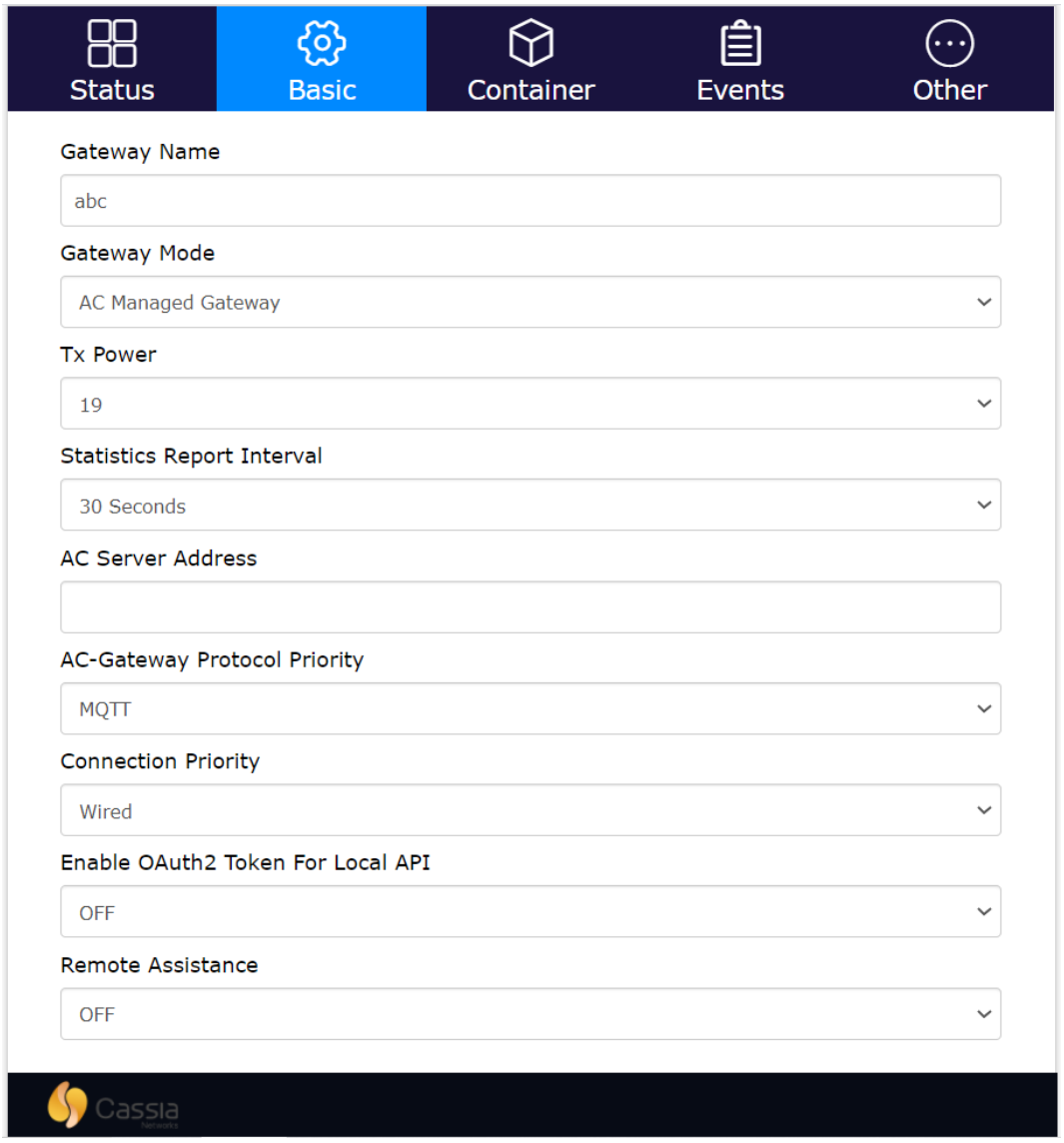
In general, Wi-Fi and cellular networks are less stable and have more interference compared to Ethernet connections. To guarantee good uplink performance, we suggest that the user use Ethernet (wired) for the uplink.

Cassia Bluetooth gateway does not operate in networks with VPN (Virtual Private Network).

Parameter	Description
Gateway Name	From firmware v2.1.1, the user can setup gateway name from the gateway's local webpage. The user can still setup gateway's name from AC as before. This is very useful for the user who doesn't share AC account to the engineers that install the Bluetooth gateway. When a new Bluetooth

	gateway is installed, the user will identify this gateway on AC by the gateway name easily, for example “Gateway 1 in factory A”.
Gateway Mode	AC Managed Gateway or Standalone Gateway
Tx Power	Bluetooth Tx power (limited by local regulatory requirements). The default Tx power of E1000, S2000, and X2000 is 19dBm and is configurable in 3/8/11/15/19 dBm. The default Tx power of X1000 is 20dBm and is configurable in 5/10/13/20 dBm. The Tx power of Japan E1000, S2000, and X2000 is fixed in 8dBm. The Tx power of Japan X1000 is fixed in 10dBm. Tx gain of X2000’s internal Bluetooth antenna is 5.7dbi. If the gain of the external Bluetooth antenna exceeds 5.7dbi, the Tx Power should be decreased to the corresponding value in compliance with local regulations.
External Antenna	Only valid for X2000. “None” means both Bluetooth chips use internal Bluetooth antennas. “Chip 0” means chip 0 uses an external antenna, but chip 1 still uses an internal antenna. “Chip 1” means chip 1 uses an external antenna, but chip 0 still uses an internal antenna. “Both” means both Bluetooth chips use external Bluetooth antennas. This parameter can only be changed on gateway’s local webpage, or through Cassia AC RESTful API. To check if the external antenna is enabled, the user can check if the received RSSI changed. Appendix I (Accessory Options) lists the candidate external antenna and RF cables. These accessories have been verified by Cassia.
Statistics Report Interval	Cassia gateway reports statistical information to AC regularly. The default statistic report interval is 30 seconds. This interval setting can be increased to 1, 2, or 5 minutes. If the user selects a cellular modem in the gateway’s console, “Statistic Report Interval” will be changed to 5 minutes automatically.
AC Server Address	Enter the domain name or IP address of the Access Controller that manages this gateway. **NOTE:** AC server address is mandatory if AC is in the cloud or MQTT is used for gateway and AC communication. If the AC server address is empty, the gateway still can connect to the AC in the same LAN with CAPWAP protocol.
AC-Gateway Protocol Priority	CAPWAP or MQTT. This is the high priority gateway-AC communication protocol. If the gateway can’t connect to AC with this protocol, it will try the low priority protocol automatically. This configuration is available from firmware 2.0.2, and the factory default setting is MQTT. If the gateway was upgraded from lower versions, this value will be CAPWAP.
CAPWAP Port	The communication UDP ports used by your AC and gateway. This setting must be identical to the one set on your AC. Otherwise, your gateway can’t talk to your AC.
Connection Priority	When two or more network connections are activated, you can set priority levels for the networks. By default, the priority is Wired > Wi-Fi > Cellular. For example, if you set priority to Wi-Fi, the new order will be: Wi-Fi > Wired > Cellular
Enable OAuth2 Token For Local API	Enable OAuth2 token for Cassia local RESTful API. The default is off. By the way, if the user uses Cassia RESTful API through AC, please do OAuth 2.0 authentication with the AC using the Developer Key and Developer Secret (in AC setting page). It is not necessary to do

	OAuth on each gateway. For the user using Cassia RESTful API in the container, it is not necessary to do OAuth authentication.
Remote Assistance	Turn this on will enable Cassia engineers to remotely access the gateway for troubleshooting purposes. By default, this function is off.



Cassia gateway configuration page -- Basic

The network uplink traffic between the gateway and the AC includes Bluetooth Low Energy traffic and management traffic. There are two ways to reduce the uplink management traffic.

1. The user can change the Statistic Report Interval to 1, 2, or 5 minutes
2. The user can select MQTT as the Data Path on the AC Settings page in v1.4, or select MQTT as AC-Gateway communication protocol on the gateway web page in v2.0.

Below are examples of network uplink management traffic with different configurations (not including Bluetooth Low Energy traffic).

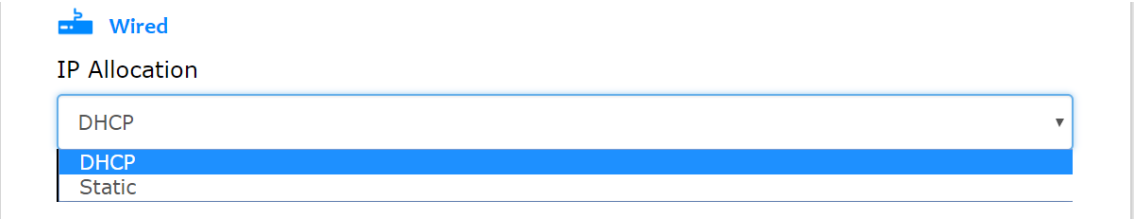
Firmware & Configuration	CAPWAP control + data (MB per month)	CAPWAP control MQTT data path (MB per month)	MQTT control + data (MB per month)
v1.3 (w/o container)	255 (DL 58, UL 197)	N/A in v1.3	N/A
v1.3 (w/ container)	390 (DL 58, UL 332)	N/A in v1.3	N/A

v1.4 (30s, w/o container)	195 (DL 43, UL 152)	165 (DL 50, UL 115)	N/A
v1.4 (30s, w/ container)	215 (DL 43, UL 172)	175 (DL 53, UL 122)	N/A
v1.4 (5min, w/o container)	170 (DL 43, UL 127)	117 (DL 45, UL 72)	N/A
v1.4 (5min, w/ container)	175 (DL 43, UL 132)	123 (DL 48, UL 75)	N/A
v2.0 (30s, w/o container)	The same with v1.4	The same with v1.4	68 (DL 21, UL 47)
v2.0 (30s, w/ container)	The same with v1.4	The same with v1.4	100 (DL 21, UL 79)
v2.0 (5mins,w/o container)	The same with v1.4	The same with v1.4	30 (DL 14, UL 16)
v2.0 (5mins, w/ container)	The same with v1.4	The same with v1.4	34 (DL 14, UL 20)

The network uplink traffic in the production environment depends on the configuration, Bluetooth Low Energy device, etc, and should be evaluated on a case-by-case basis. It is recommended to use scan filter API to reduce Bluetooth Low Energy uplink traffic. Please refer to SDK Implementation Guide for details.

5.2.1. Wired Settings

For a wired connection, please select DHCP (default) or Static IP.



Cassia gateway configuration page – Wired Connection

In Static IP allocation, please enter your network information, including IP, netmask, gateway, and DNS.

For your network setting information, please contact your IT administrator.

5.2.2. Wi-Fi Settings

Cassia's Bluetooth gateway supports Wi-Fi Client mode and Wi-Fi Hotspot mode (2.4GHz only). For the initial deployment, the gateway operates in Hotspot mode by default. This allows the user to connect to the gateway via Wi-Fi using a laptop or mobile device for configuration purposes. The Cassia Bluetooth gateway will advertise an SSID: cassia-xxxxxx (the "x's" correspond to the last 6-digit of the gateway's MAC address). For additional details, see section 4.6.

To use the Wi-Fi as your uplink, please switch the Operating Mode to the Client mode. Please complete the rest of the configuration fields. For details on your Wi-Fi settings, please contact your IT administrator.

From firmware 2.0.3, the user can enable "Verify before saving" before switching to Client mode. If the gateway can't connect to Wi-Fi AP within 30 seconds, it will switch back to Hotspot mode automatically. This function will avoid an un-necessary gateway reset if the user sets the wrong Wi-Fi configuration. If the Wi-Fi client is set to static IP, after the gateway fail to connect to Wi-Fi AP and fall back to Wi-Fi hotspot mode, the hotspot IP address will be changed from 192.168.40.1 to the new static IP.

In Static IP allocation, please enter your network information, including IP, netmask, gateway, and DNS.

NOTE:

1. X1000 and S2000 only support 2.4GHz Wi-Fi. E1000 and X2000 support both 2.4GHz and 5GHz Wi-Fi. Wi-Fi hotspot mode only supports 2.4GHz.
2. The country code should be set correctly when using 5G Wi-Fi. Otherwise, 5G Wi-Fi may not work correctly.
3. Once changed Wi-Fi operation mode to the Client, the gateway will stop sharing the Wi-Fi hotspot and changes the connection to the configured WIFI network. You can enable the Wi-Fi hotspot by setting Wi-Fi operation mode to Hotspot from AC or gateway console. You can find the gateway's local IP address in AC. The local IT department can also find out the gateway's local IP address by accessing the Wi-Fi AP device list or by performing the network scan. In case a static IP is used, the address is known.
4. Before firmware 2.0.3, if there was an error in Wi-Fi SSID, password, or IP address configurations, you cannot access the gateway anymore. Please press the reset button for 10 seconds to reset the gateway.

Cassia gateway configuration page – Wi-Fi Connection

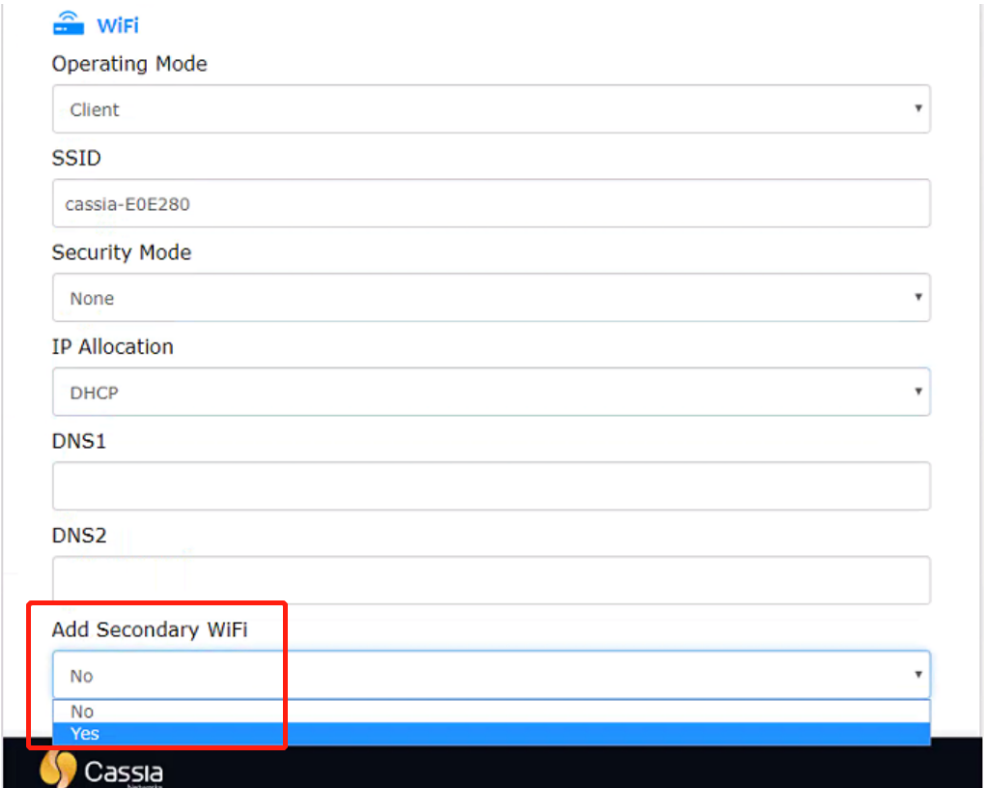
From firmware 1.4 and above, Cassia's gateway supports additional Wi-Fi security modes. The user can choose the Wi-Fi Security Mode, provide the required inputs, and then connect to the Wi-Fi AP with enterprise-level security.

Security Mode	Required Inputs
None	N/A
WPA2-PSK	Password
WPA[TKIP]+WPA2[AES]	Password
[Enterprise]WPA2	• If EAP Type is PEAP-MSCHAPV2, please provide Identify and Password. • If EAP Type is TTLS, please provide Identify, Password, and CA Certificate.
[Enterprise]WPA[TKIP]+WPA2[AES]	

	• If EAP Type is TLS, please provide Identify, Password, CA Certificate, Client Certificate, Private Key, and Private Key Password.

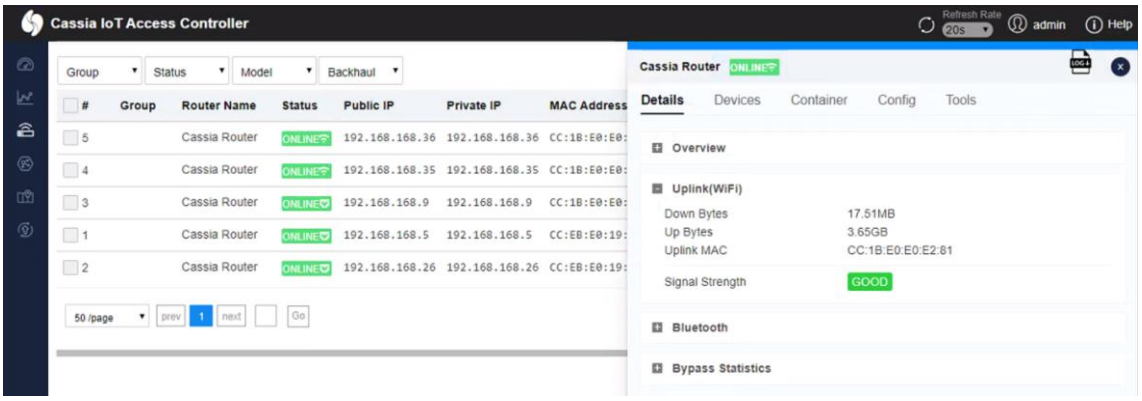
Cassia gateway configuration page – Wi-Fi Security Mode

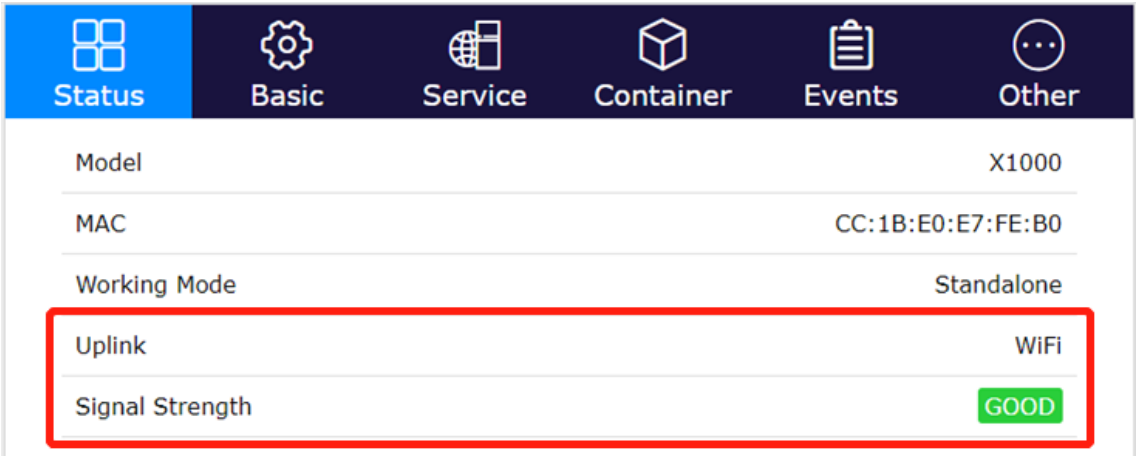
From firmware 2.0, the user can set two Wi-Fi SSID as uplinks for redundancy. Gateway will switch to the secondary Wi-Fi SSID automatically if the first SSID can't be detected or can't be connected. If the secondary Wi-Fi SSID is enabled, both Wi-Fi SSID protocols should be DHCP.



From firmware 2.0, the Cassia Bluetooth gateway will measure the Wi-Fi signal strength and show it on AC (AC->Gateway->Details->Uplink) and gateway console (Status tab) as GOOD, MEDIUM, or POOR. If the signal strength is POOR, please try other Wi-Fi SSID, try 5G Wi-Fi, or try other uplink solutions.

Wi-Fi Signal Strength	Wi-Fi RSSI
GOOD	> -50
MEDIUM	-65 ~ -50
POOR	< -65



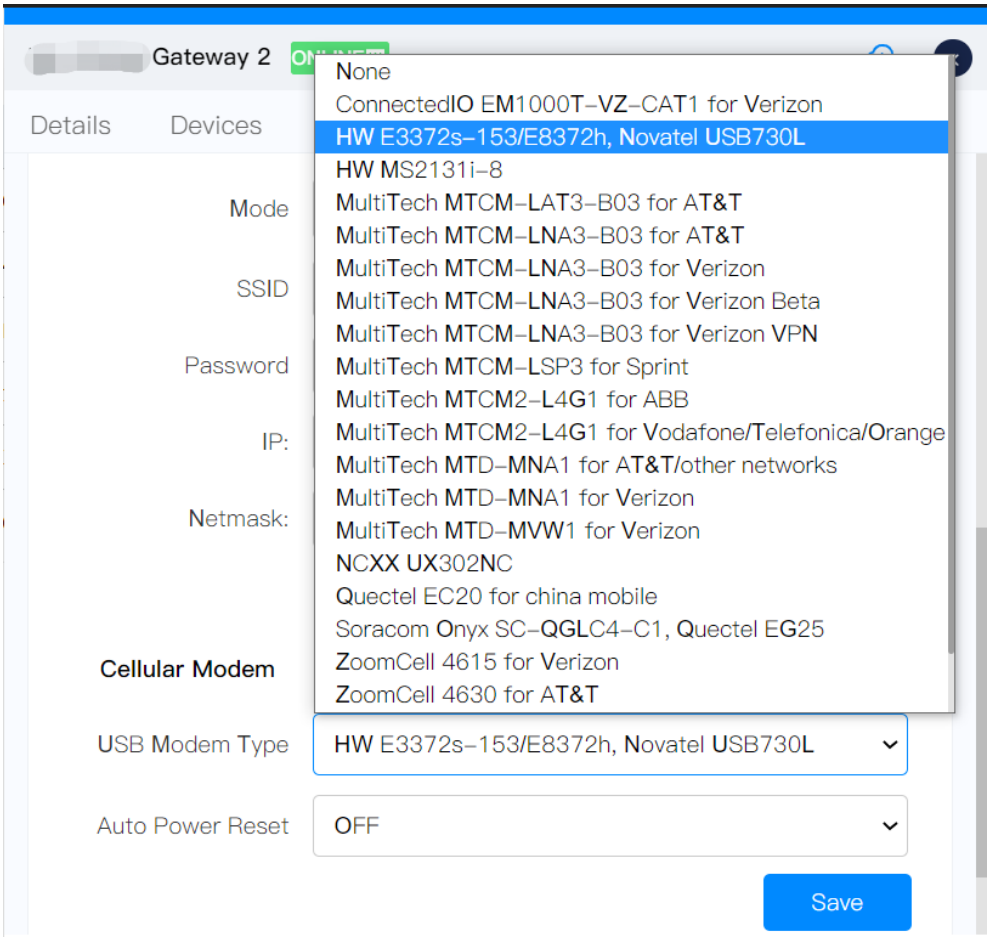


5.2.3. USB Cellular Modem

Cassia's gateway supports USB cellular modem as the network uplink. You will have to purchase a supported USB cellular modem and a SIM card with an active data plan that works with the USB cellular modem.

Before using any USB cellular modem, please connect it to your laptop/desktop to ensure the internet can be accessed with the USB cellular modem. After testing the connection to the internet, please connect the USB cellular modem to the USB port on the Cassia Bluetooth gateway, select the right modem type and configure the parameters, if needed.

Cassia's Bluetooth gateway also supports the use of any USB-powered Wi-Fi modems. In this case, the gateway can connect to the Wi-Fi modem by Wi-Fi uplink (chapter 5.2.2).



Cassia gateway configuration page – USB cellular modem

The USB cellular modem with RNDIS Driver Ethernet Type 1 & Type 2 is supported.

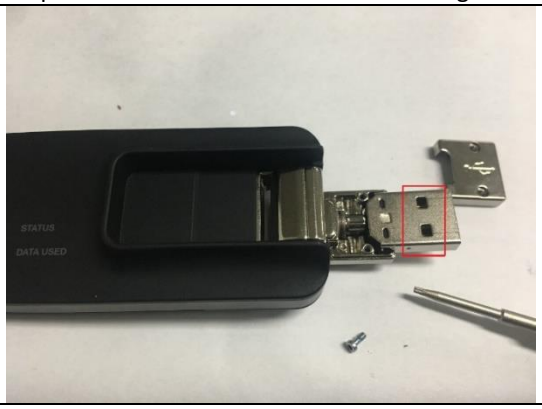
- Type 1: An APN needs to be specified. For example, wyleslte.gw7.vzwentp and 10569.mcs are KORE Wireless APN. If you are using a SIM card from another cellular operator, please contact the cellular operator for the right APN.
- Type 2: It applies the settings automatically and shows the LAN connection. e.g. HW E3372s-153 modem.

Below are the USB cellular modems that can be selected by default:

- HW MS2131i-8
- HW E3372s-153
- HW E3372h-153
- HW E8372h-153 (Europe, support 2G)
- HW E8372h-155 (China, doesn't support 2G)
- HW E8372h-320 (Europe, added in firmware v2.1.1, doesn't support 2G)
- HW E8372h-820 (China, added in firmware v2.1.1, doesn't support 2G)
- Novatel USB730L (for Verizon)
- MultiTech MTD-MVW1 (for Verizon)
- MultiTech MTD-MNA1 (for Verizon, AT&T, and other Cellular operators)
- MultiTech MTCM-LAT3-B03 (for AT&T, T-Mobile, and other Cellular operators)
- MultiTech MTCM-LNA3-B03 (for AT&T, Verizon and Verizon VPN)
- MultiTech MTCM-LSP3-B03 (for Sprint)
- MultiTech MTCM2-L4G1 (for Vodafone, Telefonica and Orange)
- Zoom 4615 (for Verizon)

- Zoom 4630 (for AT&T, T-Mobile, and other Cellular operators)
- ConnectedIO EM1000T-VZ-CAT1 (for Verizon)
- NXCC UX302NC (for DoCoMo)
- Soracom Onyx SC-QGLC4-C1
- Quectel EC20 (for China Mobile)
- Quectel EG25

To fit USB730L into the bottom enclosure of the X1000, the USB connector of U730L should be turned over. Please follow the steps below.

Step 1: Remove the two screws of the USB connector	Step 2: Remove the cover with the USB logo
	
Step 3: Turn over the USB connector	Step 4: Put the cover and the two screws back
	

New USB cellular modems may be used by selecting USB Modem Type “Custom”. Below is the custom configuration example of cellular modem AK-020. For USB cellular modem and SIM card related information, please contact the cellular carrier.

Cellular Modem Parameter	Value
Interface Name	ppp0
Protocol	3g
APN	3gnet
Service	umts
Dial Number	*99#
Device	/dev/ttyUSB0
Default Route	1
Peer NDS	1
IPV6	1

With a USB cellular modem, the Cassia Bluetooth gateway needs to be in a place where there is good cellular network coverage. From firmware 2.0, the user can check the cellular signal strength on AC (AC->Gateway->Details->Uplink) or gateway console

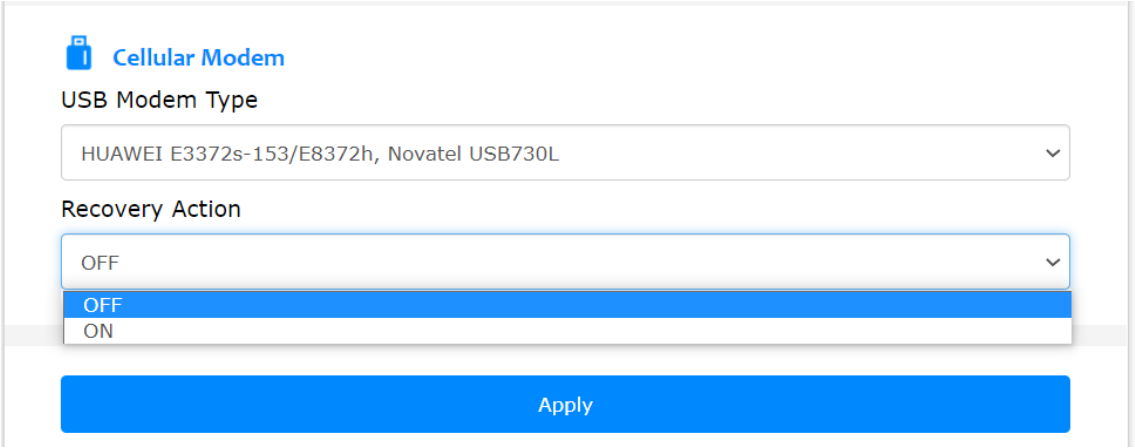
(Status tab) as GOOD, MEDIUM, or POOR. If the signal strength is POOR, please try SIM cards from other cellular operators or try other uplink solutions. Only MultiTech cellular modems, HW cellular modems and ConnectedIO EM1000T-VZ-CAT1 support the showing of cellular signal strength.

Below is the mapping for MultiTech and HW cellular modems.

Cellular Signal Strength	MultiTech	HW
GOOD	> 14	4 and 5
MEDIUM	9 ~ 14	3
POOR	< 9	1 and 2

What is more, from firmware 2.0.3, the user can see IMEI and IMSI on AC (AC->Gateway->Details->Uplink) and gateway console for MultiTech cellular modems and HW MS2131i-8. If the user changed the default setting of parameter “Device” for MultiTech cellular modems, the value of RSSI, IMSI and IMEI may become wrong.

Cassia gateway supports USB cellular modem auto recovery function. After setting “Recover Action” to ON, Cassia gateway will power reset the USB cellular modem (X2000) or reset the USB interface (other gateways) if it can’t reconnect to the cellular network in 10 minutes. For an AC managed gateway, if the cellular connection can’t be recovered in one hour, the gateway will soft reboot automatically. All cellular modems connected by USB port are able to support this function.



From firmware 2.1.1, the user can choose to not using LTE lower frequency bands (lower than 1GHz) on below USB cellular modems by switching off option “LTE Low Frequency Band”. This function will increase the stability for the gateway using below USB cellular modems.

- MultiTech MTCM-LNA3-B03 (for AT&T, Verizon and Verizon VPN)
- MultiTech MTCM2-L4G1 (for Vodafone, Telefonica and Orange)
- Soracom Onyx SC-QGLC4-C1

5.3. Container Tab

From firmware 1.3 and above, Cassia’s Bluetooth gateway E1000, X1000, and X2000 support custom applications in the container (OS is Ubuntu 16.04.3).

NOTES for v2.0.3 firmware

- Before firmware 2.0.3, when HTTPS is enabled on the gateway, the Cassia API URL used in the container APP should be updated to use port 443. From firmware 2.0.3, port 80 between container and gateway firmware is always enabled, so APP doesn't need to be updated regardless of the gateway's HTTPS settings.

NOTES for v2.0.2 firmware

- After upgrading gateway firmware to 2.0.2, if the APP uses BlueZ with Gatttool and Bluetoothd (e.g. noble or python Bluetooth lib) instead of Cassia Bluetooth stack and Cassia RESTful API, **please change 'Cassia Bluetooth Stack' to close** (in AC console -> Gateway -> Config-> Bluetooth Setting, or gateway console -> Other -> Bluetooth Setting, default is open). Otherwise, Bluetooth operations in the APP may return failure.

  Cassia Bluetooth stack and Cassia RESTful API offer the state of the art Bluetooth scan and connection performance. It is highly recommended to keep the Cassia Bluetooth stack open and use Cassia RESTful API to achieve the best performance Bluetooth IoT system.

- From firmware 2.0.2, an option to enable and disable container local SSH login is added in the Container tab. The container local SSH login is OFF by default for security reasons. Please turn it ON, before you want to local SSH login the container. Reset gateway will change this option into the default value OFF.

- From firmware 2.0.2, the output of the RESTful API to obtain gateway configuration from AC will be changed (GET http://{your AC domain}/api/cassia/info?mac=<hubmac>). The container status will be removed from the default API output, to avoid the oversized UDP packets problem. Container status can be got separately by the same API with the additional parameter 'fields=container'. Please refer to SDK WIKI for details.

- From gateway firmware 2.0.2, DNS name server in Cassia Bluetooth gateway will be propagated into container /etc/resolv.conf. Besides two default DNS name servers 8.8.8.8 and 114.114.114.114 , the container will use the DNS setting in the Network section of the gateway webpage Config tab as an additional DNS name server. This feature solves the problem that the firewall blocks two default DNS servers.

Legacy NOTES

- **Please remember to change the container SSH password upon the first login.**

- Please implement APP log rotation to avoid flooding container storage. From v1.4.3, the container can use up to 2.3GB. For the gateways with firmware lower than v1.4.3, if APP log floods gateway storage, the gateway may be offline and can't recover by a reboot. The user has to press the factory reset button to reset the gateway and then delete the container.

- It is suggested to keep the memory usage in the container below 70%. The other 30% is for peak hours and abnormal cases. It means the container should use less than 90MB, which includes memory used by custom application and all the tools running in

the container.

- Reset container will delete and re-create the container. The files under /opt will be kept, and the custom APPs not under /opt will be deleted.
- Factory reset gateway will not impact the container, APP, and container files.
- If you want to upgrade an existing APP, please make sure that the name and/or version is different.
- Cassia gateway container uses a compact version of Ubuntu. Certain packages may not be pre-installed and/or available.
- Please consider compiling your application code in a full development environment before loading and attempting to run in the container.
- The user has SSH/root access to the Ubuntu container. However, Ubuntu is running as a container, so its core cannot be modified, and the properties of sysfs, e.g. /proc, is read-only.
- Please make sure the ports in chapter 4.3 are opened outbound on the gateway side firewall. The user can check if a TCP port is opened by using Netcat on the gateway's console

The container and APP share CPU, memory, and storage with the host gateway. Please check the below table for more information. When there is no APP installed, the container CPU usage is usually lower than 5%, the container memory usage is usually lower than 1%, and there is about 1.1 GB storage free (container uses about 1.2 GB)

Type	S2000	E1000	X1000	X2000
Support edge computing	No	Yes	Yes	Yes
Maximum memory can be used by container and APP	N/A	128 MB	128 MB	700 MB
Maximum CPU can be used by container and APP	N/A	2 cores, 1.5 GHz	2 cores, 1.5 GHz	2 cores, 1.5 GHz
Maximum storage can be used by container and APP	N/A	2.3 GB	2.3 GB	2.3 GB

The first container version is v1.1.1 (can be installed on all gateway versions). The latest container version is v2.0.1 (can only be installed on gateway firmware 2.1.1 or higher version). Please check below table for the major difference. The user can keep using v1.1.1 container if they don't need the new features in v2.0.1 container. Please verify your APP together with the new container carefully before rolling out new container to more gateways, since the Ubuntu version changed and the pre-installed utilities and packages are different.

Please download the container firmware from the link below (this page is password protected, please get in touch with your Cassia sales representative for assistance): https://www.cassianetworks.com/support/knowledge-base/router-gateway-firmware/

Difference	Container v1.1.1	Container v2.0.1
Gateway firmware	Any version	v2.1.1 or higher version
Container OS	Ubuntu 16.04.3 LTS	Ubuntu 20.04.2 LTS

Default SSH password (username is “cassia”)	cassia	cassia-xxxxxx (xxxxxx is the last 6 characters of gateway MAC in lowercase, e.g. the SSH password of gateway CC:1B:E0:E0:8E:B4 is cassia-e08eb4)
Default root password	Default password of root user is “cassia”	Please run command “sudo passwd root” to set password for root user before running “su -”
Pre-installed utilities and packages	Please check below table	Please check below table
ASP.NET support	ASP.NET Core not pre-installed	ASP.NET Core 3.1.16 pre-installed

Below is the list of utilities and packages pre-loaded in container v1.1.1 and v2.0.1.

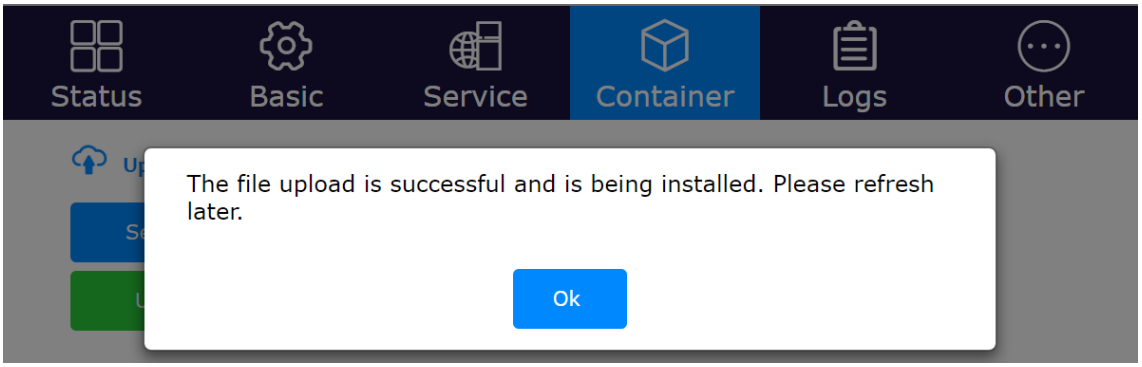
Name	Container 1.1.1	Container 2.0.1
BlueZ	5.37	5.53
Bluetoothd	5.37	5.53
Dbus	1.10.6	1.12.16
Python 2	2.7.12	2.7.18
Python 3	3.5.2	3.8.5
Python Pip	8.1.1	20.0.2
python-gobject	3.20.0	3.34.0
dbus	1.10.6	1.12.16
python3-dbus	No	1.2.16
Node	6.11.5	10.19.0
Nodejs	4.2.6	10.19.0
NPM	3.10.10	No
node-gyp	6.11.5	No
noble	4.4.6	No
GCC	5.4.0	9.3.0
G++	5.4.0	9.3.0
curl	7.47.0	7.68.0
ASP.NET Core	No	3.1.16

Please follow the steps below on the gateway console to install the container. The detailed installation and deployment guide can be found in Cassia Custom Application Deployment Instructions in https://www.cassianetworks.com/support/knowledge-base/general-documents/.

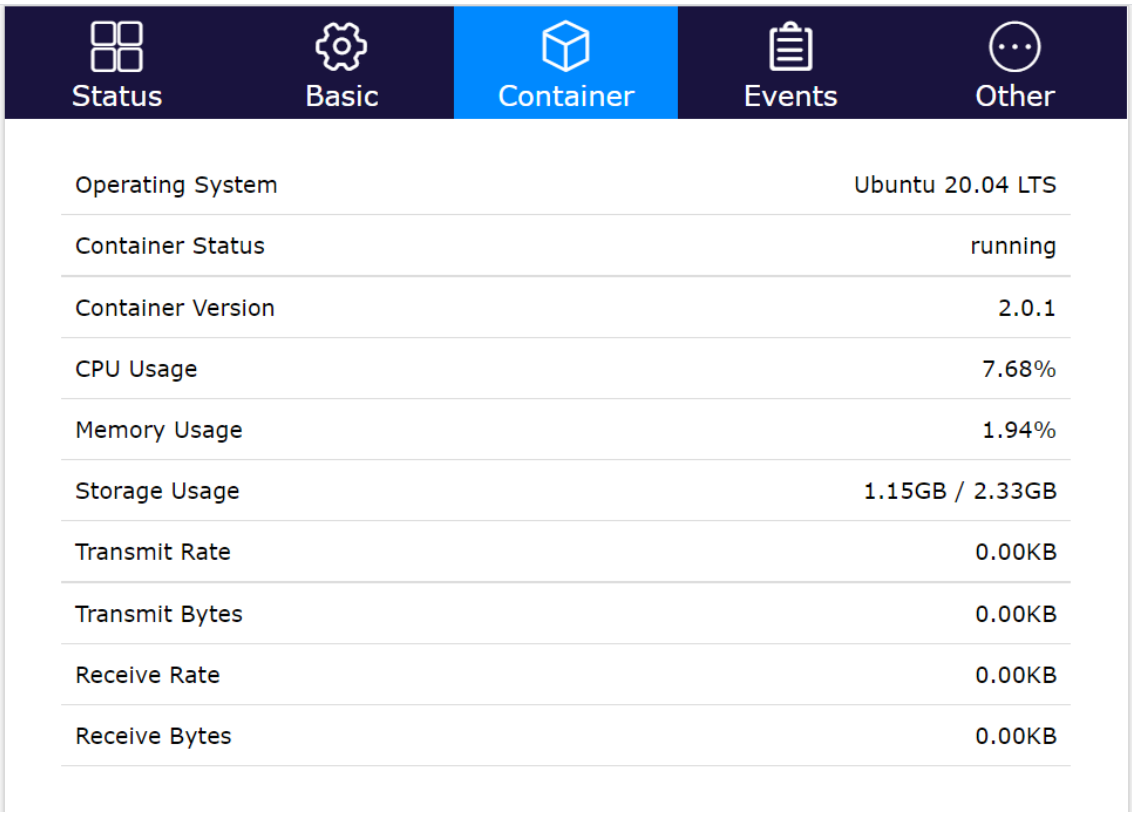
From firmware 1.4.2, the user can install a container from a smartphone locally. Please save the container firmware on your smartphone in advance and login gateway’s local console from the Wi-Fi hotspot (2.4GHz only) or the gateway’s private IP.

Select and install container firmware:

The container will be uploaded and installed on the gateway.



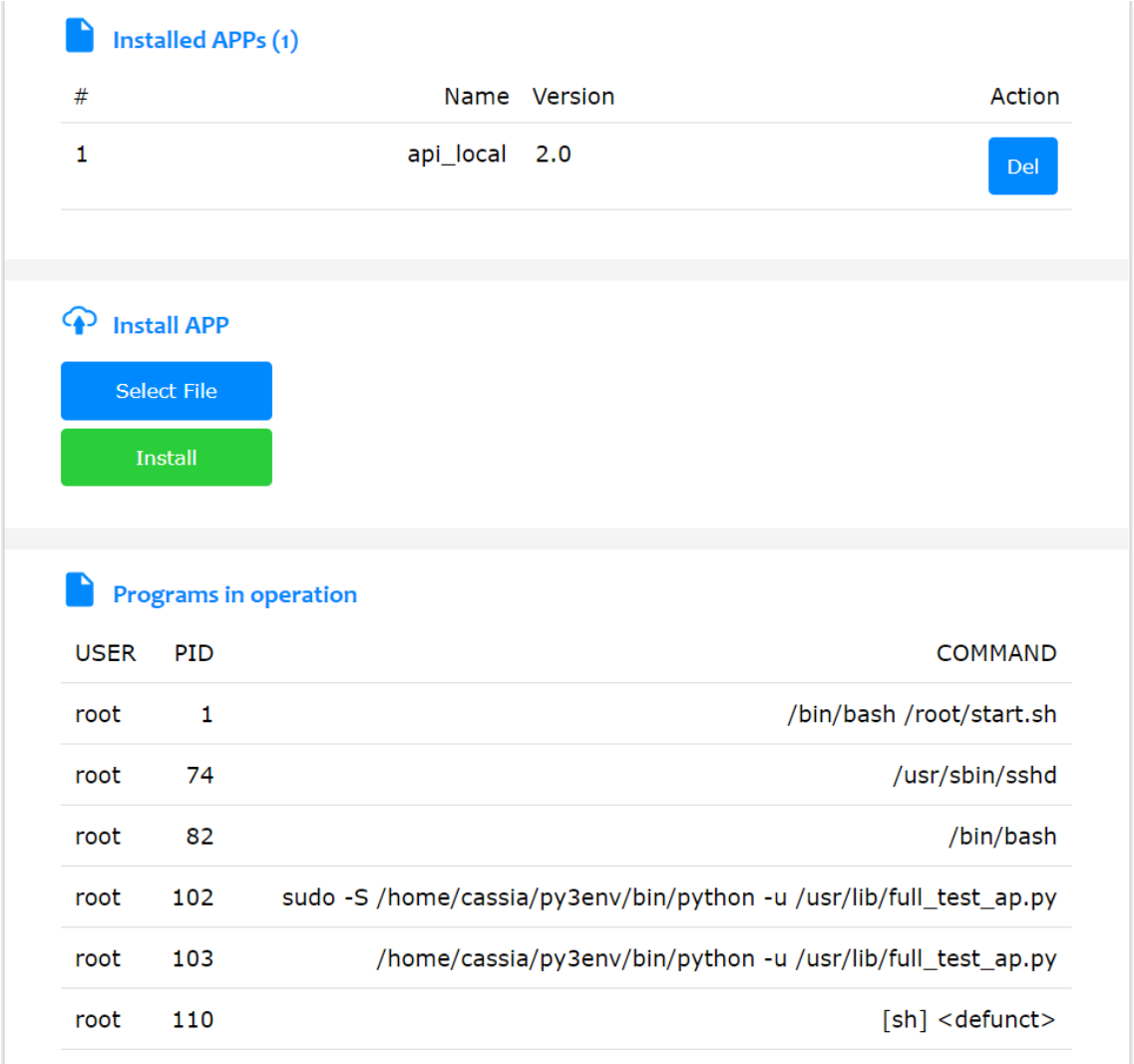
Please refresh the web browser. You will see the information of the container and the custom application.



Cassia gateway configuration page -- Container

The Container tab page displays Operating System, Container Status, Container Version, Storage Usage, Transmit Rate, Transmit Bytes, Receive Rate, Receive Bytes, CPU Usage, and Memory Usage of the container.

Parameter	Description
Operating System	The core of the container, e.g. Ubuntu 16.04.3 in release 1.3
Container Status	Working status of the container
Container Version	The firmware version of the container
Storage Usage	Storage usage and reserved by the container (out of 2.3GB storage)
Transmit Rate	Transmit Rate by the container
Transmit Bytes	Transmit Bytes by the container
Receive Rate	Receive Rate by the container
Receive Bytes	Receive Bytes by the container
CPU Usage	CPU used by the container (out of 2 CPU cores)
Memory Usage	Memory used by the container (out of 128MB RAM for E1000 and X1000, and out of 700MB RAM for X2000)



Cassia gateway configuration page – Container cont.

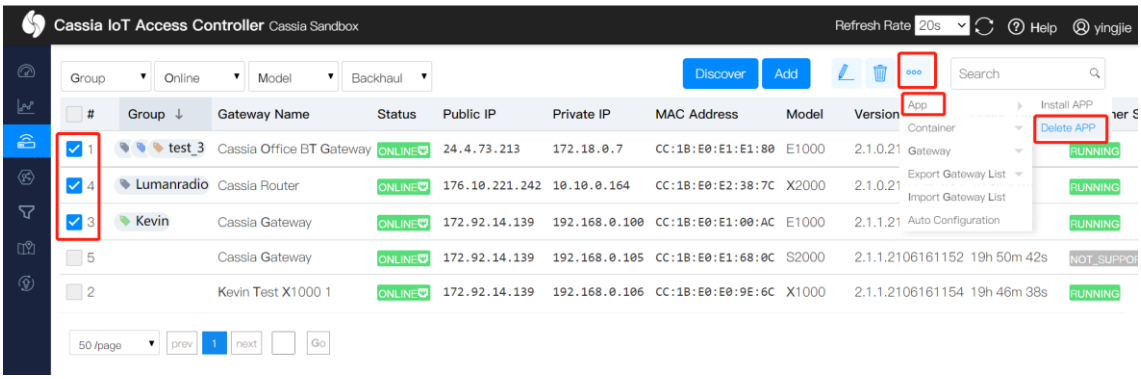
The Container tab page also displays the installed APP on the container and the programs in operation.

The user can update the APP by clicking the button “Select File and Install”. From firmware 2.1.1, container and APP can be continuously downloaded after being disrupted (MQTT

should be used between gateway and AC). From firmware 1.4.2, the user can update the APP from the smartphone locally. Please save the APP on your smartphone in advance and login gateway's local console from the Wi-Fi hotspot (2.4GHz only) or the gateway's private IP.

From firmware 2.0.3, the user can delete the installed APP by clicking the Del button. This action will delete /root/apps/${app_name}.sh and /root/apps/${app_name}.version, but will remain all other APP files unchanged (avoid deleting important customer data). Please delete the other APP files, if necessary, by adding delete script (recommended, available from firmware v2.1.1), adding codes in autorun.sh of the new APP, or by SSH into the container.

The user can also follow the below steps to install or delete APP for a batch of gateways.



After the container is installed, the gateway and container will be in the same subnet. The IP address of the gateway is 10.10.10.254/24. The IP address of the container is 10.10.10.253/24.

```
cassia@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:16:3e:28:51:9d
          inet addr:10.10.10.253  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::216:3eff:fe28:519d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:883532 errors:0 dropped:0 overruns:0 frame:0
          TX packets:855270 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:210580223 (210.5 MB)  TX bytes:56505328 (56.5 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1250 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1250 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:116330 (116.3 KB)  TX bytes:116330 (116.3 KB)
```

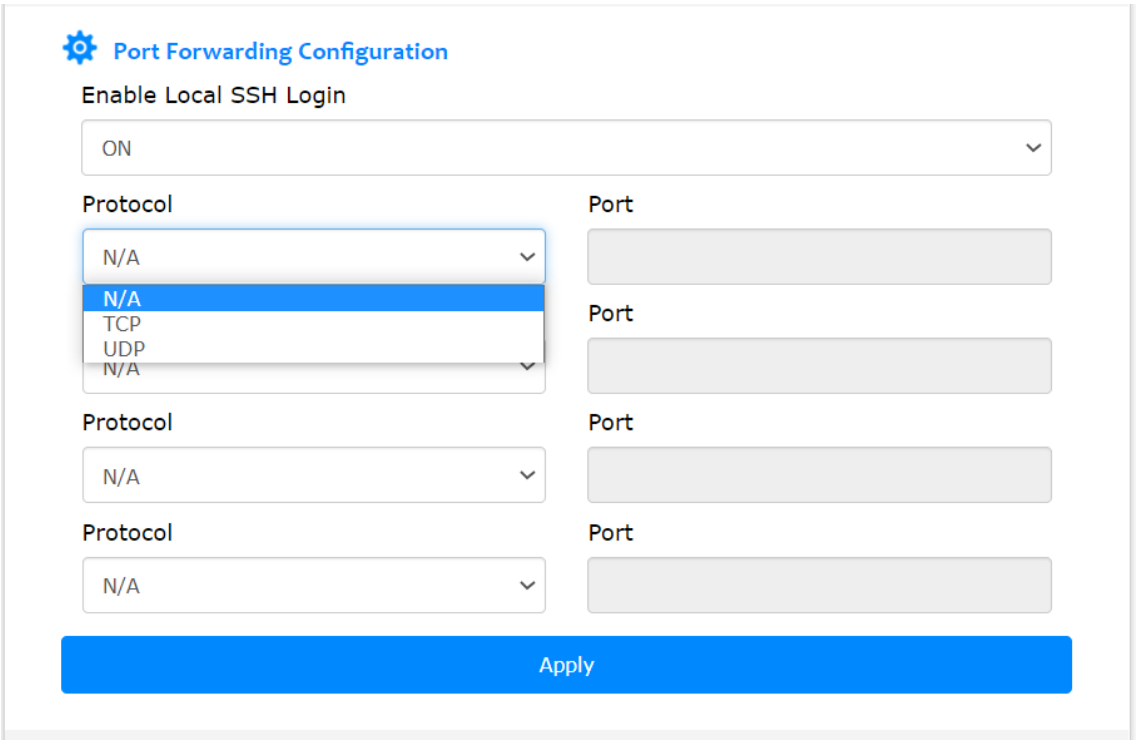
APP in the container can call local RESTful API like below (Turn on scanning as an example).

$curl –v 10.10.10.254/gap/nodes/?event=1&active=1

```
cassia@ubuntu:~$ curl -v http://10.10.10.254/gap/nodes/?event=1
*   Trying 10.10.10.254...
* Connected to 10.10.10.254 (10.10.10.254) port 80 (#0)
> GET /gap/nodes/?event=1 HTTP/1.1
> Host: 10.10.10.254
> User-Agent: curl/7.47.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Server: nginx
< Date: Fri, 27 Mar 2020 14:04:35 GMT
< Content-Type: text/event-stream
< Transfer-Encoding: chunked
< Connection: keep-alive
< Access-Control-Allow-Credentials: true
< Cache-Control: no-cache
< Access-Control-Allow-Headers: Content-Type
< X-Powered-By: Cassia
< Access-Control-Allow-Origin: *
< Access-Control-Allow-Methods: GET,POST,PUT,DELETE
<
:keep-alive

data: {"name":"(unknown)","evtType":3,"rssi":-65,"adData":"1EFF060001092002360D61D3C1BD
A805DF34AFD924B0662B308CC3FDDA88702","bdaddrs":[{"bdaddr":"19:36:03:67:DE:F7","bdaddrT
ype":"random"}]}
```

From firmware 1.4.1, the user can configure a maximum of four TCP or UDP ports for container port forwarding. By using this functionality, the user can set up a server (e.g. a web server) in the container and access it via the gateway's private IP address and the configured port. The port range is [60000, 65525]. N/A means the port is closed.

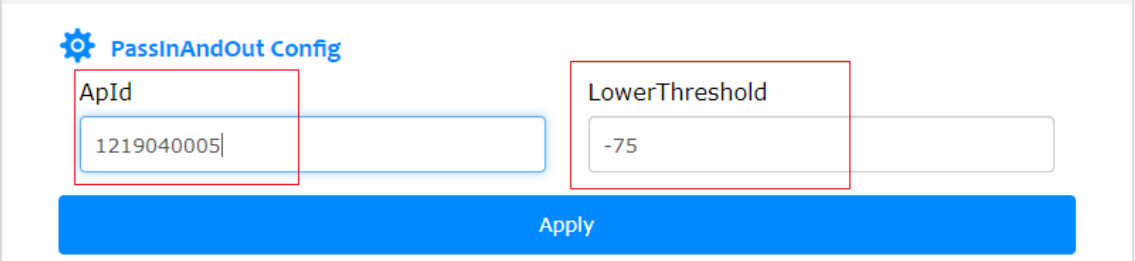


Cassia gateway configuration page – container continued

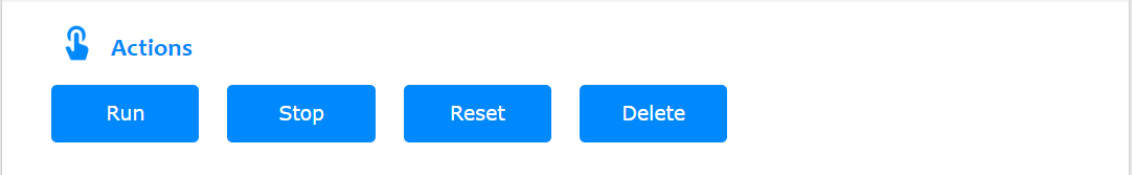
From firmware 1.4.1, the user can add their own APP configuration console in Cassia gateway's local console and AC's console.

First, please add meta.json (defines the configuration items) in the APP package. After that, the user can find their APP configuration console on the gateway local console and AC

console. After the configuration, the gateway will generate file config.json under folder /root/config/<app_name>/.



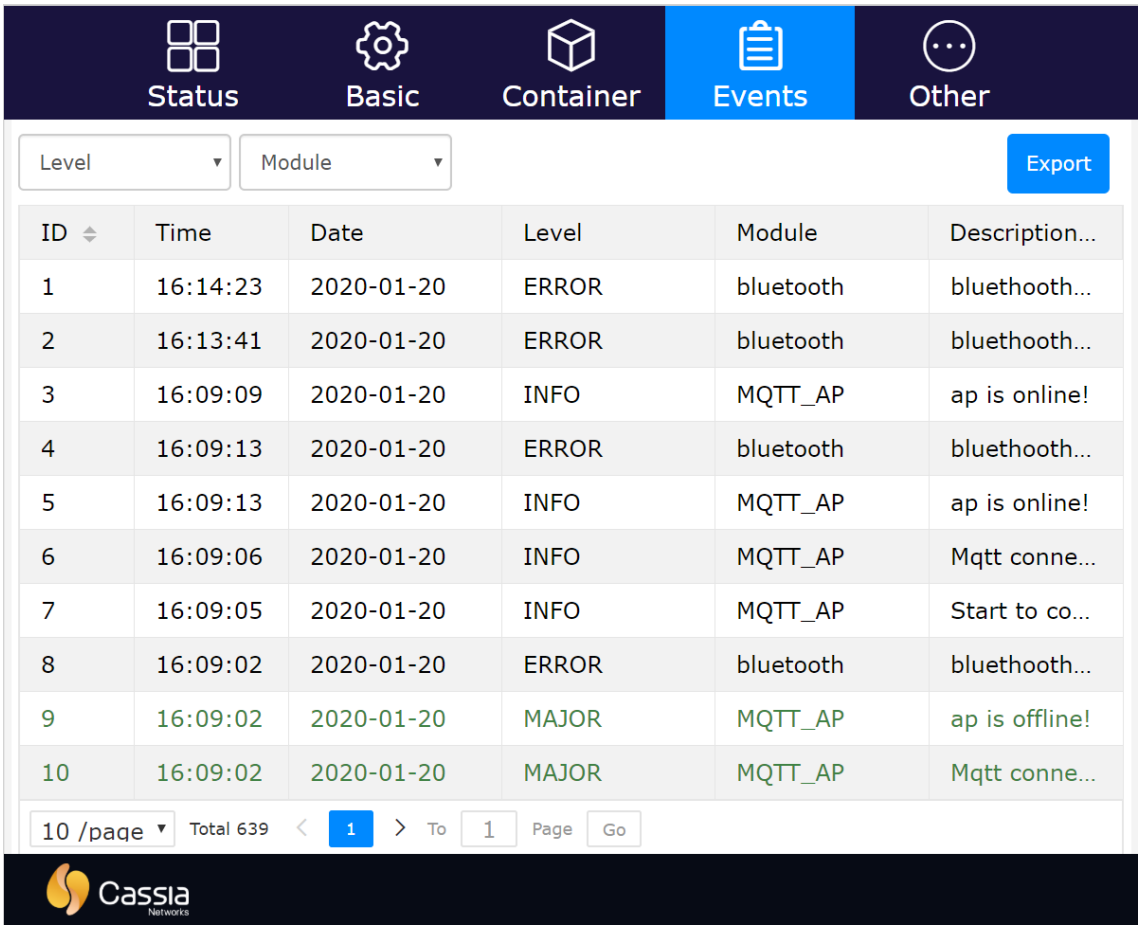
The user can also Run, Stop, Reset or Delete the container by clicking the buttons.



For more information, please check Cassia Custom Application Deployment Instructions here: https://www.cassianetworks.com/support/knowledge-base/general-documents/.

5.4. Events Tab

The Events tab page displays events of different Level (Info, Major, etc.) and different Module (Web, Bluetooth, MQTT, WTP, Network, etc.). The user can click the Export button to export the logs for further analysis.



Cassia gateway configuration page – Event

5.5. Other Tab

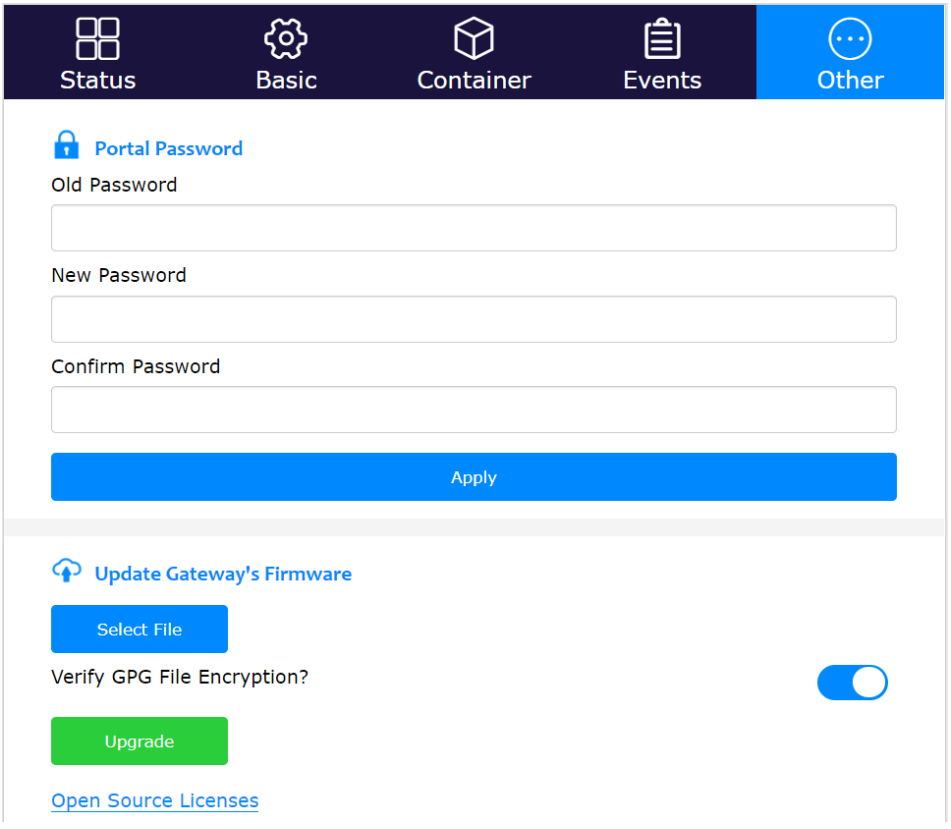
The Status tab page displays the gateway's login password (Portal Password). When logging in for the first time, the gateway's console will require the user to set the login password, which should include numbers, letters, and special characters. The password length should be between 8-20. If the user forgets the gateway login password, they can reset it through the AC. The read only AC account doesn't have the permission to reset the gateway's login password.

The user can update the gateway's firmware from AC or gateway local console by clicking the "Select File and Upgrade" button. From firmware 2.1.0, gateway firmware can be continuously downloaded after being disrupted.

If the firmware image is encrypted with *.gpg, please switch on "Verify GPG File Encryption?". Please turn it off, if the firmware image is *.gz file format. From 2022 May 1st, Cassia will only deliver gpg format firmware for Cassia Bluetooth gateway types, except for S2000.

From firmware 1.4.2 and above, the user can update the gateway's firmware from a smartphone locally. Please download the gateway firmware onto your smartphone in advance and log into the gateway's local console from the Wi-Fi hotspot (2.4GHz only) or the gateway's private IP.

The latest firmware download is available here (this page is password protected, please get in touch with your Cassia sales representative for assistance): https://www.cassianetworks.com/support/knowledge-base/router-gateway-firmware/.



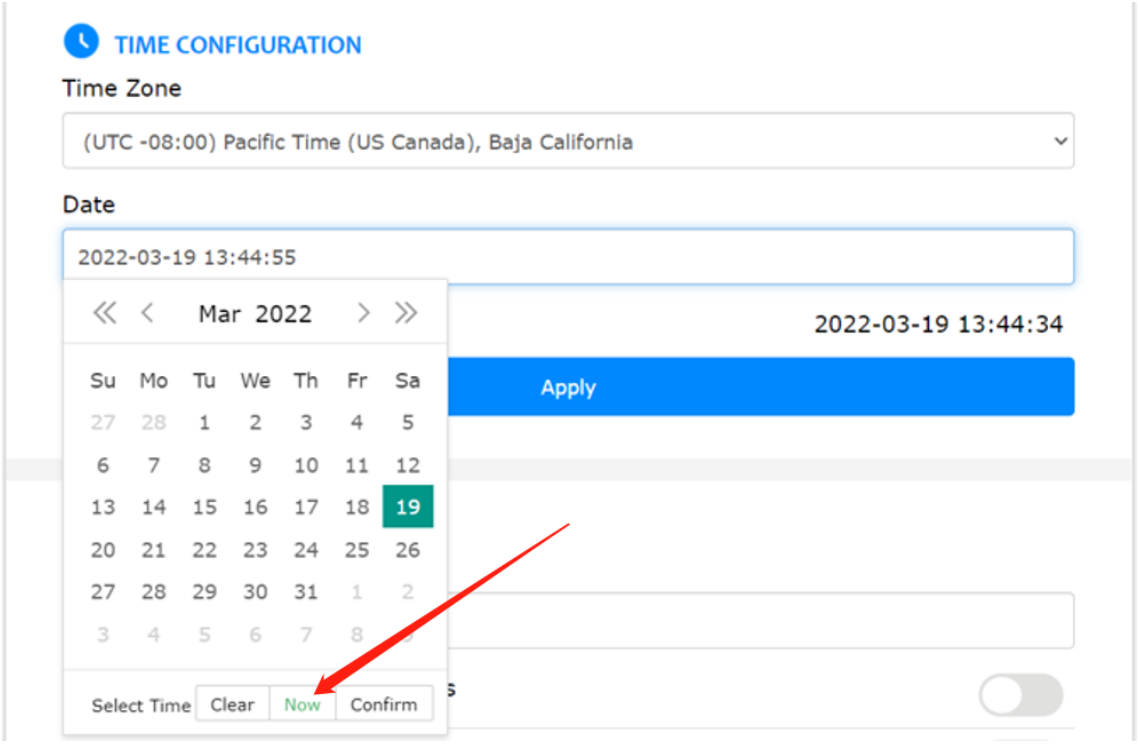
Cassia gateway configuration page – Other

You can set the gateway's local time zone and local time.

The gateway will always use its local time zone, because the gateway and AC might be in different time zone. The gateway's default local time zone is UTC +08:00. From firmware 2.1.1, in order to support day saving time, the time zone setting on AC and gateway is changed from zone based to location (country or city) based.

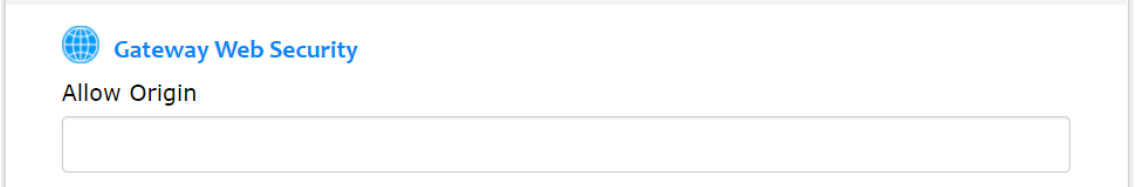
The gateway's default local time is 1970-01-02, 00:00:00. Customer can set the gateway's local time when necessary, for example before filling in the SSL certificates in gateway (see Appendix E, 3.1). After connecting to AC, the gateway will synch its time with the AC automatically.

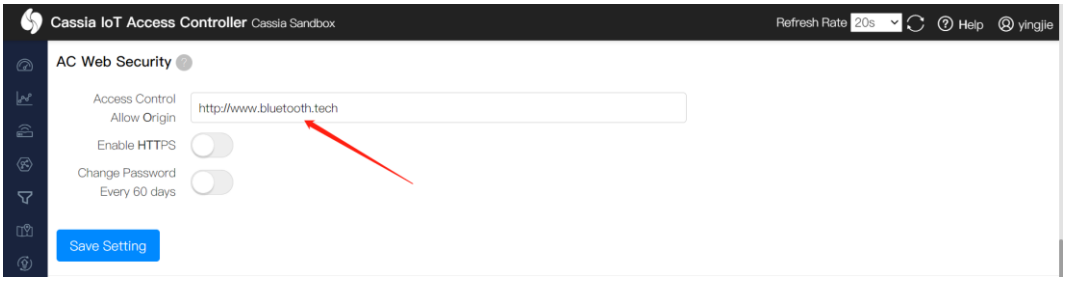
Below is an example.



From firmware v2.0.3, CORS is disabled by default on AC and Router due to security reasons. Client-side scripts (e.g. JavaScript) are prevented from accessing the AC webpage and gateway local webpage, unless "Access Control Allow Origin" in AC settings and "Allow Origin" in gateway webpage is set.

For example, when using the Bluetooth debug tool, please set "Access Control Allow Origin" and "Allow Origin" to * or the URL of the requesting page http://www.bluetooth.tech. Please refer to http://www.bluetooth.tech/debugger2/dist/Debugger2-Troubleshooting.pdf for detailed instruction.

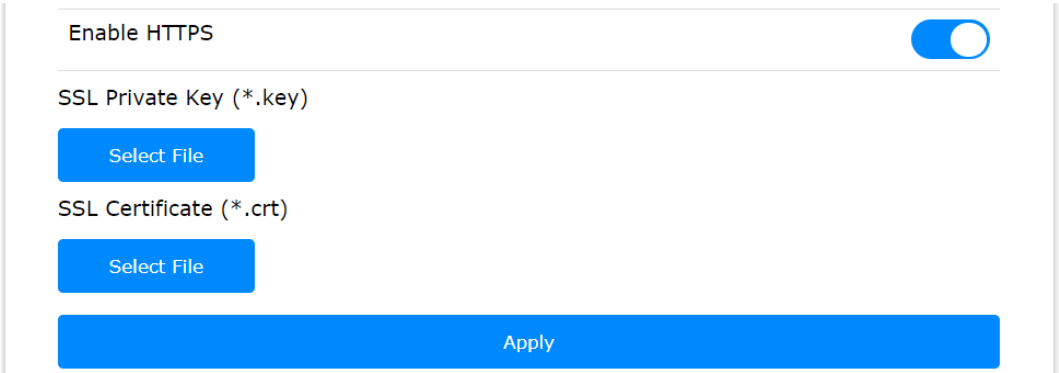




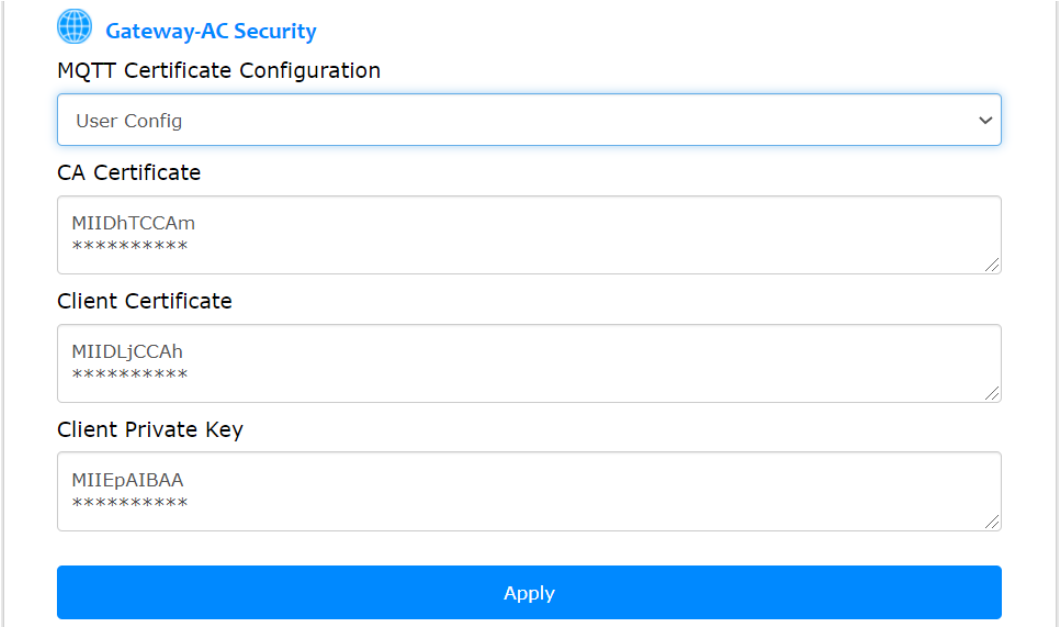
If you want to use HTTPS to access the gateway web or call local RESTful API, please switch on “Enable HTTPS” and provide the SSL Private Key and SSL Certificate files.

Below is an example for generating a self-signed certificate. It is suggested to use CA-signed certificates to secure security.

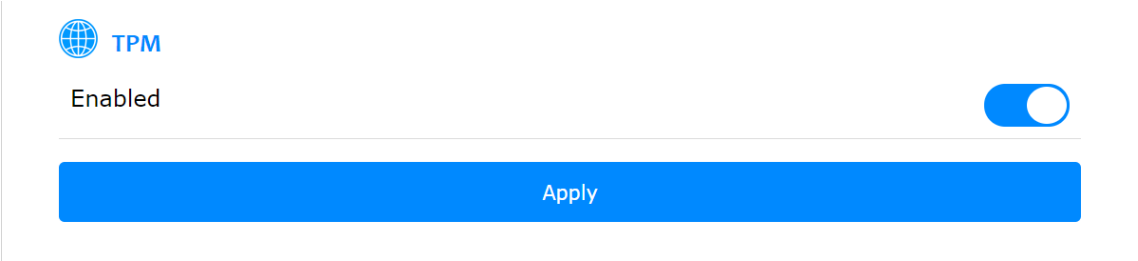
```
openssl genrsa -des3 -out ca.key 2048
openssl req -new -x509 -key ca.key -out ca.crt -days 3650
openssl genrsa -out server.key 2048
openssl req -new -key server.key -out server.csr
openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt
```



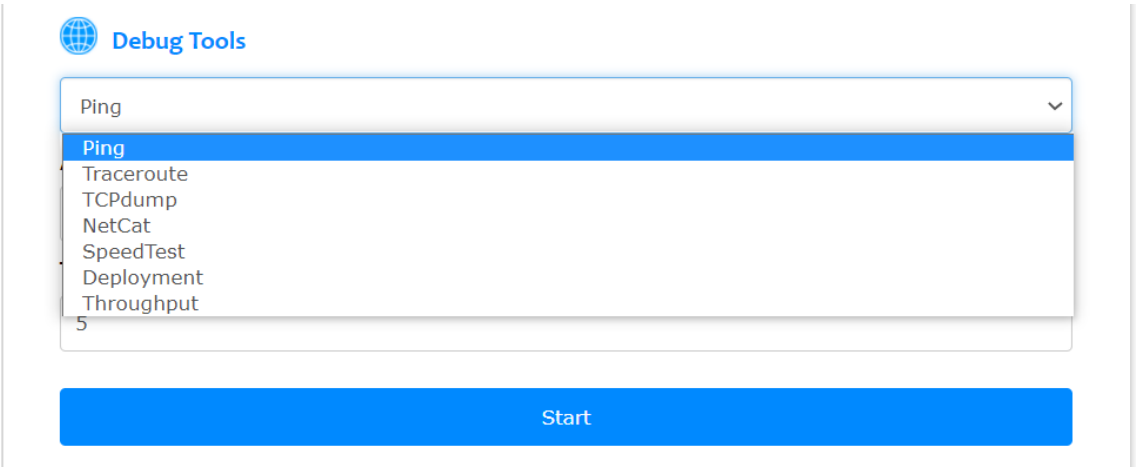
The user can import a dedicated SSL Private Key and SSL Certificate for the secure communication between gateway and AC. Cassia gateway always uses secured CAPWAP and MQTT to communicate with AC, no matter if default or custom certificates are used.



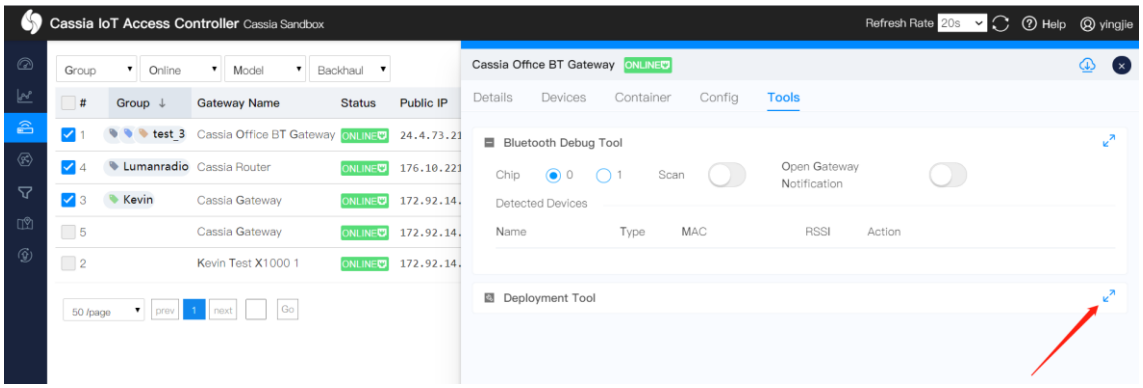
The user can enable TPM (Trusted Platform Module) on X2000 to further enhance the safety level. Please note, the startup time of X2000 will increase from 40 seconds to about 80 seconds. By default, the TPM will be disabled. This configuration is only available on the gateway website.



From firmware 1.4, the user can run network debug tools Ping, Traceroute, TCP dump, and NetCat on the gateway's local console. From firmware 2.0.3, the user can run Speed Test too. Speed Test will not work if the gateway has multiple uplinks, e.g. Ethernet and Wi-Fi are connected at the same time. These debug tools will help on-site engineers to identify network issues. S2000 only support Ping, Traceroute, NetCat and Deployment tool.

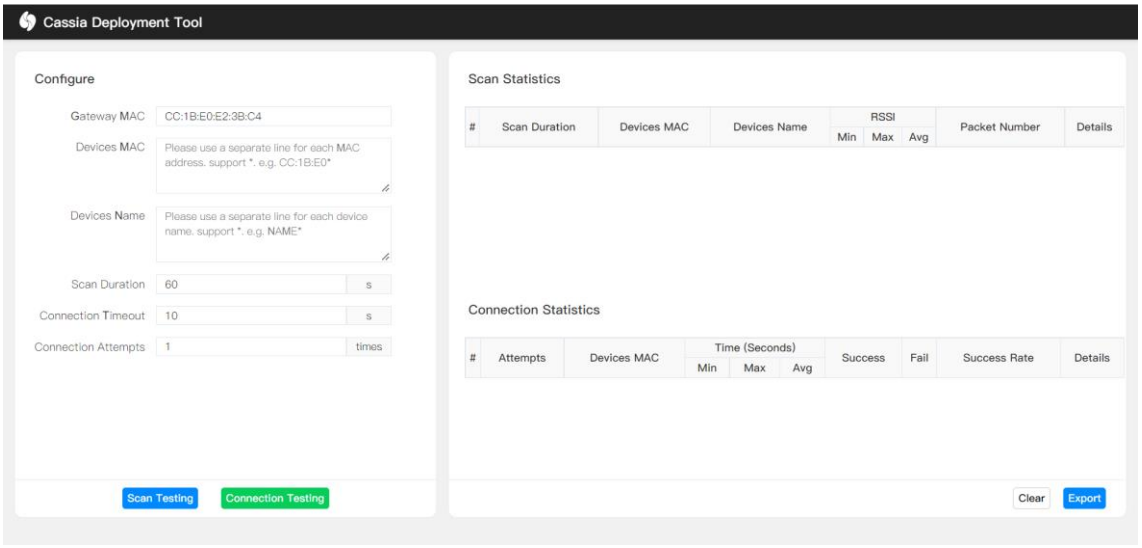


From firmware 2.1.0, the user can run the deployment tool by selecting "Deployment" in the gateway's local console, or run it from the AC console tools tab. Deployment tool can help the user to assess the gateway and device's Bluetooth performance during the planning and deploying phase.

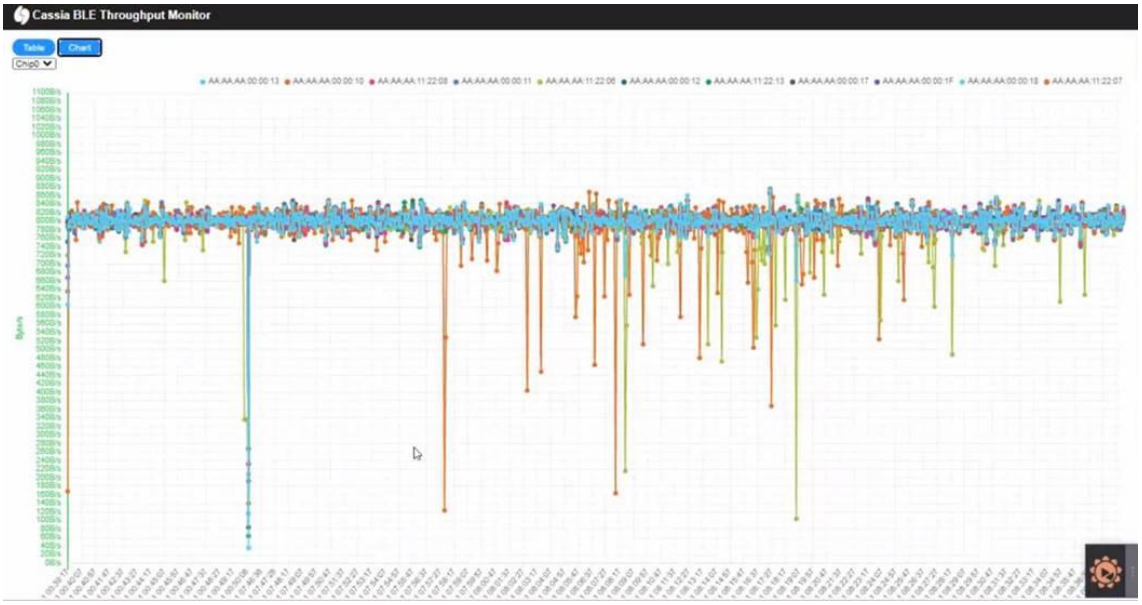


The customer can check the scan and connect performance in real-time, including RSSI, the number of scanned packets, scan and connect duration, connection success and failure

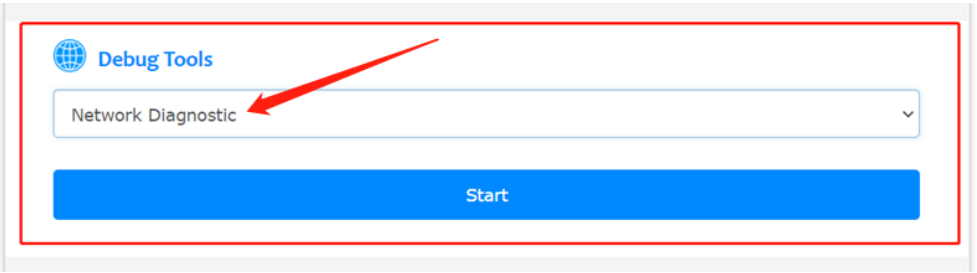
rate, etc. Device name filter and MAC filter with wildcard are supported. To get the correct display format, please use the Deployment tool on the computer only.



From firmware 2.1.0, the user can run the Bluetooth Low Energy throughput monitor tool by selecting “Throughput” in the gateway’s local console. This tool can show how many Bluetooth Low Energy connections on each chip and show the throughput of all the connections or part of them. The user can check the result in chart format (not supported by S2000) or table format. To get the correct display format, please use this tool on the computer only.

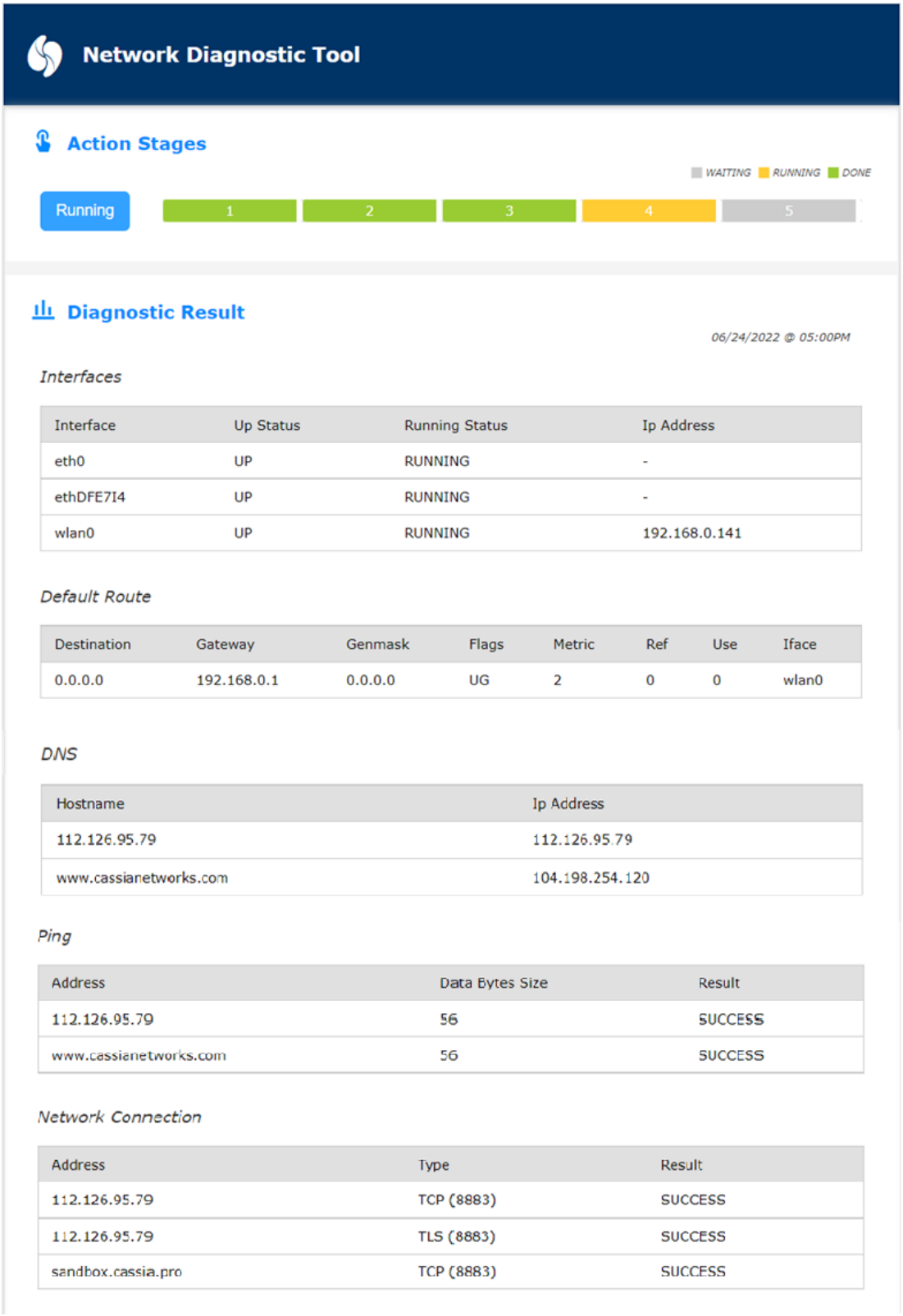


From firmware 2.1.1, the user can run the Network Diagnostic tool on the gateway’s local console. Network Diagnostic tool can help you to assess the gateway’s network status during the deploying and troubleshooting phase.



If you have run network diagnostic on this gateway before, you will see the diagnostic result of last time. Please click the Start button to start new network diagnostics.

Below is an example of network diagnostics. In this example, the “AC Server Address” is 112.126.95.79 and the gateway uses Wi-Fi as uplink. According to the diagnostic result, the Wi-Fi interface is up and has got the IP, the DNS works well, ping to AC success, and the TCP and TLS connection to the AC also works fine. The www.cassianetwork.com and sandbox.cassia.pro is used as a reference for the diagnostics.



Network Diagnostic Tool

Action Stages

WAITING RUNNING DONE

Running | 1 | 2 | 3 | 4 | 5

Diagnostic Result

06/24/2022 @ 05:00PM

Interfaces

Interface	Up Status	Running Status	Ip Address
eth0	UP	RUNNING	-
ethDFE7I4	UP	RUNNING	-
wlan0	UP	RUNNING	192.168.0.141

Default Route

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.0.1	0.0.0.0	UG	2	0	0	wlan0

DNS

Hostname	Ip Address
112.126.95.79	112.126.95.79
www.cassianetworks.com	104.198.254.120

Ping

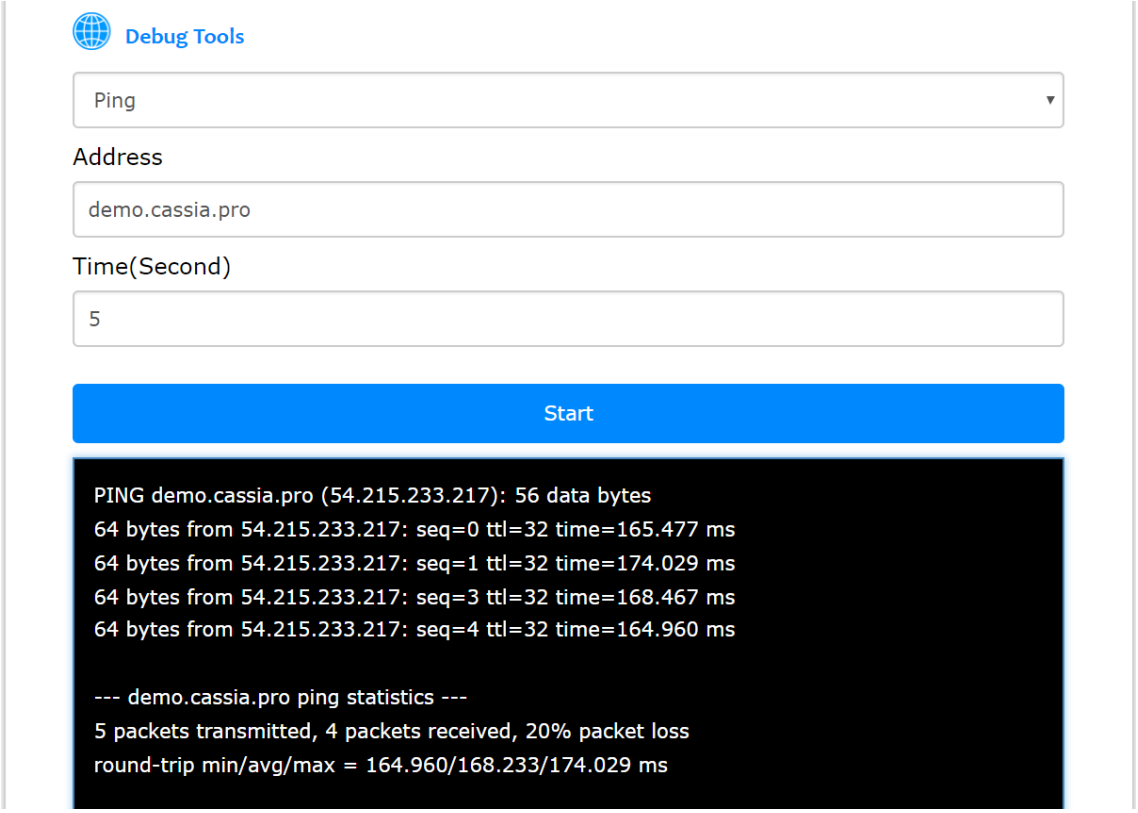
Address	Data Bytes Size	Result
112.126.95.79	56	SUCCESS
www.cassianetworks.com	56	SUCCESS

Network Connection

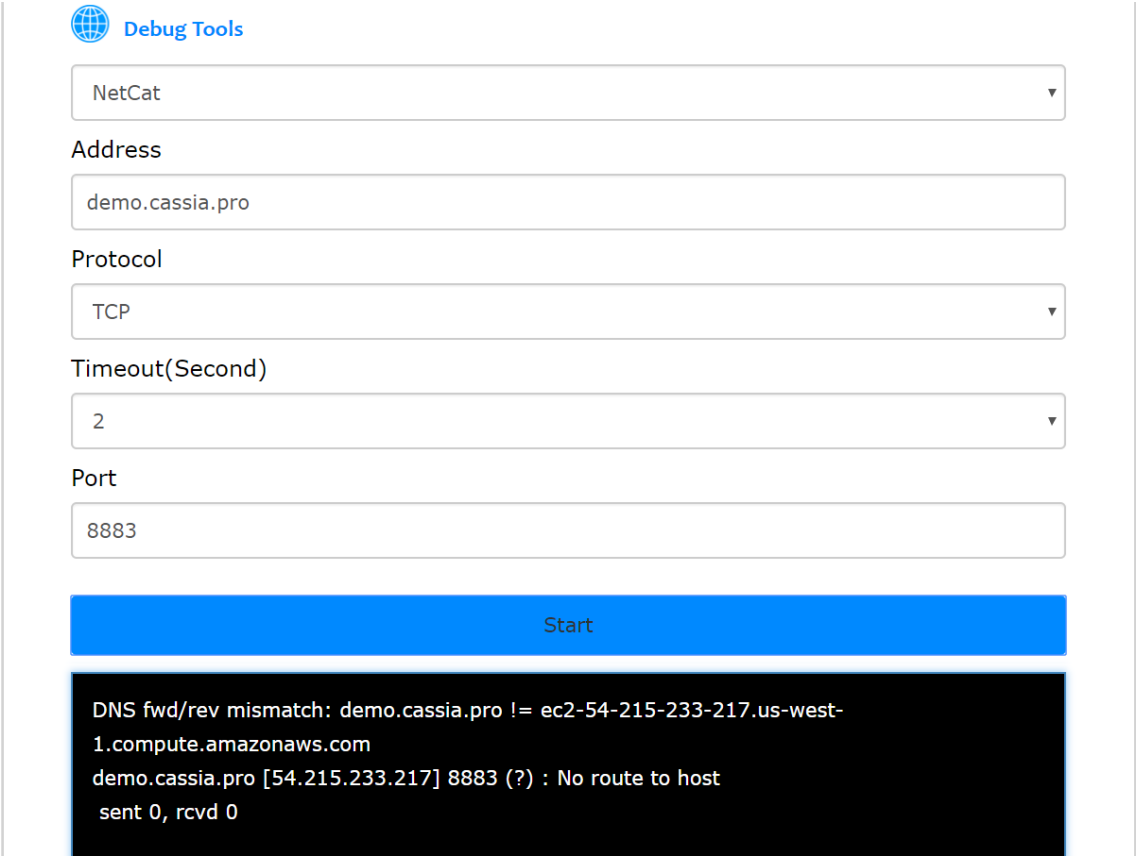
Address	Type	Result
112.126.95.79	TCP (8883)	SUCCESS
112.126.95.79	TLS (8883)	SUCCESS
sandbox.cassia.pro	TCP (8883)	SUCCESS

Below are examples for Ping, NetCat, and SpeedTest.

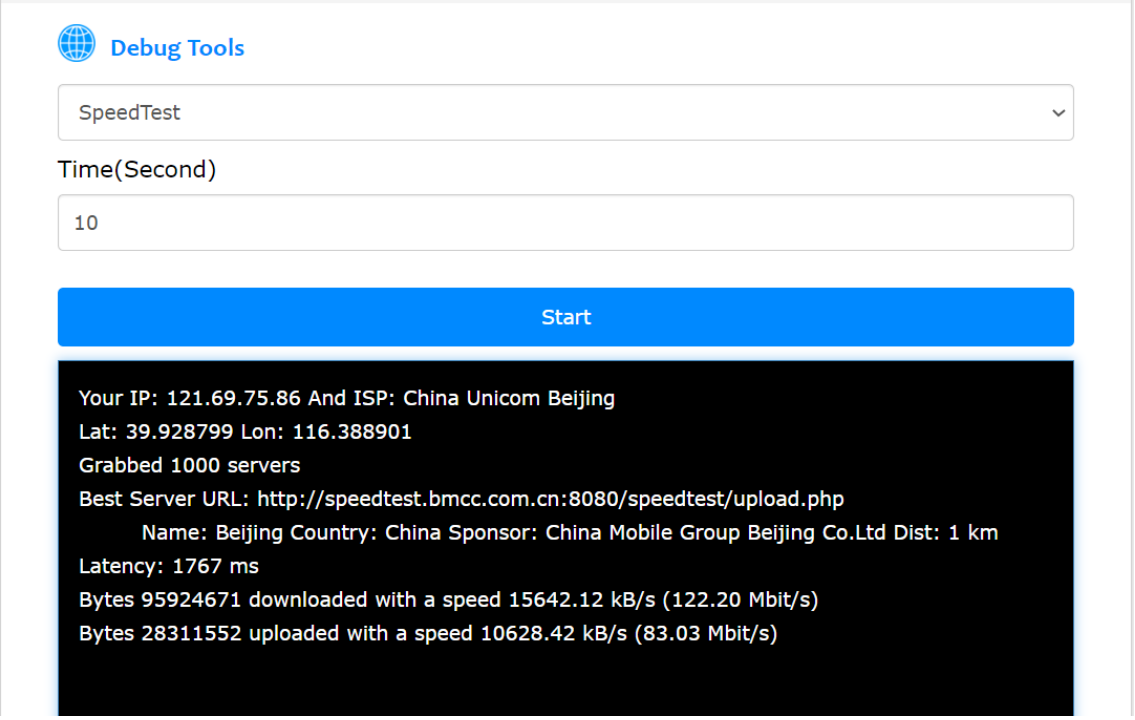
Example 1: Check if the AC is reachable.



Example 2: Check if the MQTT TCP port 8883 is opened.



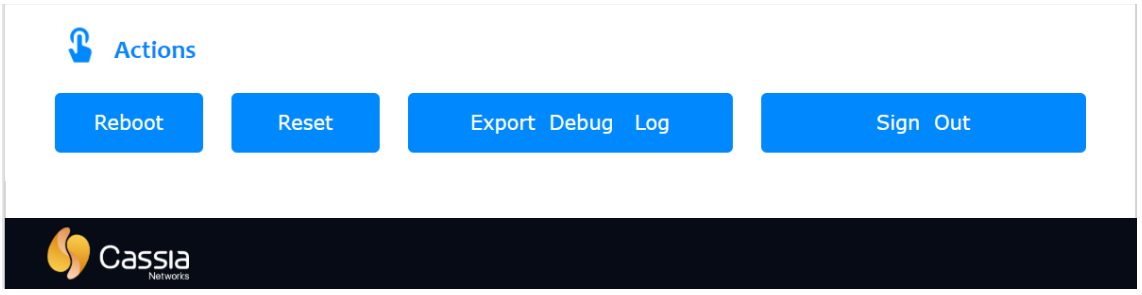
Example 3: Check the download and upload speed of the uplink connection (Ethernet, Wi-Fi, or cellular).



The user can click the Reboot button to perform a restart of the gateway. The user can also click the Reset button to reset the gateway's configuration to the default profile settings and enable a Wi-Fi hotspot (2.4GHz only). The country code, container, and customer APP will not be impacted. Please check chapter 4.5 for more information.

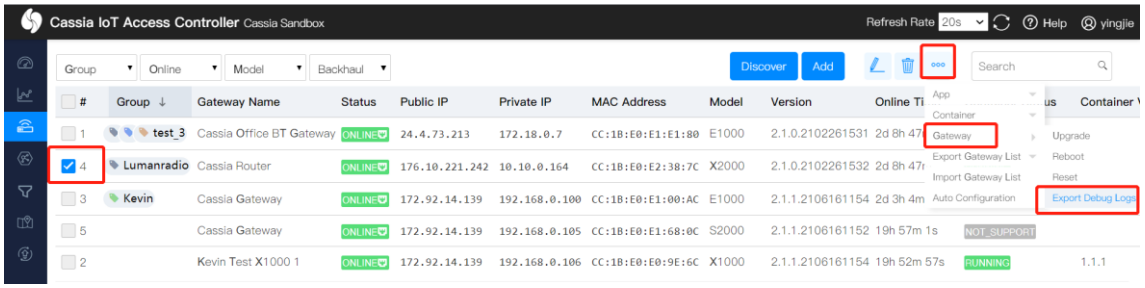
When the user clicks the Export Debug Log button, the gateway's debug log can be downloaded for troubleshooting. This log is not readable to end-users. Please email it to Cassia Support support@cassianetworks.com for further analysis.

To minimize cybersecurity risks, please remember to click the Sign Out button after the gateway configuration.



Cassia gateway configuration page – other continued

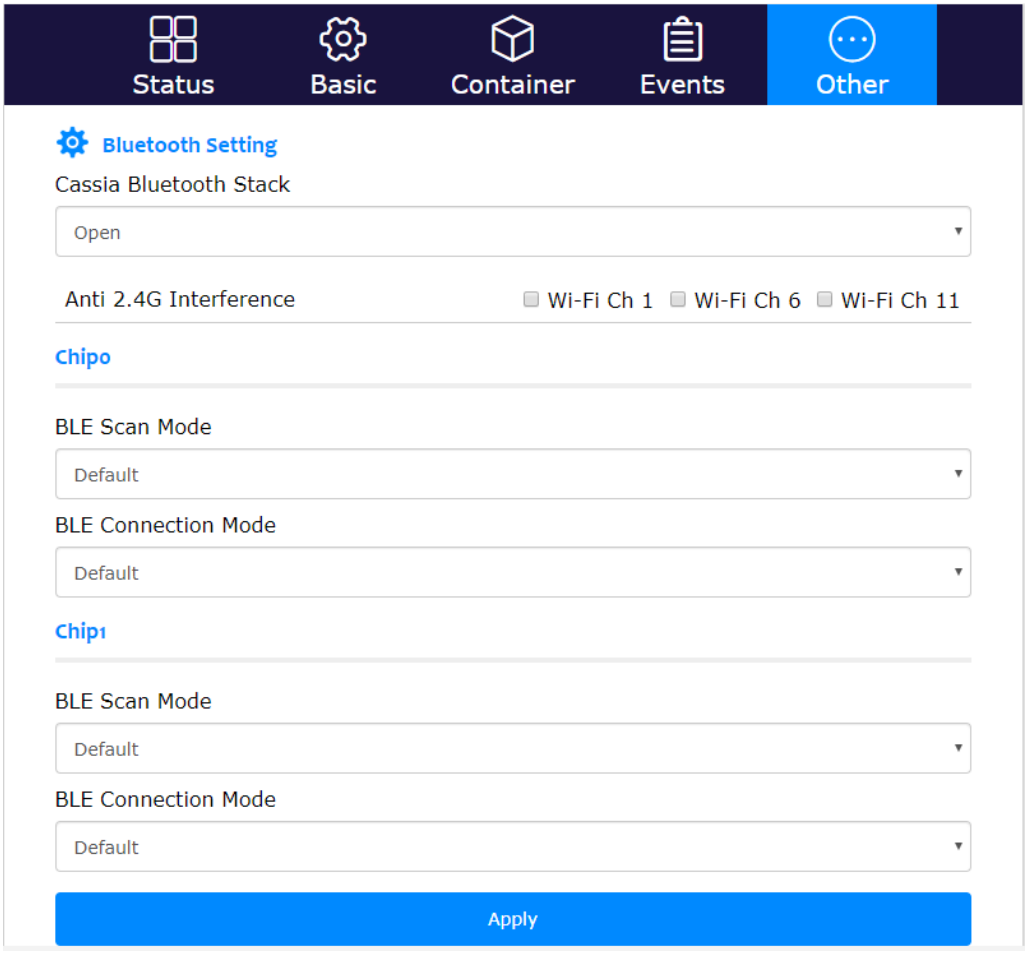
From firmware 2.0.3, the user can download the gateway debug log from AC too (see below screenshot). Only one gateway's debug log can be downloaded from AC at the same time. It may take 2-5 minutes (time out in 10 min) to download one gateway debug log. Please don't touch the AC console and wait until the download is finished, otherwise, the download may be interrupted.



If the gateway is configured as standalone mode (in the Basic tab), the user can configure below Bluetooth parameters on the gateway's local console. If the gateway is configured as AC managed mode, the user can only set these parameters on the AC server console.

One Bluetooth chip can support scan and connection at the same time. If Default is selected, the gateway will use a set of pre-defined parameters. If Custom is selected, the user can define the Cassia gateway's Bluetooth Low Energy parameters, e.g. connection interval. The table below shows the default, maximum and minimum values of each parameter.

Parameter	Default (ms)	Min (ms)	Max (ms)
Scan Interval	15	2.5	10240
Scan Window	10	2.5	10240
LE Page Scan Interval	60	2.5	10240
LE Page Scan Window	30	2.5	10240
Connection Min Interval	7.5	7.5	4000
Connection Max Interval	30	7.5	4000
Latency	0	0	499
Supervisor Timeout	1000	100	32000



Cassia gateway configuration page – Other continued

Cassia Bluetooth gateway E1000, S2000, and X2000 offers a more flexible Bluetooth configuration and two state-of-the-art Bluetooth modes: pure scan and high speed multiple connection modes. The two Bluetooth chips can run in a different mode with a different configuration, for example, one chip uses pure scan mode, and the other chip uses high speed multiple connection mode. Before changing BLE connection mode, please disconnect all the Bluetooth Low Energy devices.

- Cassia Bluetooth Stack: default is open.

  After upgrading gateway firmware to 2.0, if the APP uses BlueZ with Gatttool and Bluetoothd in the container (e.g. noble or python Bluetooth lib) instead of Cassia RESTful API, **please change 'Cassia Bluetooth Stack' to close** (in AC console -> Gateway -> Config-> Bluetooth Setting, or gateway console -> Other -> Bluetooth Setting). Otherwise, Bluetooth operations in the APP may return failure.

  Cassia Bluetooth stack and Cassia RESTful API offer the state of the art Bluetooth scan and connection performance. It is highly recommended to keep the Cassia Bluetooth stack open and use Cassia RESTful API to achieve the best performance Bluetooth IoT system.

- Scan Mode: set the Bluetooth Low Energy scan parameters to default, continues scanning, pure scan, or customized mode.

  Continues scanning mode has better scan performance, and the Bluetooth Low Energy connection capability is still kept.

  Pure scan mode offers the best scan performance in high noise floor and massive Bluetooth Low Energy device scenarios. It is not allowed to make connections in pure scan mode. If pure scan mode is enabled, it is not possible to configure the Connection Mode.

  Pure scan supports filtering the scan data by RSSI, raw data, and MAC address. The RSSI filter can filter out the Bluetooth Low Energy devices whose RSSI value is weaker than this value. The raw data filter can filter the scan packets with data xx (2-12 hex numbers) from offset yy (0-31). The MAC filter can filter the packets with MAC xx (2-12 hex numbers) from offset yy (0-5). If Pure Scan is enabled, only one MAC filter is allowed on one Bluetooth Low Energy chip. If customer wants to filter MAC address with two very different patterns, they can use chip 0 to scan one MAC filter and use chip 1 to scan the other MAC filter, or try to use continues scanning mode (lower scan performance) with one Bluetooth Low Energy chip and add parameter "filter_mac" to filter multiple different MAC.

  Scan mode is not valid when Cassia Bluetooth Stack is closed.

  From firmware 2.1.1, scan API can scan the Bluetooth Low Energy devices with two chips and merge the scan result together. This new function can be enabled by adding parameter "chip=all" in scan API.

  NOTE: For S2000, if the received advertising packets are more than 200 per second, it is recommended to use scan filters to reduce the S2000's CPU load.

- Connection Mode: set the Bluetooth Low Energy connection parameters to default, high speed multiple connections, or customized mode.

  High speed multiple connection mode optimized the connection performance when receiving data from multiple Bluetooth Low Energy devices simultaneously. If high

speed multiple connection mode is enabled, it is not possible to configure the Scan Mode.

From firmware 2.1.1, BLE4.2 data length extension (DLE) will be enabled on gateway E1000, S2000 and X2000 by default. In Bluetooth Low Energy 4.0/4.1, the link layer data channel pay load size is up to 27 Bytes. In Bluetooth Low Energy 4.2/5.0 with DLE enabled, link layer data channel pay load size is up to 251 bytes. It is more efficient to transfer data with bigger packet. The benefits include 2~3 times faster device firmware upload and sensor big data download, and battery saving due to more efficient transmission.

Connection mode is still valid when Cassia Bluetooth Stack is closed.

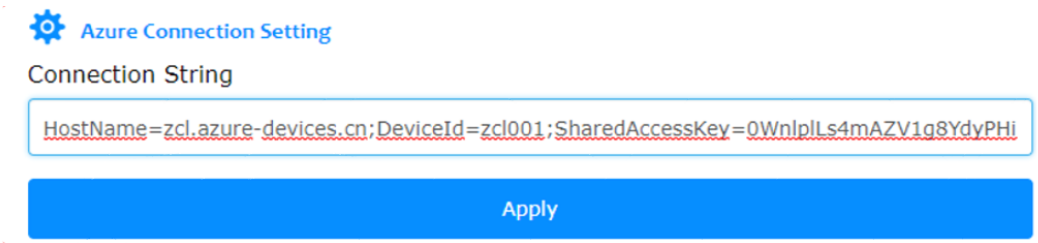
From firmware 2.0.3, the user can enable the “avoid 2.4G interference” feature to minimize the 2.4Ghz interference between Wi-Fi and Bluetooth Low Energy. To avoid 2.4Ghz interference, we recommend installing Cassia Bluetooth gateway at least 3 feet (1 meter) away from Wi-Fi access points. But in some cases, there still may be 2.4Ghz interference even Cassia Bluetooth gateway and Wi-Fi access points are installed 3-6 meters away from each other. For example, if there is continuous Wi-Fi download on one specific Wi-Fi 2.4Ghz channel, Wi-Fi may cause strong interference to Bluetooth Low Energy. In this case, the user can set the Wi-Fi channels which have the most interference (channel 1, 6, or 11) in Bluetooth Setting. Then, Cassia Bluetooth gateway will avoid using these frequencies. Please check your Wi-Fi channel configuration on the Wi-Fi access point or contact your IT team.

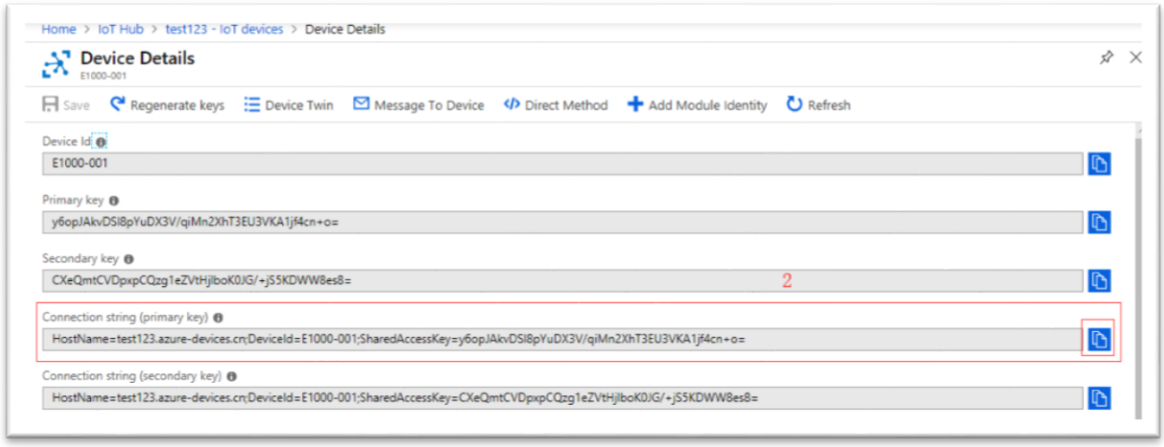
From firmware 1.4 and above, Cassia supports Azure IoT SDK on X1000 and E1000. The Cassia gateway must be operated in standalone mode and connected to Azure IoT Hub by MQTT protocol.

Azure IoT SDK support is a Beta version in firmware 1.4. Please contact support@cassianetwork.com for Azure beta program details.

The user can control the Cassia gateway by calling the “Direct Method” or “Message to Device” interface. The JSON format is based on local RESTful API. The feedback and data from Cassia gateway are reported to Azure IoT Hub in JSON format. Also, the user can POST JSON string from Cassia gateway container to Azure IoT Hub.

First, please set the gateway to standalone gateway, copy Connection String from Azure IoT Hub, and paste it in the Cassia gateway (see below figures). These are the only configurations needed on the Cassia gateway.



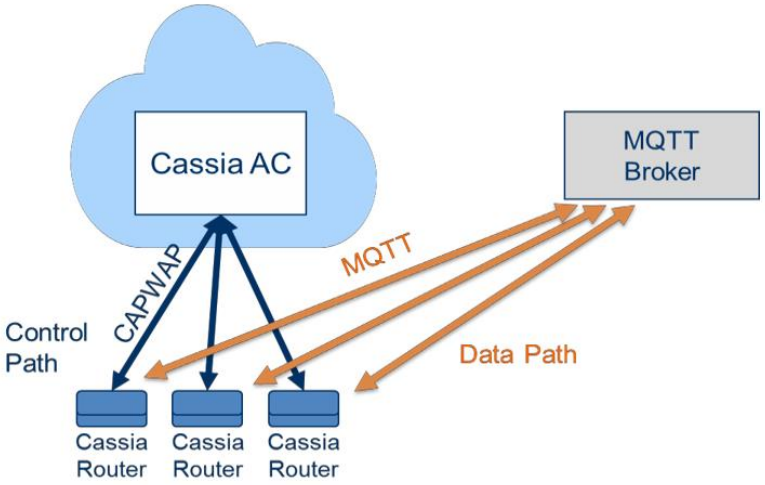


5.6. Service Tab

The Cassia gateway can send scanned data directly from the gateway to a third-party server while keeping the control path to the AC. We call this function “bypass” mode.

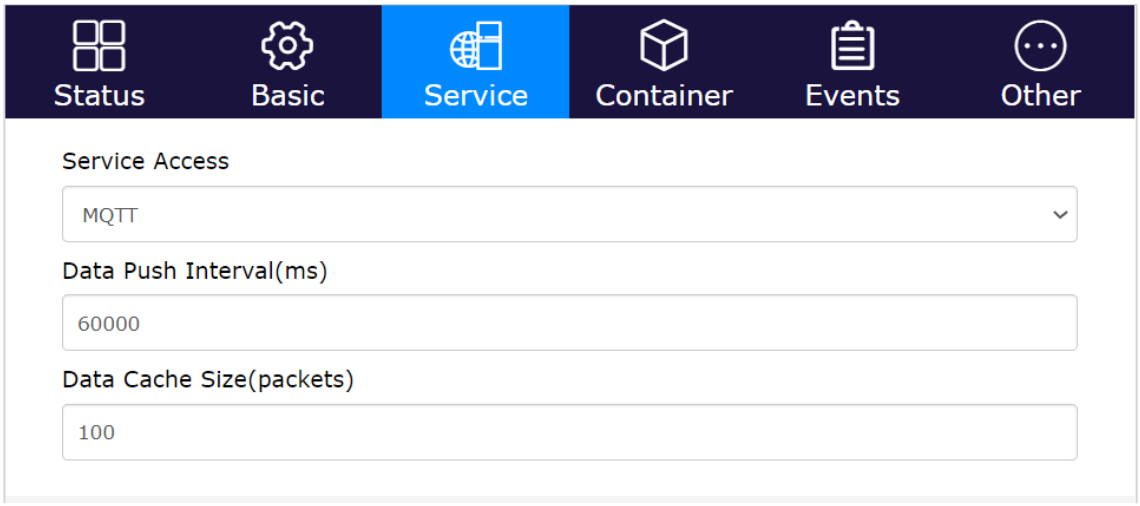
MQTT (MQ Telemetry Transport) is described on the mqtt.org site as a machine-to-machine (M2M) / IoT connectivity protocol. It is a publish/subscribe messaging transport protocol, designed for constrained devices and low-bandwidth, high-latency, or unreliable networks.

Since release 1.2, Cassia gateway supports MQTT protocol on the bypass traffic which means that the Cassia gateway can publish advertisement messages it receives from the Bluetooth Low Energy sensors to an MQTT server/broker. Other clients, such as web applications on your laptop and smartphone device can subscribe to the topics from the MQTT-Broker.



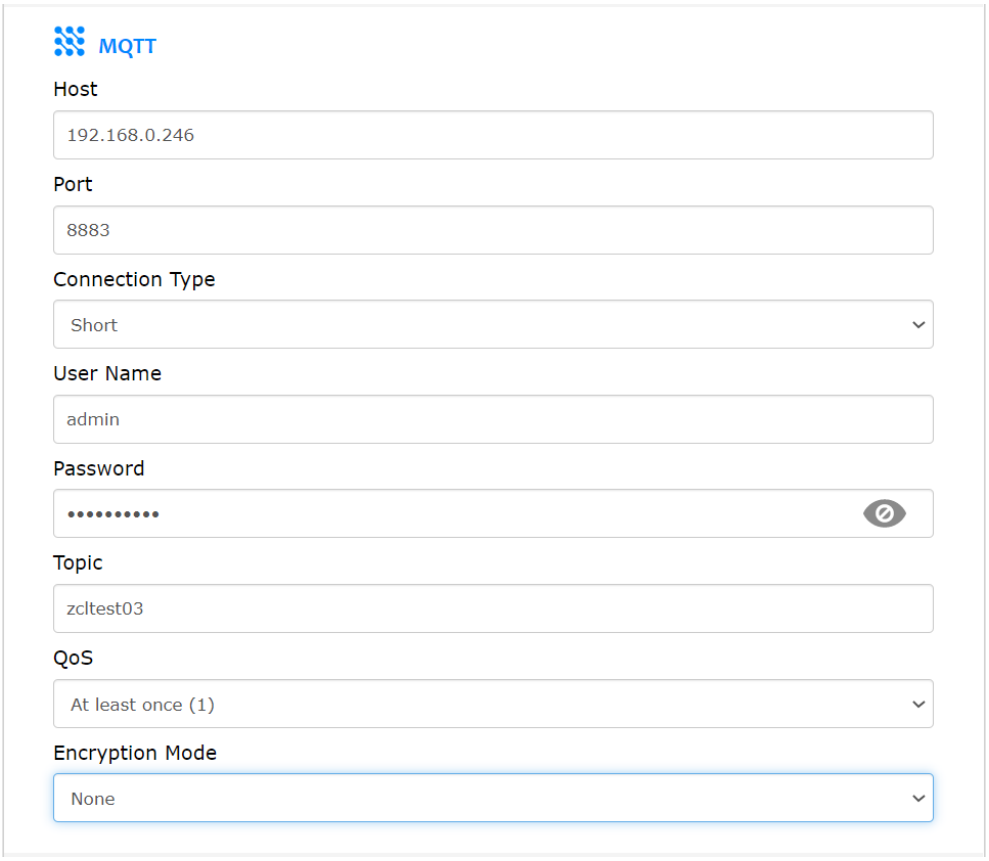
Cassia MQTT Bypass Architecture

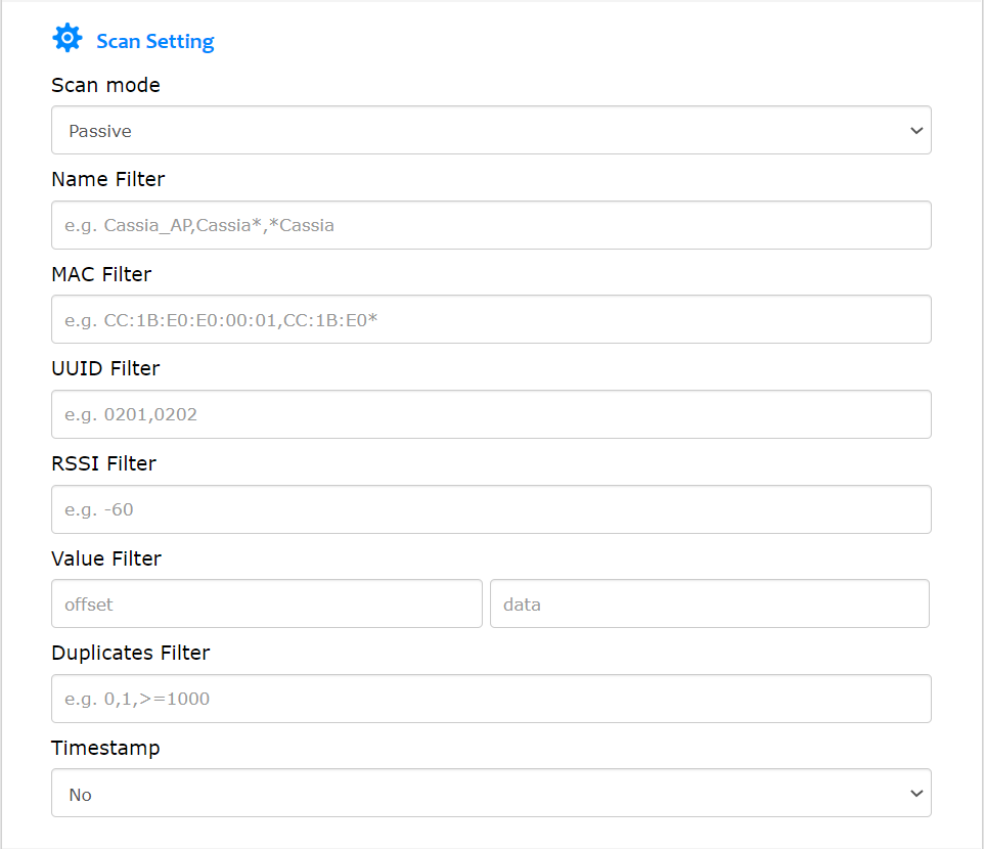
When the gateway is running in AC Managed mode (configured by Gateway Mode in Basic tab), the user can only configure the gateway’s MQTT in the AC console (see the configuration in AC->Gateway->Config->Bypass). When the gateway is running in Standalone mode, the user can configure the MQTT function in the gateway console Service tab. The user can set up data push and data cache configuration, MQTT configurations, and scan settings.



Cassia gateway configuration page – Service

To reduce MQTT packets and MQTT overheads, the gateway can cache a maximum of 100 advertisement packets or a maximum of 60 seconds, and send them to the MQTT broker together.





Cassia gateway configuration page – Service continued

Parameter	Description
Scan Mode	Passive or active scan • The difference between active and passive scan is that active scan requests a SCAN_RESPONSE packet from the advertiser. • A passive scan generally takes more time since the gateway must listen and wait for an advertisement versus actively probing to find an advertiser. However, with the passive scan, devices consume less battery power.
Filter	Scan filters for advertisement packets • Name: supports full name, prefix (for example Cassia*) and suffix (for example *Cassia) name filters • MAC: supports full MAC and prefix MAC filters (for example CC:DD:EE*) • UUID: filter based on UUID in the advertisement packets. • RSSI: filter out devices whose RSSI value is weaker than this value. • Value: filter advertisement packets with data xx from offset yy. If offset is not set, the gateway will filter data xx with any offset. • Duplicates filter: for a value equal to or larger than 1000 (ms), if the received advertisement packets are the same, the gateway will only send one advertisement packet to the MQTT broker before the timer times out. If the gateway receives a different advertisement packet, it will send the new advertisement packet to the MQTT broker immediately. Value 1 means only send one packet for one device, which is usually used to detect how many Bluetooth low energy devices are around the Bluetooth gateway. Default is 0 (no timer). The keywords used for filtering need to be in the advertisement packets. The UUID in advertisement packets may be only part of the UUID in Bluetooth low energy profile.
Time Stamp	Add timestamp in the bypass MQTT packets. Default is no

For detailed configuration on MQTT, please check MQTT Configuration Guide: https://www.cassianetworks.com/support/knowledge-base/general-documents/

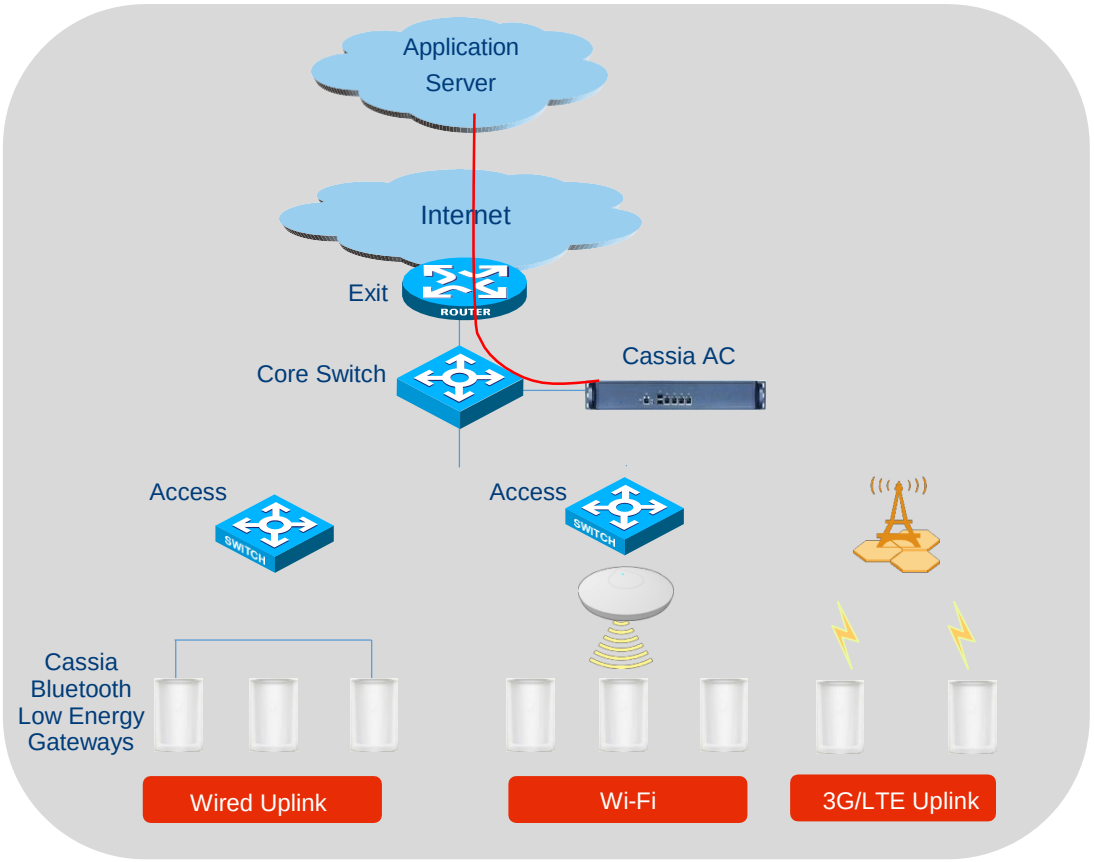
6. More information on Access Controller

6.1. Deployment Options

The Cassia AC can be deployed on an on-premise server, in a private cloud, or Cassia's public cloud. Administrators can access the Cassia AC from a web-browser, through a PC, or a tablet without any special training.

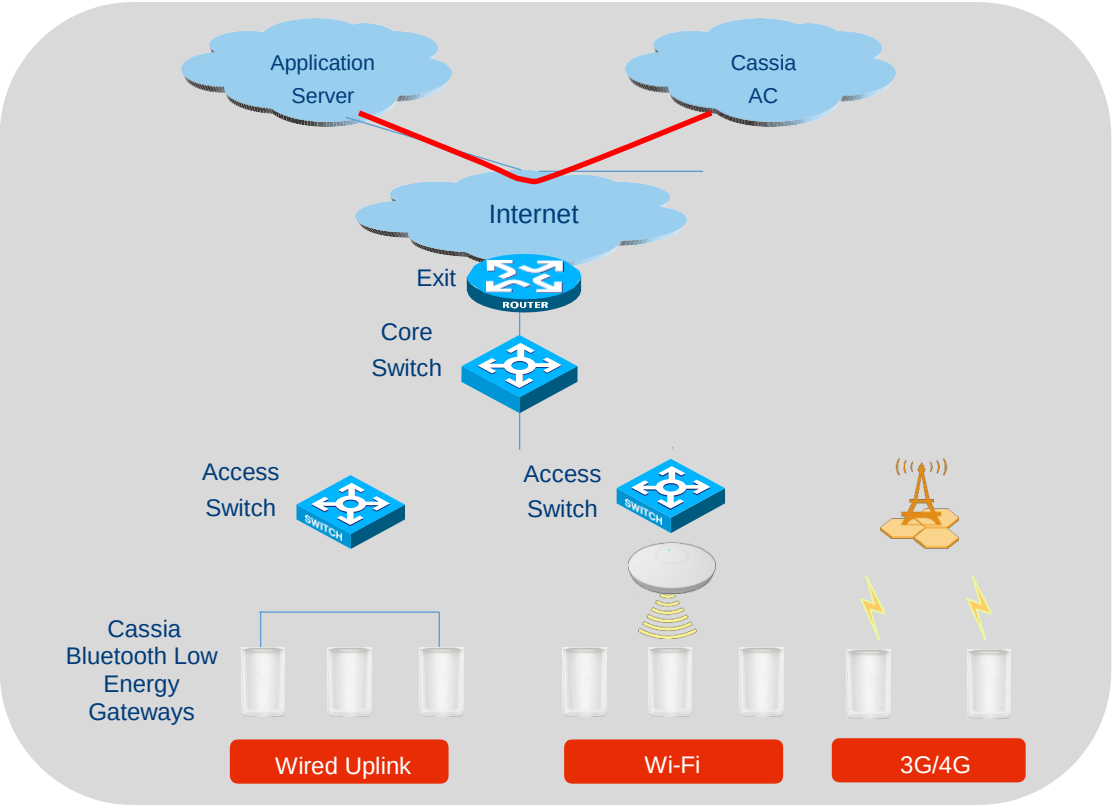
Before upgrading AC software, please make sure the host server has a minimum of 2GB free storage.

- On-premise or private cloud
  - Cassia's AC on-premise server or user-provided server
  - Deployed next to the core network switch



Cassia AC deployment – on-premise or private cloud

- Self-managed or Cassia-managed public cloud
  - Deployed on public clouds like Azure, AWS, Google Cloud, or AliCloud
  - Setup and maintenance are required



Cassia AC deployment – public cloud

Cassia's Bluetooth gateway will auto-discover AC by:

- Specifying the AC's IP address/domain name in the gateway's settings
- Cassia's distribution system (gateways need to have Internet access)
- Broadcasting on the same subnet (gateways and the AC need to be in the same subnet)
- DHCP option43 or DNS setting

6.2. AC Statistics

AC statistics page shows the statistical data of the AC throughput, memory/CPU, gateways, devices, AC API calls, and traffic amount per day, per week, or month.

- Throughput: the aggregated AC throughput of Ethernet and Bluetooth, both uplink and downlink
- Memory/CPU: RAM consumed and CPU consumed over time
- Gateways: number of online and offline gateways
- Clients/Devices: number of connected and detected devices
- API Calls: the number of success and failed AC API calls of all the gateways managed under this AC. The success API calls are shown in the green column. The failed API calls are shown in the red column. Only the AC API calls will be recorded. The local API calls

and the API called in the container will not be recorded.

- Traffic amount: the aggregated advertising packets, the successful connection requests, and the notification packets of all the gateways managed under this AC.

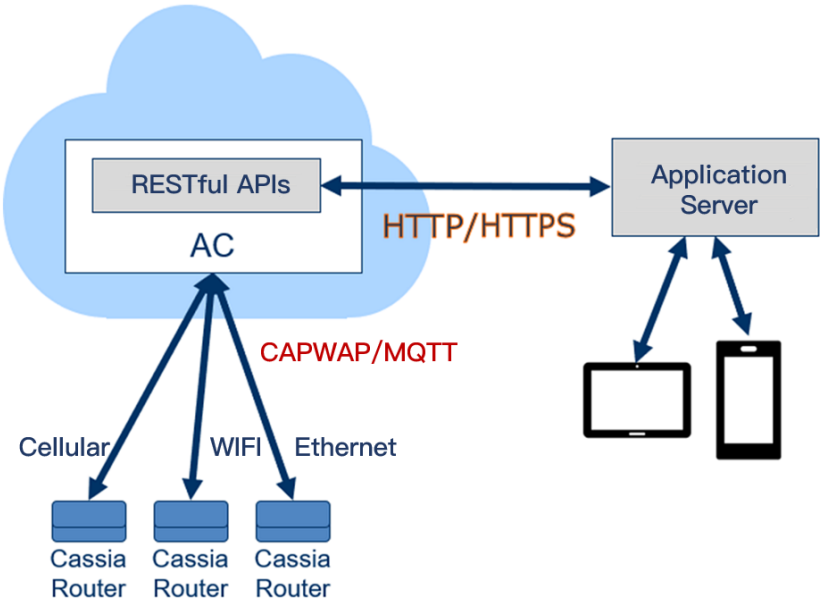
6.3. Interface & Protocol

Please see the figure below for the interfaces compatible with the Cassia AC server

- Before firmware 2.0.2, the communication between the Cassia Bluetooth gateways and the AC is over CAPWAP. It is a UDP-based protocol and uses UDP ports 5246 and 5247. It uses DTLS 1.2 to ensure security.

  From firmware 2.0, the user can select MQTT to replace CAPWAP. MQTT uses TCP port 8883 and TLS 1.2. MQTT improves the robustness of gateway and AC communication and can help the IP packets to pass through the user's firewall, in case the firewall doesn't allow UDP packets to pass. One AC can support MQTT and CAPWAP at the same time. Please check chapter 4.4 for more information.

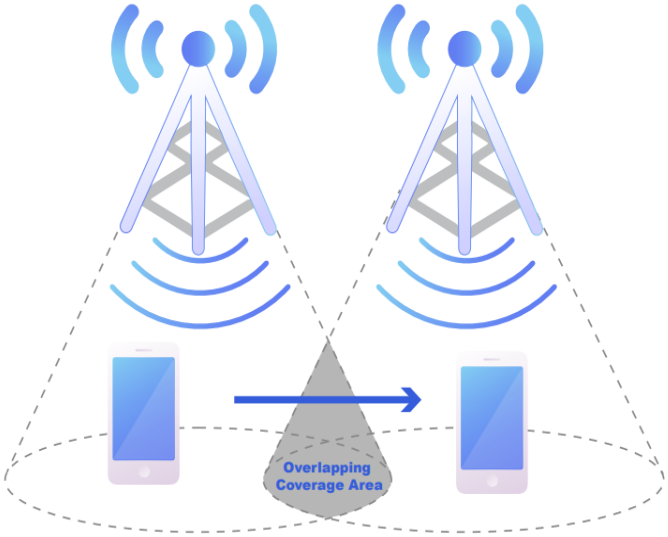
- The interface between the AC and the application server is using RESTful APIs, on HTTP (port 80) or HTTPS (port 443). We strongly suggest you to use HTTPS. For details on Cassia's RESTful APIs please see the next section.



Compatible Interfaces with Cassia AC

6.4. Bluetooth Roaming

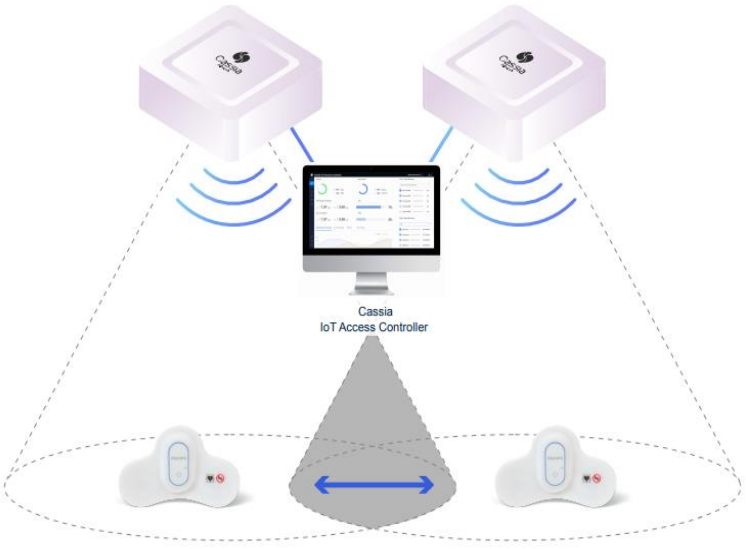
For cellular and Wi-Fi, roaming occurs when a mobile device switches its association to the wireless base station with a stronger RF signal when moving from the coverage area of one base station to the next. A successful roaming is one that doesn't interrupt the user data communication during the roaming handoff.



What is Bluetooth Roaming? Bluetooth roaming occurs when a Bluetooth device switches its association to the Bluetooth gateway with a stronger RF signal when moving from the coverage area of one Bluetooth gateway to the next.

Cassia invented fast and secure Bluetooth roaming technology to solve this problem without requiring any changes to the Bluetooth protocol and/or end devices.

- Ensures continuous user data connection during roaming handoff
- Ensures seamless and fast Bluetooth roaming without any human intervention
- No changes are required to the Bluetooth protocol and/or end devices
- Highly secure at all times
- Bluetooth roaming can be applied for any mobile Bluetooth IoT applications



Unlike Cellular and Wi-Fi, Bluetooth protocol has no inherent roaming support, and Bluetooth end devices can’t initiate a roaming handoff. As a result, Bluetooth roaming has

to be initiated and coordinated by Cassia's IoT AC and Cassia's Bluetooth gateways.

- All Bluetooth gateways under the Cassia IoT Access Controller (AC) function as a single gateway from the mobile device perspective
- No security renegotiation (e.g. re-pairing etc.) is needed, and the user data connection remains continuous during roaming handoff
- This ensures seamless, fast, and secure Bluetooth roaming without human intervention and without requiring any changes to the Bluetooth protocol and/or end devices

To enable Bluetooth roaming, the AC software should be version v2.1.0 or higher, Cassia Bluetooth gateway should be E1000, S2000 or X2000 with firmware v2.1.0 or higher, and AC and the gateways must be on the same local network (if AC is on the cloud, need further verification). Please use Gateway Auto-Selection API, and set parameter random=1. No configuration on the AC or gateway console is needed.

Sample: **https://github.com/CassiaNetworks/CassiaSDKGuide/blob/master/node_examples/roaming.js**

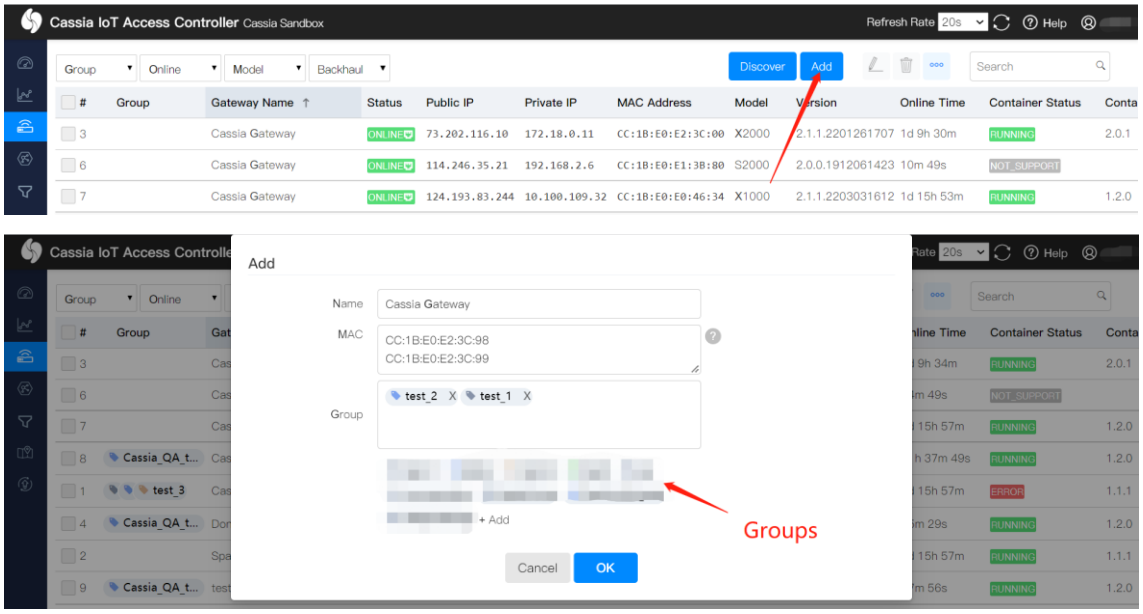
github.com/CassiaNetworks/CassiaSDKGuide/blob/master/node_examples/roaming.js

```
127  function connectWithAutoSelection(token, devices) {
128    return req({
129      url: `${AC_HOST}/aps/connections/connect?access_token=${token}`,
130      method: 'POST',
131      headers: {'Content-Type': 'application/json'},
132      body: JSON.stringify({
133        /*
134        * you can define a Router range to connect to devices, or '*' means all online Routers
135        */
136        aps: '*',
137        devices: devices,
138        /*
139        * (Mandatory) use the roaming feature, Router use random address to connect devices,
140          AC will reconnect devices among Routers,
141        * you can listen to connection-state changes in combination SSE
142        */
143        random: 1,
144        /*
145        * (Optional): in ms, the connection request will timeout if it can't be finished within this time.
146        * The default timeout is 10,000ms. The range of value is 1000ms - 20000ms.
147        */
148        timeout: 20000
149      })
150    });
151  }
```

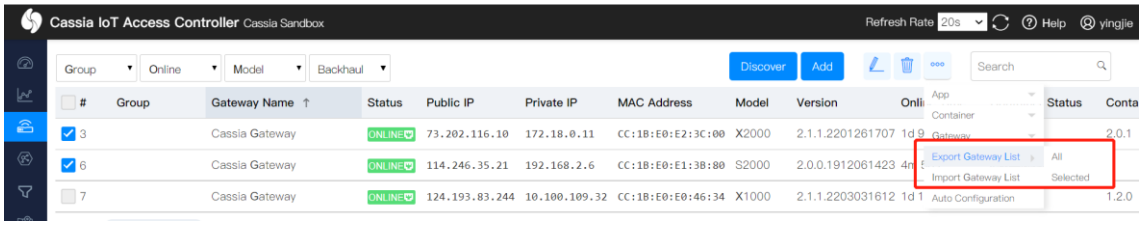
6.5. Add Gateways in AC

NOTE: Please always use AC version equal or newer than gateway versions, otherwise you may meet strange behaviors. For example, the gateway with 2.1.1 firmware can only connect with 2.1.0 AC with CAPWAP protocol, due to single port feature introduced in 2.1.1.

Before sending the gateways to customers, please add the gateways in AC following below steps. You can also set name and group for these gateways. After that, when the gateways are powered up and correctly configured, they will connect to the AC automatically.



You can also export all the gateways or the selected gateways to a file and import it to another AC later.

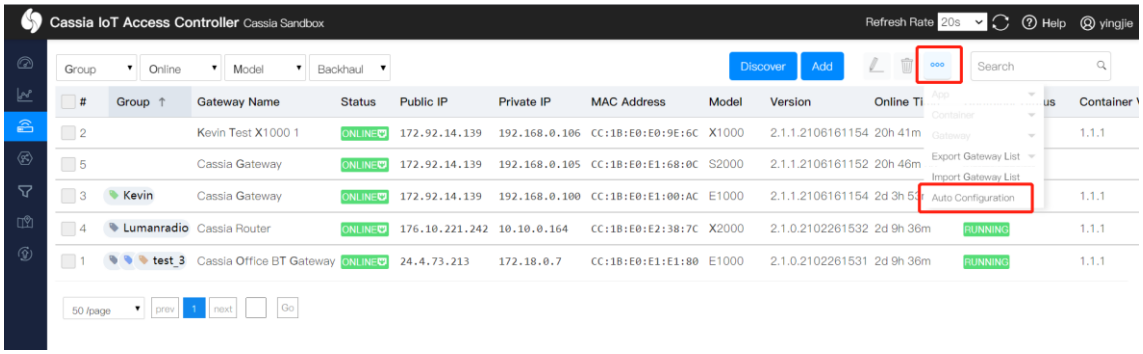


6.6. Gateways Auto Configuration

This is an ease of deployment feature introduced in firmware 2.1.1. This feature greatly simplifies and speed up the gateway deployment and the pre-configuration before shipping gateways to the end users.

By using this feature, when a gateway connects to the AC for the first time or each time (configurable), AC will send the new configuration to the gateway automatically. The user doesn't need to login to each gateway's local console and set configuration one by one.

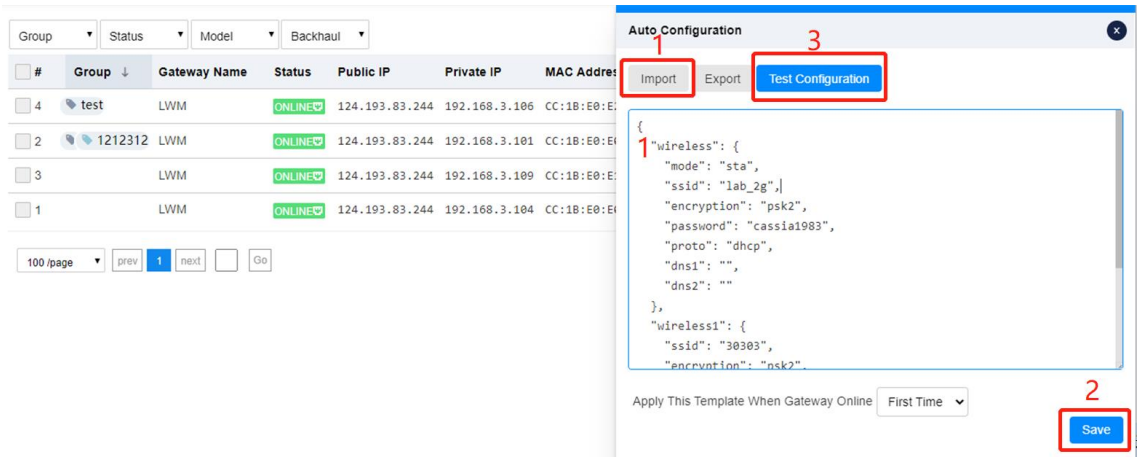
What is more, for the users who use AC and gateway in intranet, e.g. hospital and school, they don't even need to set AC address in gateway's local console. When AC address is empty, the gateway will search and connect to AC in the LAN automatically. In this case, the gateways can be configured automatically by AC without touching the gateway's local console.



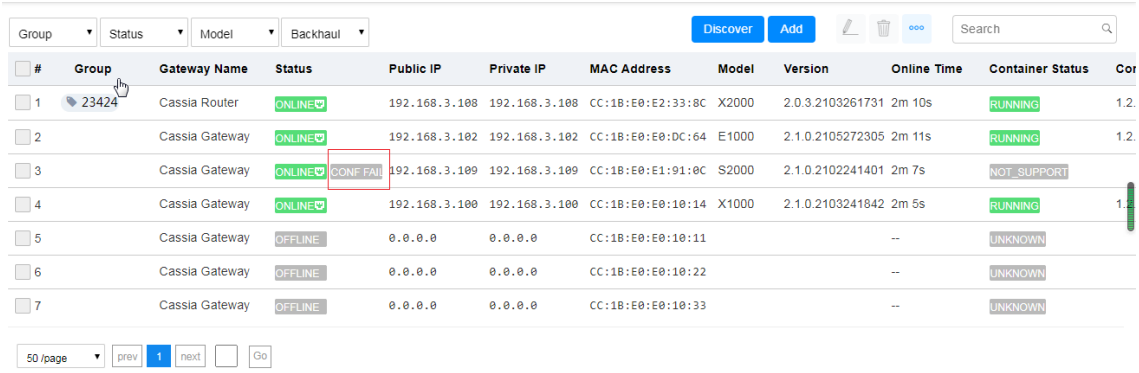
First, please input or import the gateway configuration into AC, select when the configuration should be sent (first time online or each time online), and then save the configuration. The current configuration can be exported into a file.

The format of the configuration complies with JSON format of Cassia RESTful API “Obtain Cassia Router’s Configuration”. Please check below link for more information about this API (https://github.com/CassiaNetworks/CassiaSDKGuide/wiki/RESTful-API#obtain-cassia-routers-configuration).

After the configuration is saved, it is suggested to check if the configuration is correct (avoid typo). Please press button “Test Configuration” and select one on-line gateway.



After that, when the new gateway is online, AC will send the configuration to the new gateways automatically. You can check the configuration result in the event log. If the configuration failed, you can find “CONF FAIL” on gateway console too.



Only the admin AC account can enable this feature. The read only AC account can’t enable this feature.

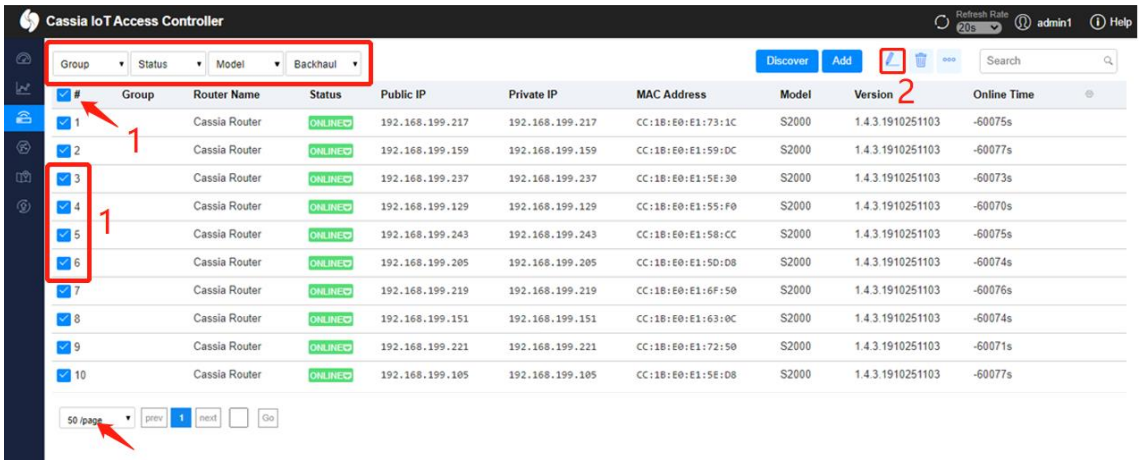
6.7. Gateway Batch Configuration

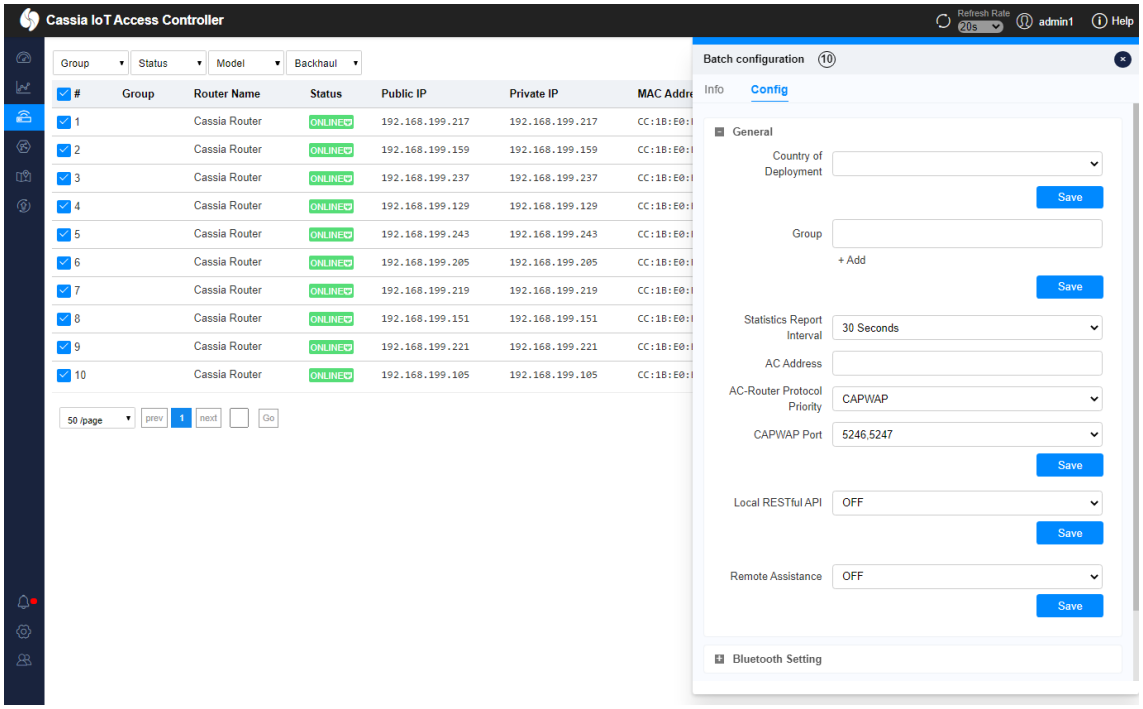
The user can select multiple gateways that belong to the same type (e.g. E1000) and configure them in batch. Batch configuration can speed up the configuration and avoid the error of human operation.

First, please select all the gateways that need to be configured in batches, or select the gateways one by one. After that, please click the edit button in the upper right corner. Then, the batch configuration page will show up.

Only the same type (S2000, E1000, X1000, or X2000) of gateways can be configured in batches.

TIPS: You can select a specific type of gateway through the filter on the top left. If you want to configure more gateways at once, please select showing 100 gateways per page in the lower-left corner.



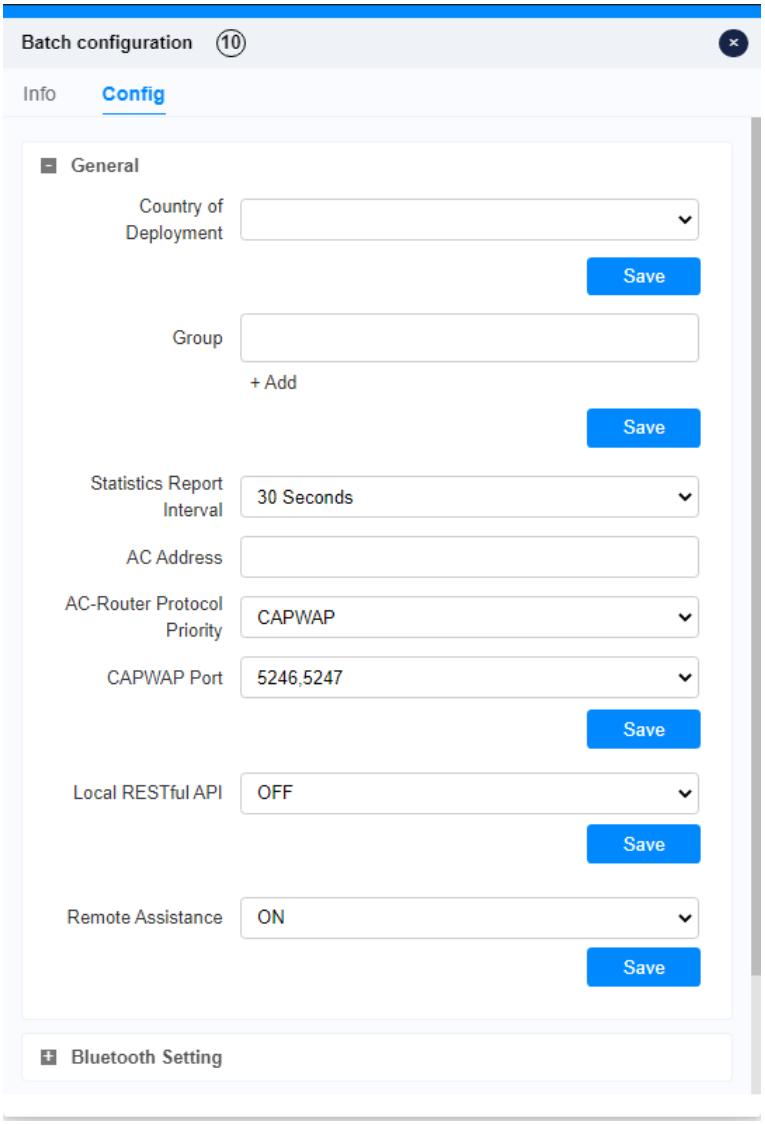


The parameters on the batch configuration page are the default parameters, instead of the actual parameters in the Bluetooth gateways. Please only modify the parameters you need to configure in batches. Please ignore the other parameters.

The following general parameters can be configured in batches

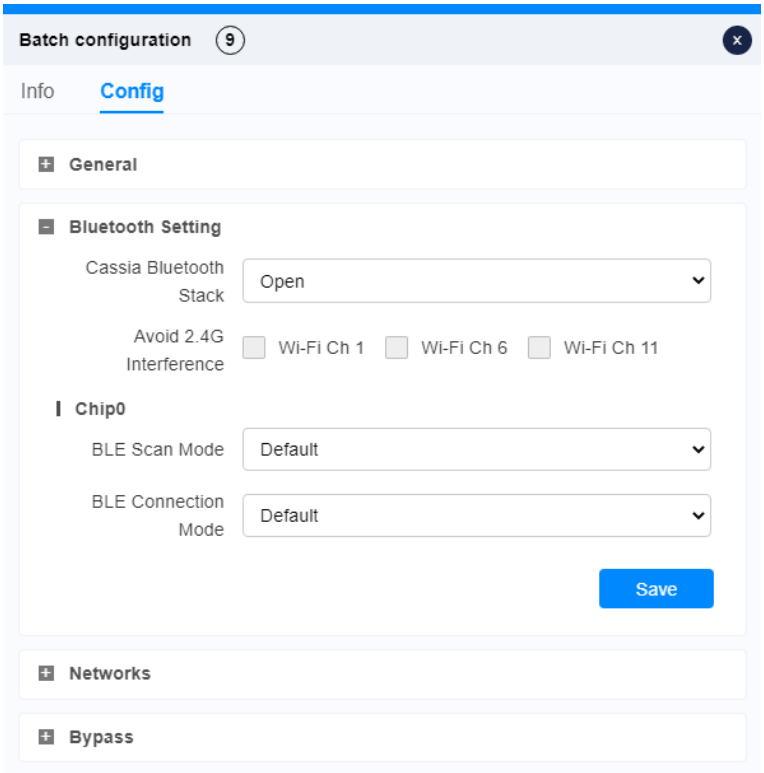
- Country of deployment
- Group: The user can tag one gateway with a maximum of three groups. The group can be used to search, filter and sort gateways or send email alert to the users

- Statistical report interval
- AC address
- The priority of communication protocol between AC and gateway: AC address must be filled in before modifying this configuration
- CAPWAP port
- Local RESTful API
- Remote assistance



The following Bluetooth parameters can be configured in batches

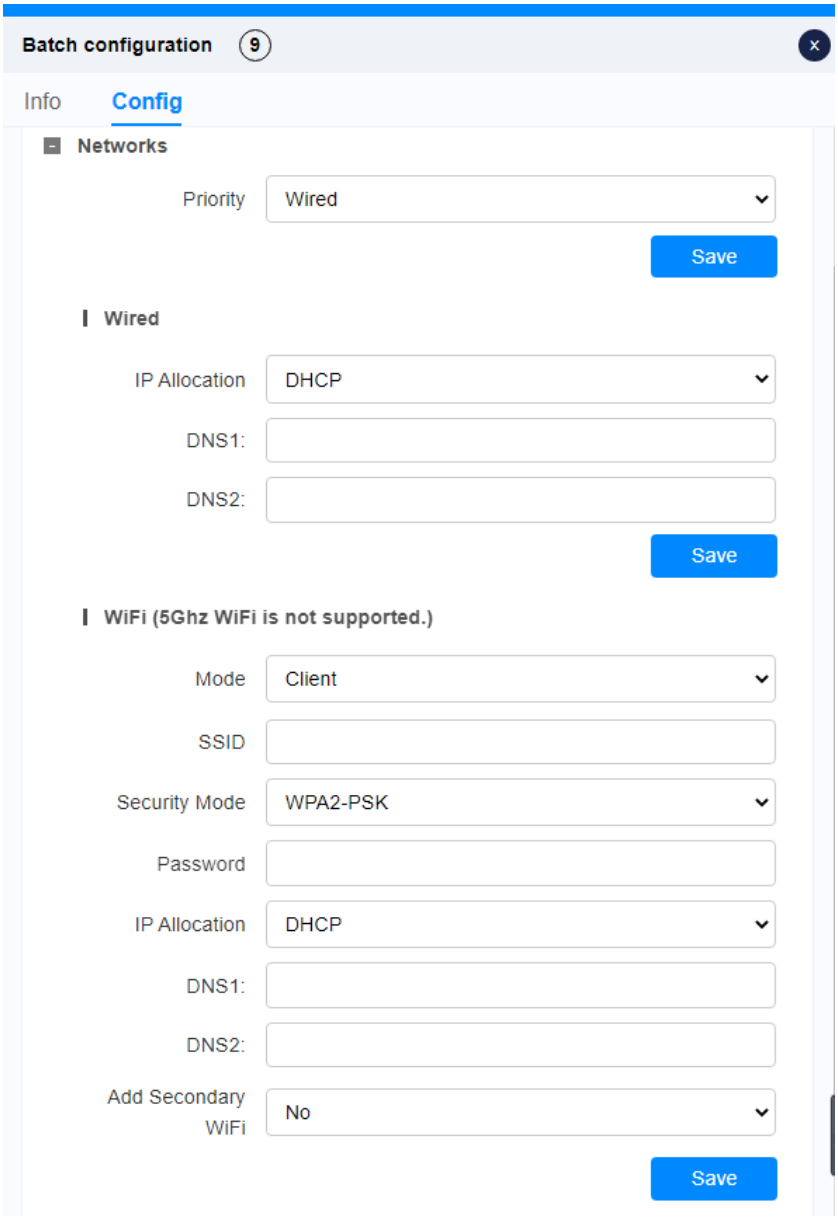
- Cassia Bluetooth stack switch
- Avoid 2.4G Interference: Reduce interference between 2.4GHz Wi-Fi and Bluetooth
- Scan mode parameters
- Connection mode parameters



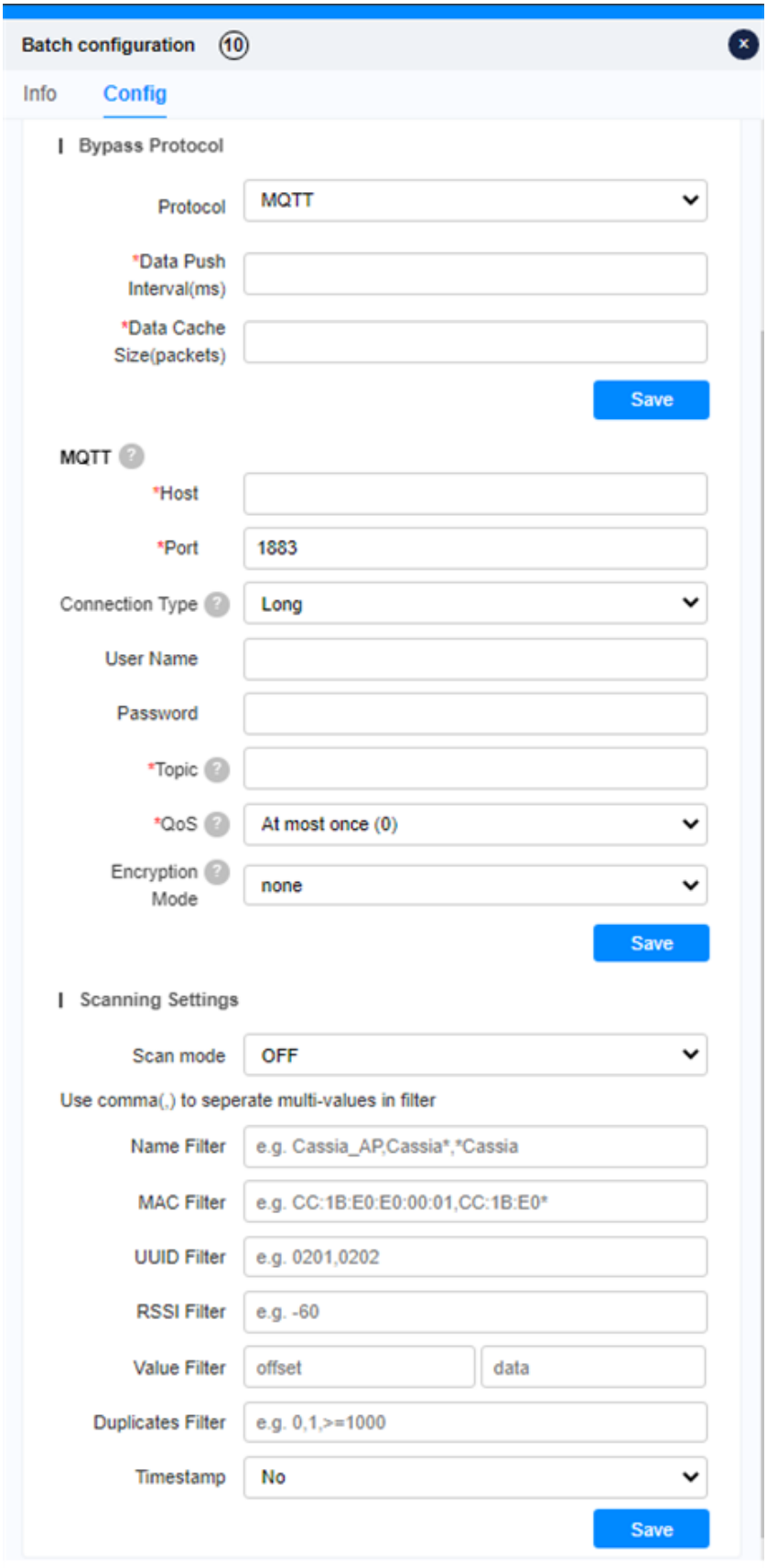
The following network parameters can be configured in batches

- Network priority
- Ethernet IP allocation method: can only be batch configured to DHCP
- WIFI working mode
    - In Client mode, the IP allocation method can only be batch configured to DHCP
    - Please don’t modify to Hotspot mode in batches. Otherwise, the Hotspot SSID and password of all gateways will be the same
- Add secondary WIFI: it will work as the backup WIFI SSID if the gateway failed to connect to the first WIFI SSID

The cellular modem configuration needs to be configured on the local console of the gateway. They can’t be configured in batches from AC.



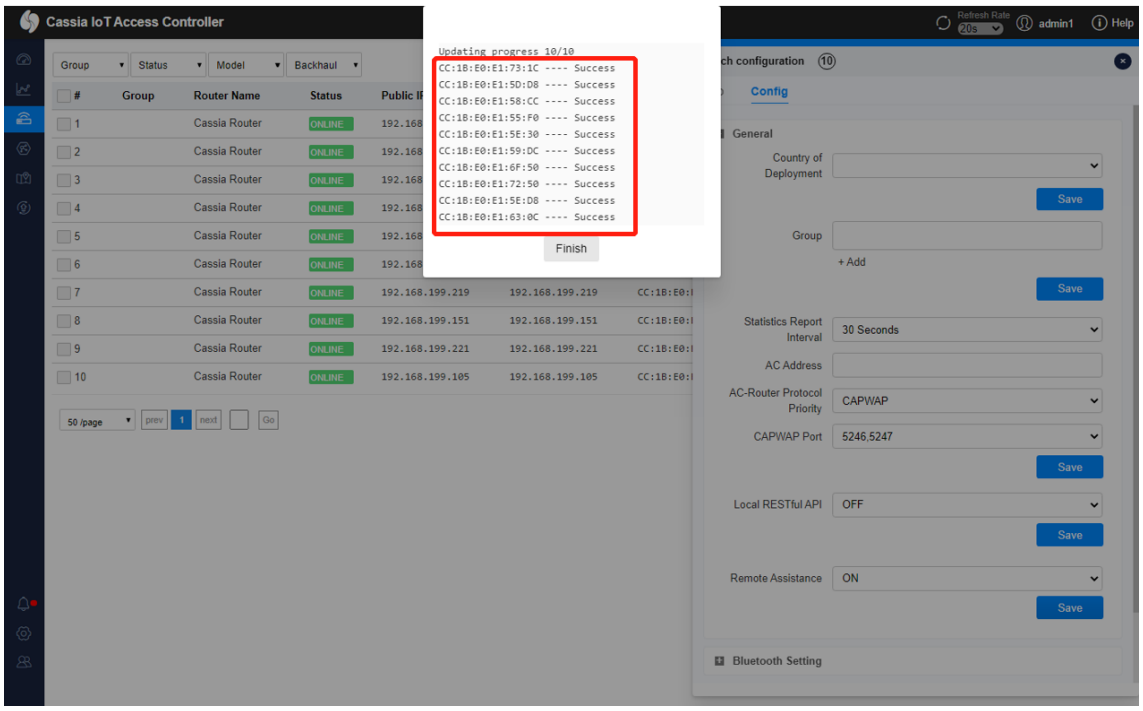
The parameters of the bypass function can be configured in batches too.



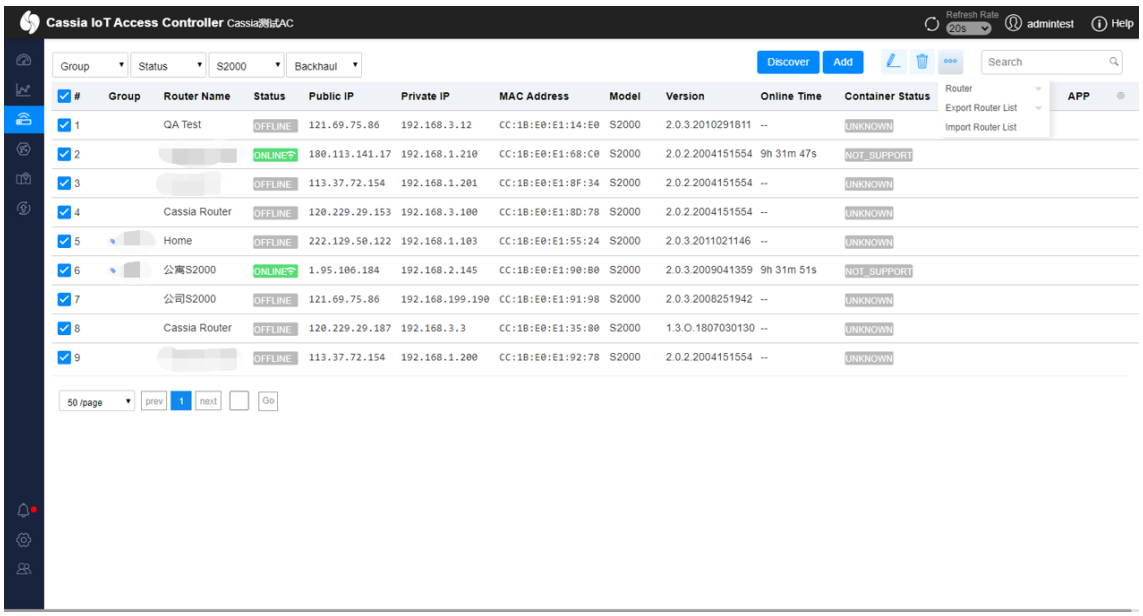
Now, you can save the configuration. After clicking the corresponding save button, the batch configuration will start. You can check the progress and results (success or failure) of the configuration on AC.

TIPS

- Only one type of parameter can be configured in batches at a time, for example, Ethernet parameters and WIFI parameters can't be configured at the same time. If you want to configure multiple types of parameters, please configure them separately.
- If the configuration of some gateways fails, you can copy the configuration results (see the red part in the below figure), and try to configure these gateways again later.



Similarly, you can also perform batch upgrades, restarts, and resets for the Bluetooth gateways. You can also perform batch operations for the containers and APPs.

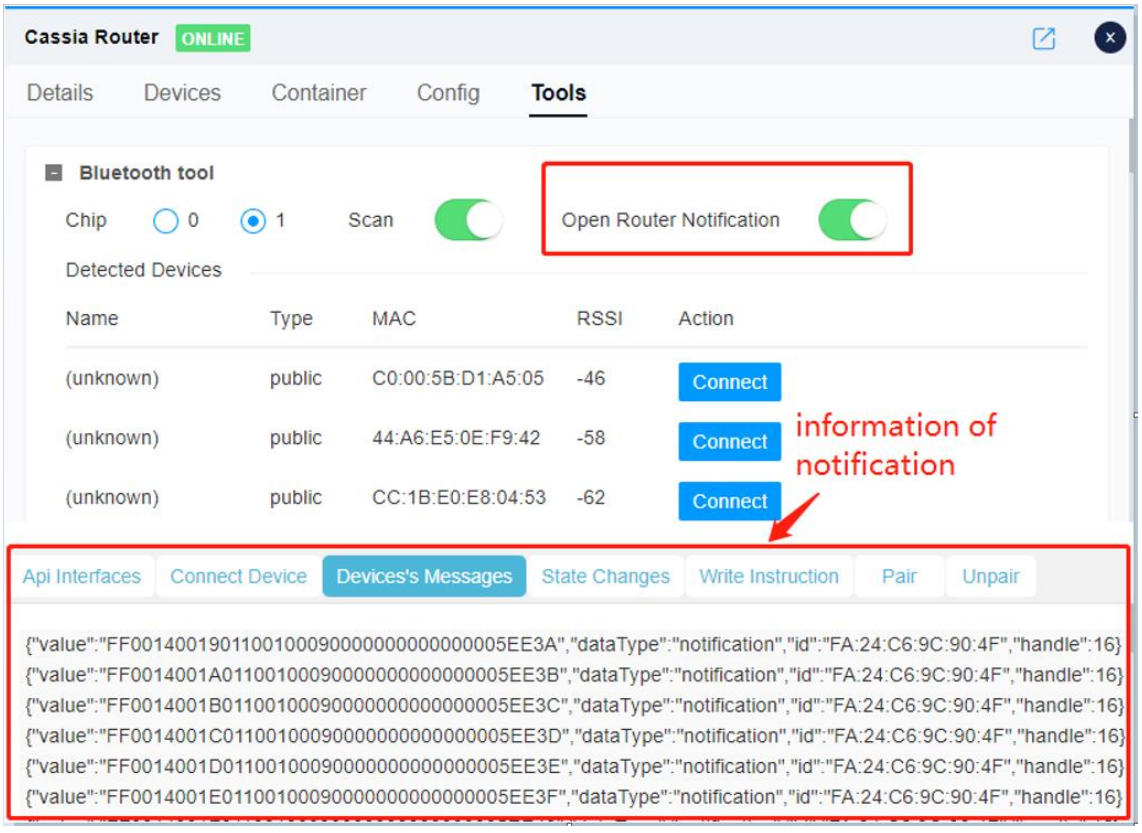


6.8. Bluetooth Debug Tool

From firmware 1.4, Cassia AC provides a simplified Bluetooth debug tool with UI (read only user doesn't have the permission). This debug tool simplifies the integration of the Bluetooth Low Energy devices and the user application with the Cassia AC and Bluetooth gateway.

The user can use this simplified Bluetooth debug tool to select a chip, start and stop the scan, connect and disconnect, pair and unpair, get services, write by the handle, and receive notifications and indications. The user can also check the RESTful API, API response messages and the Bluetooth Low Energy data on the debug tool.

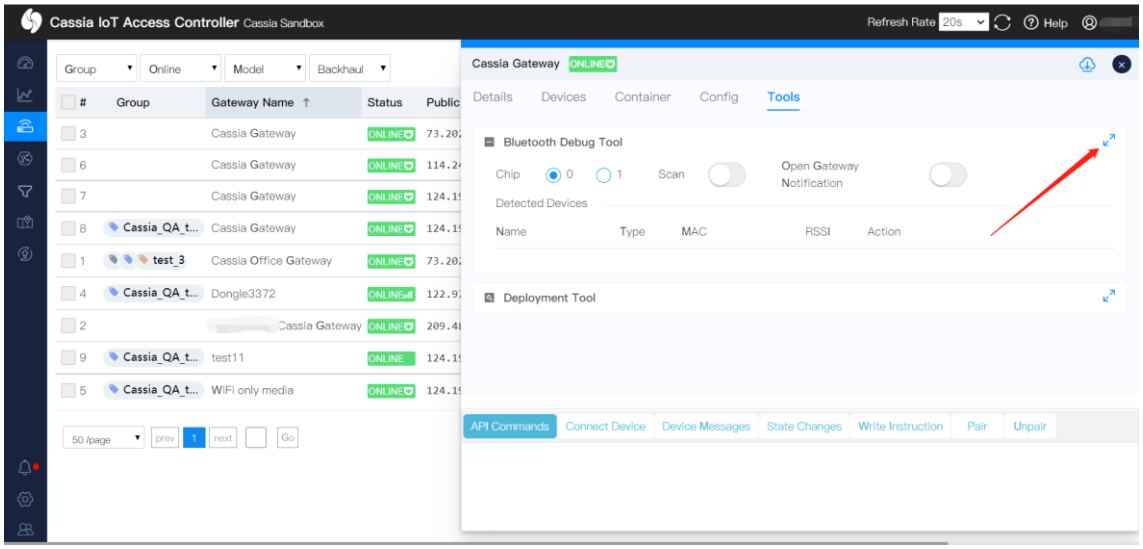
Please connect a Cassia gateway to the Cassia AC, power on the Bluetooth devices, and place them near the Cassia gateway. Please click the gateway from the Gateway list, and click the Tools tab. See the screenshot of the simplified Bluetooth debug tool below.

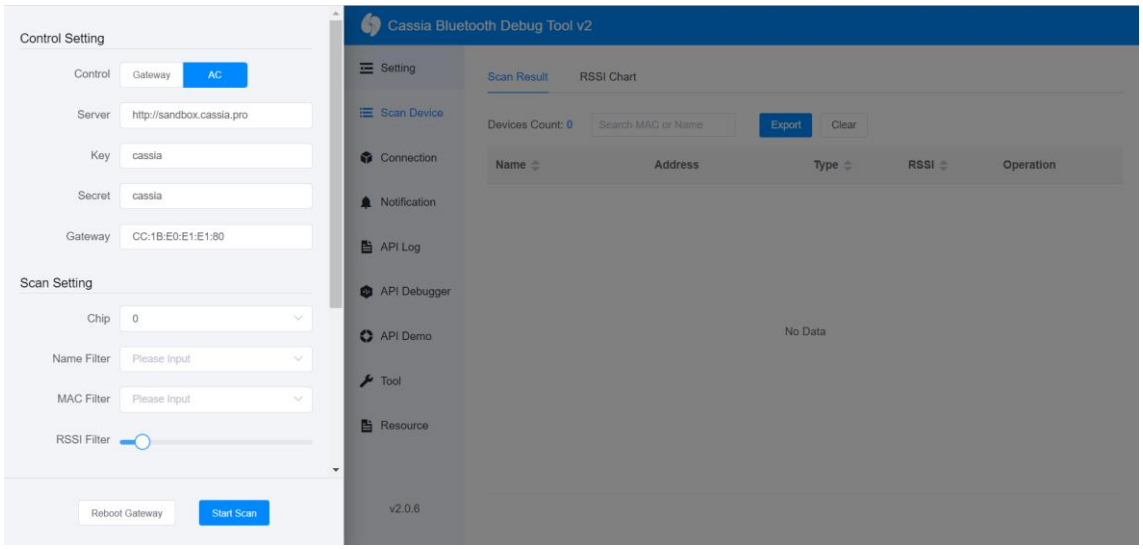


Simplified Bluetooth Debug Tool in Cassia AC

For more information, please check the Cassia AC Bluetooth Debug Tool User Guide here: https://www.cassianetworks.com/support/knowledge-base/general-documents/.

Cassia AC also offers a full version Bluetooth debug tool like below.





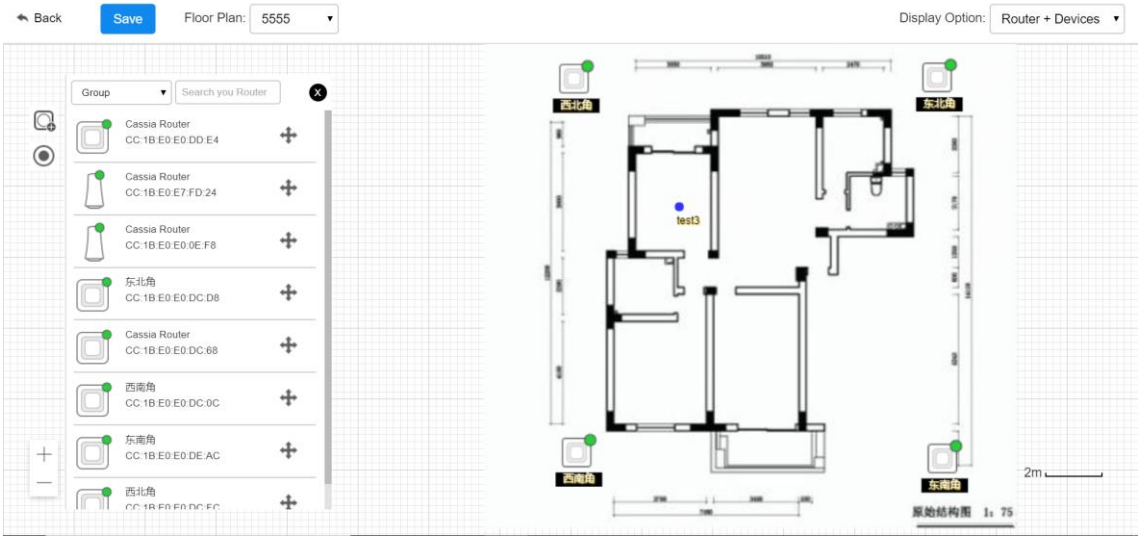
Please use “Cassia Bluetooth Debugger 2” on http://www.bluetooth.tech, if you are using AC software lower than v1.4 or you are a read only user (doesn’t have the permission to run Bluetooth debug tool in AC).

6.9. Enhanced Locationing

From firmware 2.0, the Cassia IoT Access Controller (AC) provides Enhanced Locationing functionality and the corresponding RESTful API (is a Beta version now). The Cassia IoT AC in conjunction with multiple Cassia Bluetooth gateways can triangulate the position of the Bluetooth Low Energy devices within its coverage. The accuracy of the enhanced locationing function is about 5 meters.

The user can use this RTLS (Real-Time Location System) function in the AC console directly. The user can also integrate the RESTful API with the user’s people and assets tracking system.

For more information, please check the Cassia Enhanced Locationing User Guide here: https://www.cassianetworks.com/support/knowledge-base/general-documents/.

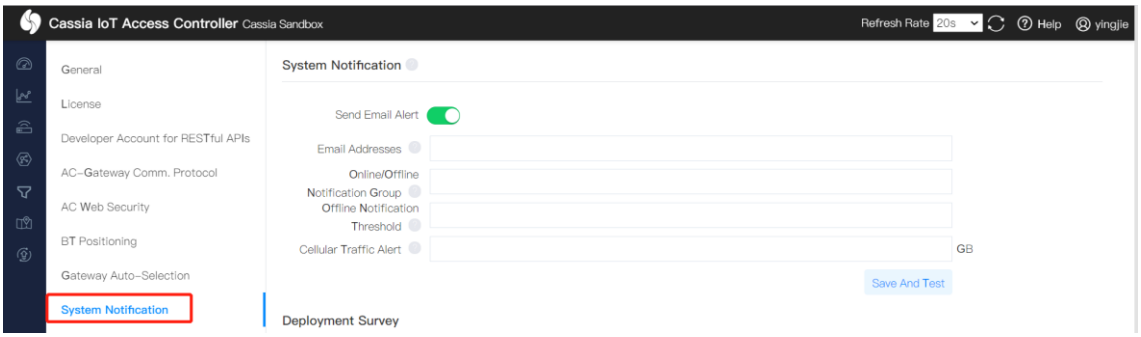


Enhanced Locationing in Cassia AC

6.10. System Notification

From firmware 2.0, the Cassia Access Controller (AC) provides system notification function. AC will send email alerts to you in the below conditions.

- AC CPU/RAM/storage usage is higher than 80%: maximum one email every day
- AC license will expire within 30 days or has expired: maximum one email every day
- More than the pre-configured number of gateways is offline within 5 minutes: send an email immediately
- Any gateway in the specific group goes offline or online: send an email immediately. The user can tag one gateway with a maximum of three groups.
- Aggregated (all the gateways that use USB cellular modems) cellular data usage in this calendar month is greater than the pre-configured threshold: maximum one email every day



Please configure the email addresses (multiple emails split with ";") that you would like to receive the email alerts, the group to monitor (maximum one group), the number of offline gateways within 5 minutes, and the threshold of aggregated cellular data usage in one calendar month. Please remember to add AC's Site Name in AC setting page, then the user will know which AC sent the system notification emails.

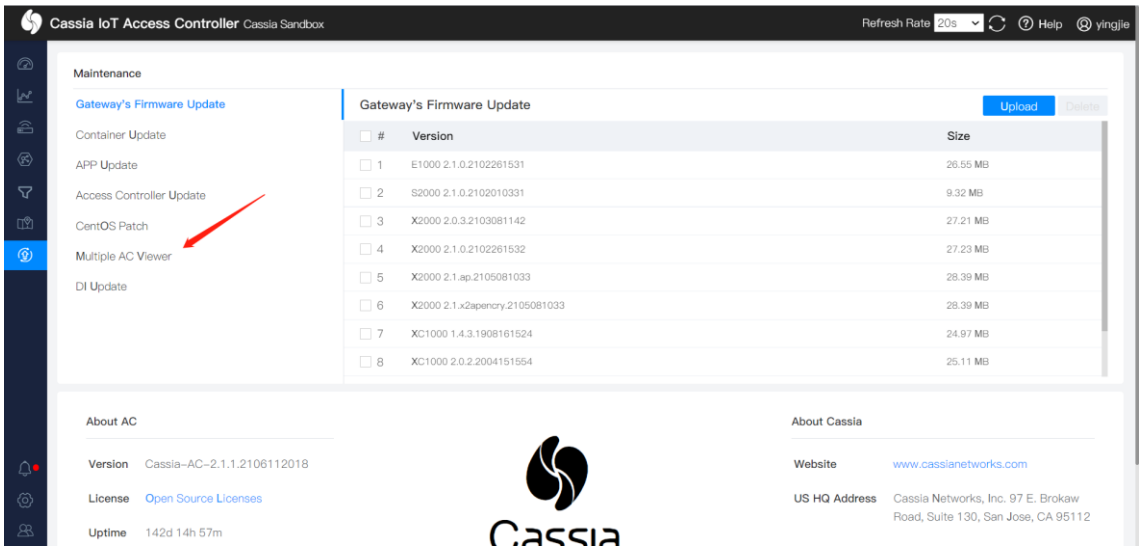
From firmware 2.1.1, customers can configure which email server should be used to send the email alerts. Below are several examples. If the configuration is correct, AC will send a test email to you right away.

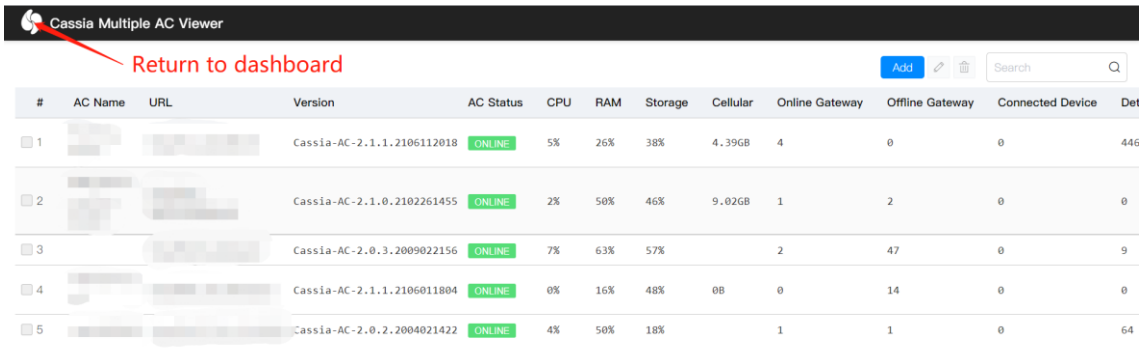
Email Server	SMTP Host	SMTP Port	SSL	TLS
Outlook	smtp-mail.outlook.com	587	False	True
Yahoo	smtp.mail.yahoo.com	587	True	False
Aliyun	smtp.mxhichina.com	465	True	False
163	smtp.163.com	465	True	False

6.11. Multiple AC Viewer

From firmware 2.1.1, the multiple AC viewer provides a central place to monitor the AC online/offline status, AC resource consumption (CPU/Memory/Storage/Cellular), online/offline gateways, and connected/detected devices for all their ACs.

To add a new AC to the monitoring list, please provide the AC Address, Developer Key & Secret (in AC setting page) of the AC.



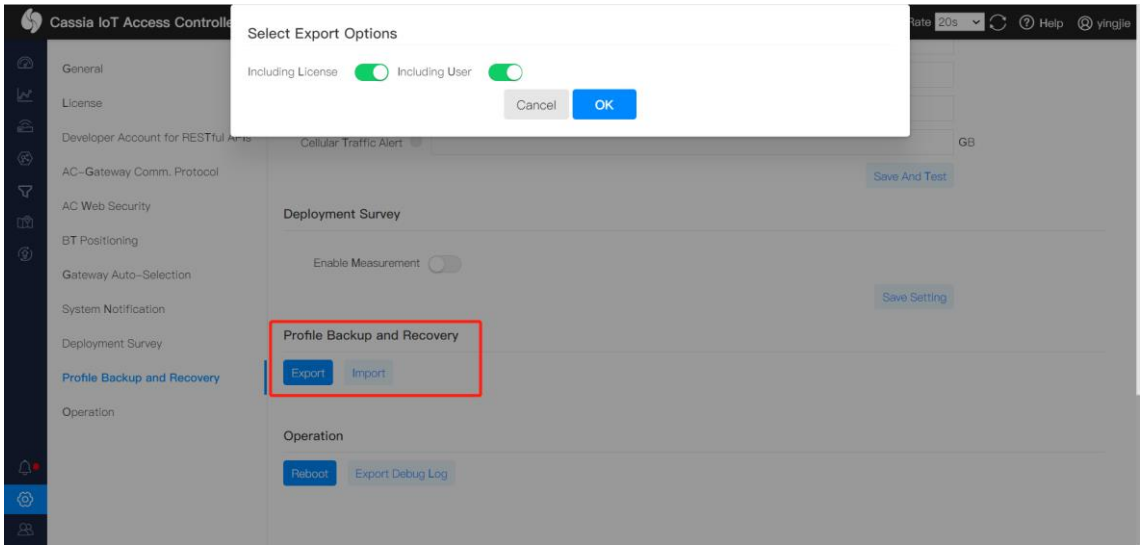


6.12. Backup AC Configuration

From firmware 2.0, customers can export the license, setting, user accounts, floor plan, gateway list, and roaming data of AC to a backup encrypted file. Please store the backup file in a secure manner.

Customers can recover the AC's configuration by importing a backup file. **NOTE**: The backup file can't be imported to the AC on a different server if the backup file includes AC license (can be excluded when exporting the backup file).

For security reasons, the Developer Key and Developer Secret is not exported to the backup file. Please input your Developer Key and Developer Secret in AC setting page after importing the backup file. You can find them in your IoT application.



7. Cassia RESTful APIs

The Cassia RESTful APIs were developed to enable third-party developers and device manufacturers to utilize Cassia's gateway Bluetooth routing and extended range capabilities while using their Cloud services to connect and control multiple Bluetooth Low Energy devices per gateway simultaneously.

Furthermore, the Cassia RESTful APIs are designed to integrate directly into the application/server using an HTTP/HTTPS-based communication protocol, which provides programming language flexibility. Cassia supports C#, Node.js, and Java, but the user can choose other languages as needed.

The Cassia RESTful APIs are built into the Cassia IoT Access Controller (AC) and Bluetooth gateways and provide the following functions:

a. Monitor Bluetooth gateways and Bluetooth Low Energy devices
b. Connect and control Bluetooth Low Energy devices
c. Support three modes: scanning, connecting, broadcasting/advertising
d. Write/read data to/from the Bluetooth Low Energy device via the Cloud server
e. Read data as notification/indication events from the Bluetooth Low Energy device via the Cloud server
f. Bluetooth 4.2 Secure Pairing
g. Room based and triangle-based location tracking

Cassia RESTful API supports HTTP (port 80) and HTTPS (port 443). We strongly suggest you to use HTTPS. Please switch on "Enable HTTPS" in AC setting page and fill in your SSL server certificate and private key. For more information about how to generate SSL certificate and key, please see section 5.5.

From firmware 2.1.0, a PHY update API is introduced to support Bluetooth Low Energy 5.0 higher data rates (2M PHY) and long range features. PHY update API is used to switch to a different PHY after a Bluetooth connection is set up. Different PHY (2M, 1M, Coded w/ S2, Coded w/ S8) can be used in two directions of a connected device or used in two connections of two devices. The BLE5.0 advertising extensions don't need a new API.

NOTE: The maximum number of SSE connections for one gateway is 32. Cassia's 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 close unused SSE connections by closing the HTTP connection. It is not recommended to frequently open and close combined SSE connections.

NOTE: From firmware 2.0, the output of the RESTful API to obtain gateway configuration from AC will be changed (GET http://{your AC domain}/api/cassia/info?mac= <hubmac>). The container status will be removed from the default API output, to avoid the oversized UDP packets problem. Container status can be got separately by the same API with the additional parameter 'fields=container'. Please refer to SDK WIKI for details.

NOTE: Room-based and triangle-based location tracking APIs and gateway auto-selection APIs lead to increased gateway traffic (high 4G cost) and increased CPU consumption. It is recommended to only enable "BT Positioning" and "Gateway Auto-Selection" on the AC setting page when needed. What is more, after upgrading AC from version 1.4.3 to version 2.0.2 and above, please double check if the "Gateway Auto-Selection" in AC setting page is still OFF.

NOTE: From v2.1.0, if the end-user's HTTP Restful API request contains "Accept-Encoding: *", the gateway will use gzip to compress the content of the HTTP response. It will reduce the traffic between the gateway and AC. It will also accelerate the HTTP response. If the HTTP request doesn't contain Accept-Encoding, the gateway will not compress the HTTP response (legacy behavior).

NOTE: 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 consistent with local API in which 'evtType' is used. For example,
{"bdaddrs":[{"bdaddr":"E1:D2:F8:F9:82:E0","bdaddrType":"random"}],"adData":"020100000000000000000000000000","name":"(unknown)","rssi":-29,"evtType":0}

For details on Cassia RESTful API guidelines, please check the Github wiki site: https://github.com/CassiaNetworks/CassiaSDKGuide/wiki.

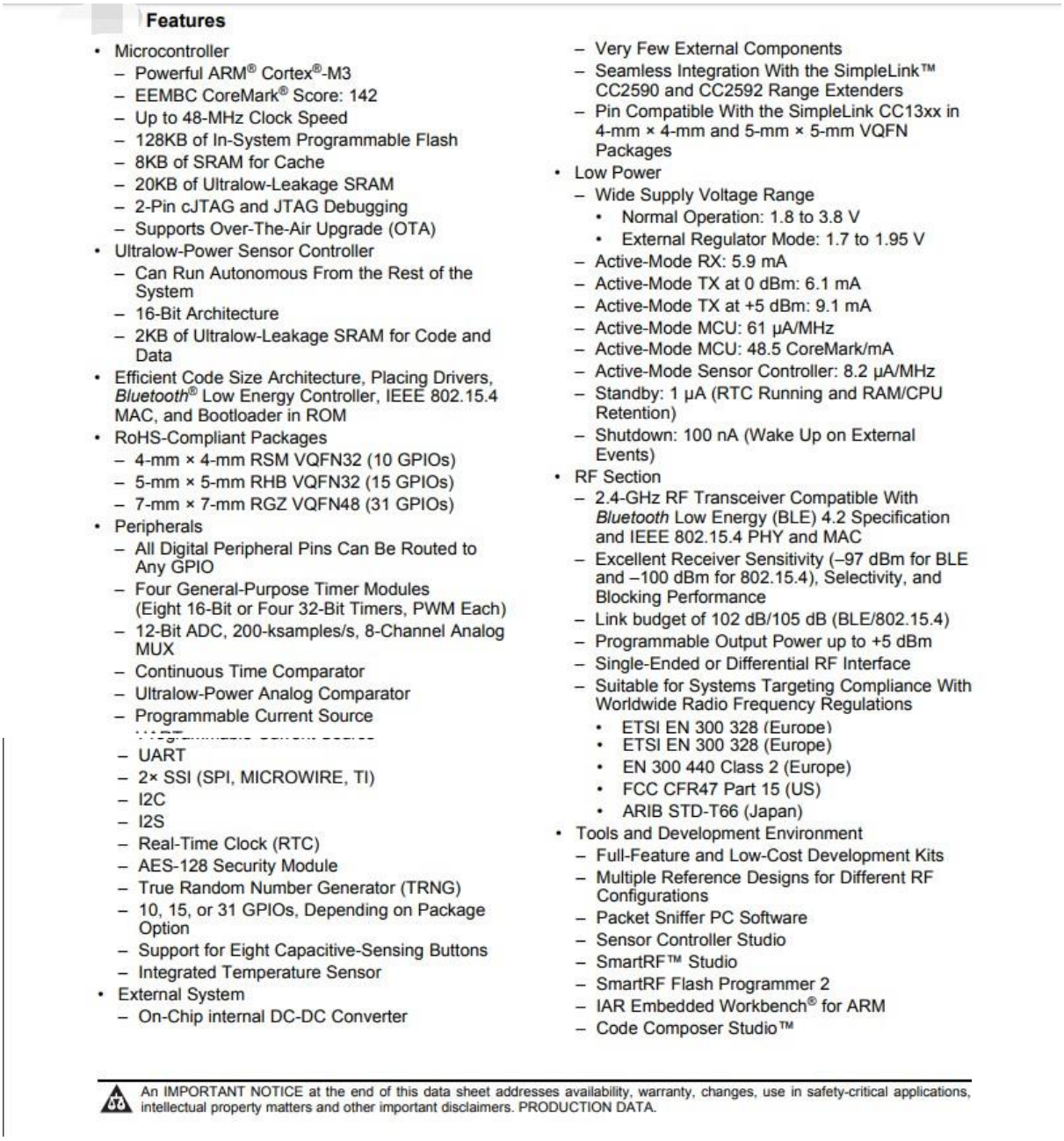
Appendix A: Cassia's TI Sensor Tag Demo

Cassia's demonstrations showcase the Cassia Bluetooth gateways and AC in use with off-the-shelf Bluetooth Low Energy devices. Please see the full list at http://www.bluetooth.tech. The following section demonstrates a Cassia Bluetooth gateway and AC in use with a Texas Instruments (TI) Sensor Tag CC2650STK.

TI Sensor Tag

1.2 Applications

- Consumer Electronics
- Mobile Phone Accessories
- Sports and Fitness Equipment
- HID Applications
- Home and Building Automation
- Lighting Control
- Alarm and Security
- Electronic Shelf Labeling
- Proximity Tags
- Medical
- Remote Controls
- Wireless Sensor Networks



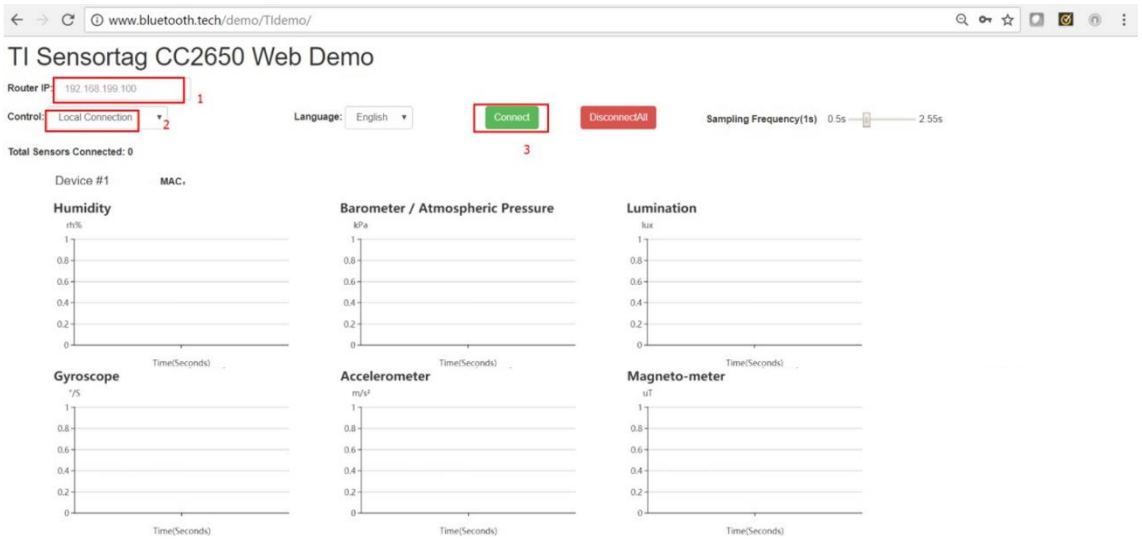
Features

- Microcontroller
  - Powerful ARM® Cortex®-M3
  - EEMBC CoreMark® Score: 142
  - Up to 48-MHz Clock Speed
  - 128KB of In-System Programmable Flash
  - 8KB of SRAM for Cache
  - 20KB of Ultralow-Leakage SRAM
  - 2-Pin cJTAG and JTAG Debugging
  - Supports Over-The-Air Upgrade (OTA)
- Ultralow-Power Sensor Controller
  - Can Run Autonomous From the Rest of the System
  - 16-Bit Architecture
  - 2KB of Ultralow-Leakage SRAM for Code and Data
- Efficient Code Size Architecture, Placing Drivers, *Bluetooth*® Low Energy Controller, IEEE 802.15.4 MAC, and Bootloader in ROM
- RoHS-Compliant Packages
  - 4-mm × 4-mm RSM VQFN32 (10 GPIOs)
  - 5-mm × 5-mm RHB VQFN32 (15 GPIOs)
  - 7-mm × 7-mm RGZ VQFN48 (31 GPIOs)
- Peripherals
  - All Digital Peripheral Pins Can Be Routed to Any GPIO
  - Four General-Purpose Timer Modules (Eight 16-Bit or Four 32-Bit Timers, PWM Each)
  - 12-Bit ADC, 200-ksamples/s, 8-Channel Analog MUX
  - Continuous Time Comparator
  - Ultralow-Power Analog Comparator
  - Programmable Current Source
  - UART
  - 2× SSI (SPI, MICROWIRE, TI)
  - I2C
  - I2S
  - Real-Time Clock (RTC)
  - AES-128 Security Module
  - True Random Number Generator (TRNG)
  - 10, 15, or 31 GPIOs, Depending on Package Option
  - Support for Eight Capacitive-Sensing Buttons
  - Integrated Temperature Sensor
- External System
  - On-Chip internal DC-DC Converter
  - Very Few External Components
  - Seamless Integration With the SimpleLink™ CC2590 and CC2592 Range Extenders
  - Pin Compatible With the SimpleLink CC13xx in 4-mm × 4-mm and 5-mm × 5-mm VQFN Packages
- Low Power
  - Wide Supply Voltage Range
    - Normal Operation: 1.8 to 3.8 V
    - External Regulator Mode: 1.7 to 1.95 V
  - Active-Mode RX: 5.9 mA
  - Active-Mode TX at 0 dBm: 6.1 mA
  - Active-Mode TX at +5 dBm: 9.1 mA
  - Active-Mode MCU: 61 µA/MHz
  - Active-Mode MCU: 48.5 CoreMark/mA
  - Active-Mode Sensor Controller: 8.2 µA/MHz
  - Standby: 1 µA (RTC Running and RAM/CPU Retention)
  - Shutdown: 100 nA (Wake Up on External Events)
- RF Section
  - 2.4-GHz RF Transceiver Compatible With *Bluetooth* Low Energy (BLE) 4.2 Specification and IEEE 802.15.4 PHY and MAC
  - Excellent Receiver Sensitivity (–97 dBm for BLE and –100 dBm for 802.15.4), Selectivity, and Blocking Performance
  - Link budget of 102 dB/105 dB (BLE/802.15.4)
  - Programmable Output Power up to +5 dBm
  - Single-Ended or Differential RF Interface
  - Suitable for Systems Targeting Compliance With Worldwide Radio Frequency Regulations
    - ETSI EN 300 328 (Europe)
    - ETSI EN 300 328 (Europe)
    - EN 300 440 Class 2 (Europe)
    - FCC CFR47 Part 15 (US)
    - ARIB STD-T66 (Japan)
- Tools and Development Environment
  - Full-Feature and Low-Cost Development Kits
  - Multiple Reference Designs for Different RF Configurations
  - Packet Sniffer PC Software
  - Sensor Controller Studio
  - SmartRF™ Studio
  - SmartRF Flash Programmer 2
  - IAR Embedded Workbench® for ARM
  - Code Composer Studio™

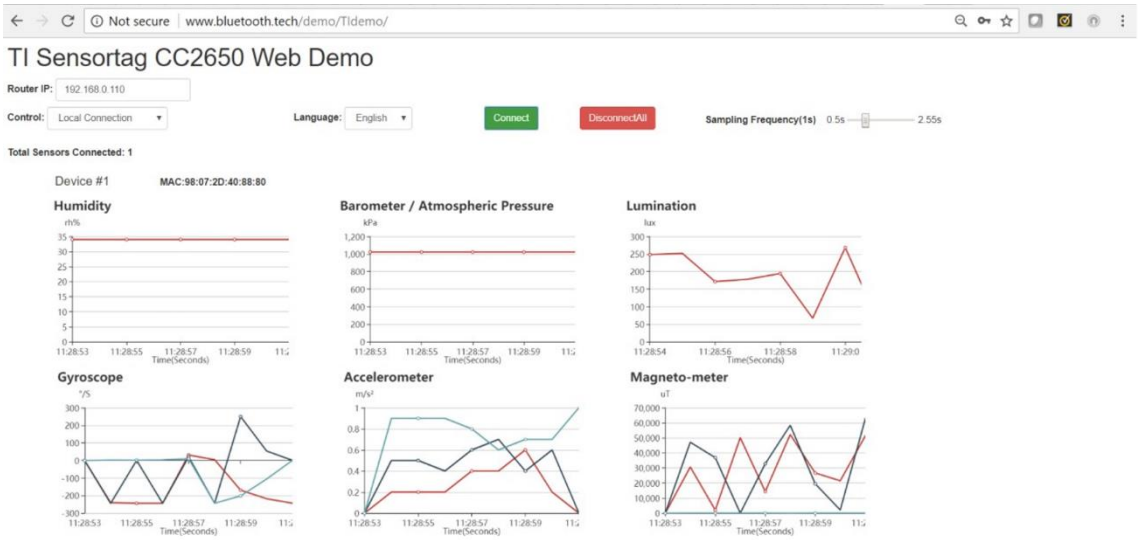
An IMPORTANT NOTICE at the end of this data sheet addresses availability, warranty, changes, use in safety-critical applications, intellectual property matters and other important disclaimers. PRODUCTION DATA.

To test using a local connection:

a) Select Local Connection on Control and enter the private IP address of your Cassia Bluetooth gateway
b) Power on your TI sensor tag. The flashing green light indicates it is working
c) Click the Connect button on the demo page. The TI sensor tag should stop flashing
d) Wait a few seconds and you will see incoming data



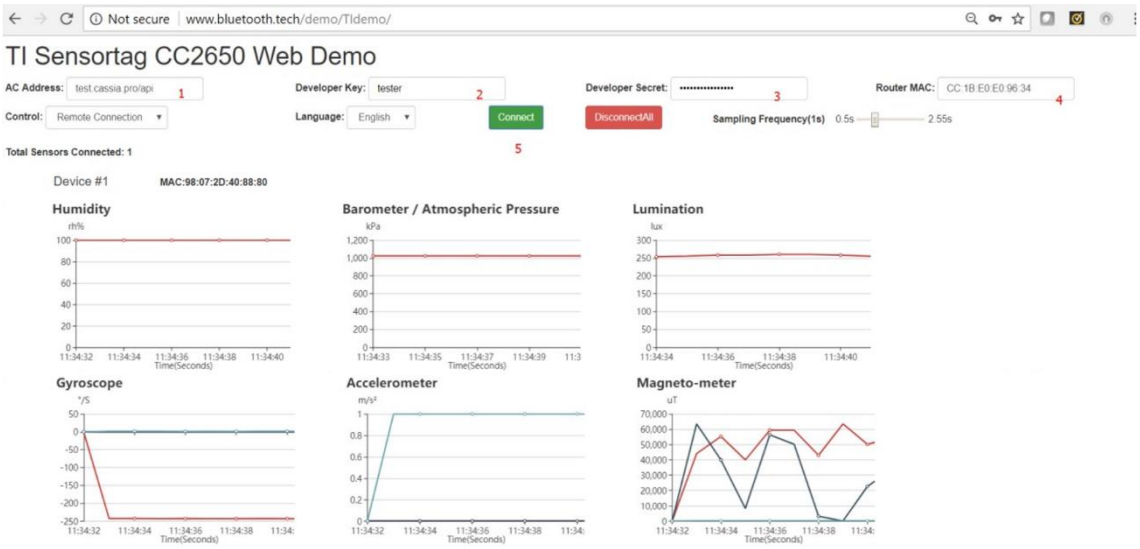
TI SensorTag Demo Page – Local Connection



TI SensorTag Demo Page with Incoming Data

To test using a remote connection:

a) Select Remote Connection on the demo page
b) Enter the AC address, developer key, developer secret, and gateway MAC address
c) Click the red Disconnect All button if you have previously connected the sensor using local mode. You should see the TI sensor tag flashing in the green light
d) Click the green Connect button on the demo page. The TI sensor tag light should stop flashing now
e) Wait a few seconds and you will see incoming data

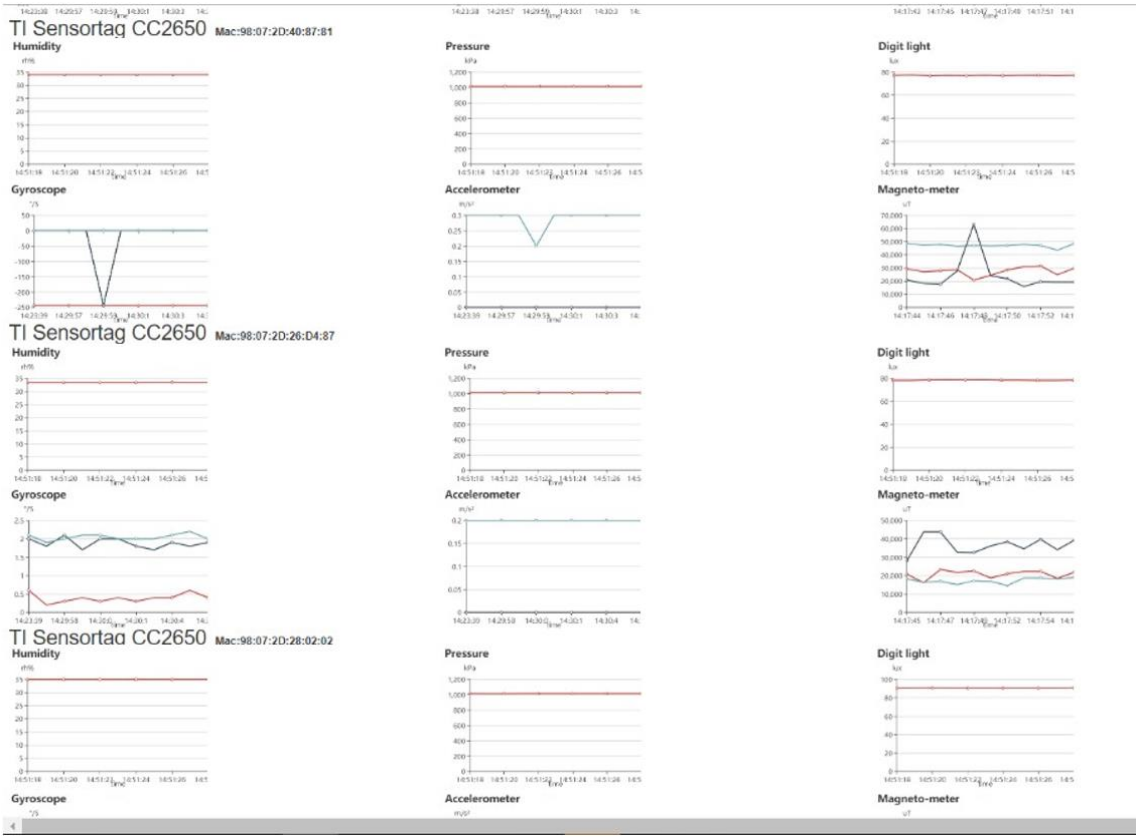


TI SensorTag Demo Page – Remote Connection

In your AC server console, you will see the sensor tag is connected under the Device page.

Cassia AC Device Page

If you power on additional TI sensor tags, they will be connected to the same gateway one-by-one.



TI Sensor Demo Page – With Multiple Sensors

Appendix B: Supported USB Cellular Modems

Please check the excel table on the next page.

Model	Technology & Bands	Data Rate	Carriers Supported	SIM Card Form Factor	Countries/Regions Certified	Size	Supported	Environmental	Comments
Huawei MS2131i-8	HSAP+ / UMTS / EDGE / GPRS / GSM 3G (UMTS): B1 (2100 MHz), B2 (1900 MHz), B5 (850 MHz), B8 (900 MHz) 2G (GSM): B2 (1900 MHz), B3 (1800 MHz), B8 (900 MHz), B5 (850 MHz)	3G (UMTS HSPA+): 21.6 Mbps, HSPA: 14.4 Mbps, HSDPA: 7.2 Mbps, HSUPA: 5.76 Mbps 2G (GSM EDGE): 236.8 Kbps, GPRS: 85.6 Kbps	Vodaphone, AT&T, T-Mobile, etc. UMTS/HSPA Multi-Carrier GSM Certified Global Certifications	Mini SIM (2FF)	China, European Economic Area, USA, Canada, Malaysia, Taiwan, South Africa, Mexico, Argentina, South Korea, Japan, Australia / New Zealand, Israel, EAC Economic Union (Russia, Belarus, Kazakhstan, Armenia and Kyrgyzstan)	84.9 mm x 27 mm x 12.3 mm	1.4.3 +		
Huawei E3372s-153 (also known as T-Mobile/Telekom Speedstick LTE V) Huwei E3372h-153	4G (LTE): B20/B8/B3/B1/B7 (800/900/1800/2100/2600 MHz) 3G (UMTS): 900/2100 MHz 2G (GSM): 850/900/1800/1900 MHz	4G (LTE FDD): DL: 150 Mbps / UL: 50 Mbps @20 MHz Bandwidth 3G (UMTS DCHSPA+): 42 Mbps / 5.76 Mbps; 21Mbps / 5.76 Mbps; 14 Mbps / 5.76 Mbps; HSUPA: 7.2 Mbps / 5.76 Mbps 2G (GSM EDGE): up to 236.8 Kbps	T-Mobile, Other carriers like Vodafone if the cellular modem has no SIM lock.	Mini SIM (2FF)	European Economic Area	88 mm x 28 mm x 11.5 mm	1.4.3 +		
Huawei E8372h-153 (Europe) Huawei E8372h-155 (China) Huawei E8372h-320 (Europe, added in firmware v2.1.1) Huawei E8372h-820 (China, added in firmware v2.1.1)	LTE / DC-HSPA+ / HSPA+ / HSPA / UMTS / EDGE / GPRS / GSM 4G (LTE): B1 (2100 MHz), B3 (1800 MHz), B7 (2600 MHz), B8 (900 MHz), B20 (800 MHz). TD-LTE B39/40/41 for E8372h-155/820 only. FDD-LTE B5 for E8372-320 only 3G (UMTS): B1 (2100 MHz), B8 (900 MHz) 2G (GSM): 850 MHz / 900 MHz / 1800 MHz / 1900 MHz Wi-Fi Hotspot: WLAN 2.5 GHz (802.11b, 802.11g, 802.11n); Supports up to 10 Wi-Fi users.	4G (LTE FDD): up to DL 150 Mbps and UL 50 Mbps @20 MHz Bandwidth 3G (UMTS DC-HSPA+): downlink up to 43.2 Mbps 3G (UMTS HSUPA): uplink up to 5.76 Mbps 2G (GSM EDGE): up to DL 296 Kbps and UL 236.8 Kbps	Multiple Carriers	Mini SIM (2FF)	European Economic Area, China	94 mm x 30 mm x 14 mm	1.4.3 + E8372h-320/820 from 2.1.1		Cassia router can connect to this modem via WiFi.
Novatel USB730L	4G LTE (LTE - LTE-U, CAT 6; US bands: B2/B4/B5/B13; Global bands: B3; Carrier Aggregation: B13+B4, B13+B2, B4+B2, B4+B4, B2+B2, B2+B5, B4+B5. Quad band - GPRS/EDGE; Quad band UMTS/HSPA; CDMA2000 1xRTT / EvDOrA) 3G (UMTS): B1 / B2 / B5 / B8 3G (CDMA EV-DO): BC0 (800 Mhz) / BC1 (1900 Mhz PCS) 2G (GSM): B2 / B3 / B5 / B8	Up to 300 Mbps downlink and 50 Mbps uplink	Verizon	Nano SIM (4FF)	USA, Canada	83 mm x 35 mm x 11.4 mm (not including USB connector)	1.4.3 +		After the USB cellular modem configuration is completed on the AC or router console, please make sure to power-cycle the router or unplug and re-plug in the USB cellular modem. In order to fit the USB730L into the bottom enclosure of the X1000, the USB connector of U730L should be turned over. Please see the User Manual for instructions. Search for "Novatel USB730L" and look at the NOTE comments.
MultiTech MTD-MVW1	4G (LTE CAT M1): B4 (AWS 1700 Mhz), B13 (700 Mhz)	Up to 300 Kbps downlink and 375 Kbps uplink	Verizon	Mini SIM (2FF)	USA, Canada	78.7 mm x 40.1 mm x 18.8 mm (not including USB cable)	1.4.3 +	Operating temperature: -40° to +122° F (-40° to +50° C) Storage temperature: -40° to +185° F (-40° to +85° C) Humidity: Relative humidity 15% to 93% noncondensing	LTE CAT M1 only modems. They can only access the cellular network where LTE CAT M1 is enabled. What is more, the router upgrade may take more than one hour because limited CAT M1 throughput.
MultiTech MTD-MNA1	4G (LTE CAT M1) Verizon: B4 (AWS 1700 Mhz), B13 (700 Mhz) AT&T: B2 (1900 Mhz), B4 (AWS 1700 Mhz), B12 (700 Mhz)	Same as MultiTech MTD-MVW1	Verizon, AT&T and other cellular operators	Mini SIM (2FF)	USA, Canada	Same as MultiTech MTD-MVW1	1.4.3 +	Same as MultiTech MTD-MVW1	LTE CAT M1 only modems. They can only access the cellular network where LTE CAT M1 is enabled. What is more, the router upgrade may take more than one hour because limited CAT M1 throughput
MultiTech MTCM-LAT3-B03	4G (LTE CAT 1): B2(1900MHz), B4 (AWS 1700MHz), B5 (850MHz), B12 / B13 (700MHz) 3G (UMTS): B2 (1900MHz), B5 (850MHz)	Up to 10 Mbps downlink and 5 Mbps uplink	AT&T, T-Mobile, and other cellular operators	Micro SIM (3FF)	USA, Canada	53.5 mm x 45.5 mm x 19.8 mm without antenna (please use flexible ribbon antennas if you want to put MTCM-LAT3-B03 inside X1000 enclosure)	1.4.3 +	Storage and operating temperature: -40° to +185° F (-40° to +85° C) Humidity: Relative humidity 15% to 85% noncondensing	If customer wants to put this in the X1000, they need ribbon cable antennas.
MultiTech MTCM-LNA3-B03	Same as MultiTech MTCM-LAT3-B03	Same as MultiTech MTCM-LAT3-B03	Verizon, AT&T, T-Mobile, and other cellular operators	Micro SIM (3FF)	USA, Canada	Same as MultiTech MTCM-LAT3-B03	1.4.3 +	Same as MultiTech MTCM-LAT3-B03	If customer wants to put this in the X1000, they need ribbon cable antennas.
MultiTech MTCM-LSP3-B03	Same as MultiTech MTCM-LAT3-B03	Same as MultiTech MTCM-LAT3-B03	Sprint	Micro SIM (3FF)	USA, Canada	Same as MultiTech MTCM-LAT3-B03	2.0.2 +	Same as MultiTech MTCM-LAT3-B03	If customer wants to put this in the X1000, they need ribbon cable antennas.
MultiTech MTCM2-L4G1-B03	4G (LTE FDD): B1 (2100 MHz), B2 (1900 MHz), B3 (1800 MHz), B4 (AWS 1700 MHz), B5 (850 MHz), B7 (2600 MHz), B8 (900 MHz), B12/B13 (700 MHz), B18 (850 MHz), B19 (850 MHz), B20 (800 MHz), B25 (1900 MHz), B26 (850 MHz), B28 (700 MHz) 4G (LTE TDD): B38 (2600 MHz), B39 (1900 MHz), B40 (2300 MHz), B41 (2500 MHz) 3G (UMTS): B1 (2100 MHz), B2 (1900 MHz), B4 (AWS 1700 MHz), B5 (850 MHz), B6 (800 MHz), B8 (900 MHz), B19 (850 MHz) 2G (GSM): B2 (1900 MHz), B3 (1800 MHz), B5 (850 MHz), B8 (900 MHz)	Up to 150 Mbps downlink and 50 Mbps uplink	Vodafone, Telefonica, Orange, and other EU operators	Micro SIM (3FF)	European Economic Area/ European Union	62.2 mm x 45.4 mm x 19.8 mm without antenna (please use flexible ribbon antennas if you want to put MTCM2-L4G1 inside X1000 enclosure)	2.0.2 +	Storage and operating temperature: -40° to +185° F (-40° to +85° C) Humidity: Relative humidity 15% to 85% noncondensing	If customer wants to put this in the X1000, they need ribbon cable antennas.
Zoom ZoomCell 4615	4G (LTE CAT 1): B4 (AWS 1700 Mhz), B13 (700 Mhz)	Up to 10 Mbps downlink and 5 Mbps uplink	Verizon	Micro SIM (3FF)	USA	80.9 mm x 50.4 mm x 15 mm (without antenna)	1.4.3 +	Operating temperature: -22° to +140° F (-30° to +60° C) Storage temperature: -40° to +185° F (-40° to +85° C) Humidity: 5% to 95%	May have heat issues encapsulated in the X1000 bottom cap. Better to use outside of the router.
Zoom ZoomCell 4630	4G (LTE CAT 1): B2/B4/B5/B12 3G (UMTS): 850 MHz / 1700 MHz / AWS 2100 MHz / 1900 MHz	LTE CAT 1: up to 10 Mbps downlink and 5 Mbps uplink HSPA: up to 7.2 Mbps downlink and 5.76 Mbps uplink	AT&T, T-Mobile, and other Cellular operators	Micro SIM (3FF)	USA	Same as Zoom ZoomCell 4615	1.4.3 +	Same as Zoom ZoomCell 4615	May have heat issues encapsulated in the X1000 bottom cap. Better to use outside of the router.
ConnectedIO EM1000T-VZ-CAT1	4G (LTE CAT 1): B2 (1900 MHz), B4 (1700 MHz), B13 (700 MHz)	Up to 10 Mbps downlink and 5 Mbps uplink	Verizon	Mini SIM (2FF)	USA	84 mm x 57 mm x 17.79 mm without antenna (please put EM1000T-VZ-CAT1 outside of X1000 enclosure)	1.4.3 +	Operating temperature: -22° to +185° F (-30° to +85°C)	This is too big for the X1000 bottom cap. Place it outside of the router. Power input: 5V DC 0.5A
NXCC UX302NC	4G (LTE): 800/1500/1800/2100 MHz 3G (UMTS): 800/850/2100 MHz 2G (GSM): 850/900/1800/1900 MHz		DoCoMo	Micro SIM (3FF)	Japan	88 mm x 30 mm x 12.2 mm (not including USB connector)	2.0.3 +	Operating temperature: 14° to 122° F (-10° C to 50° C) Humidity: 15% to 90%	Can't use Softbank's SIM card

Appendix C: WPA2 Enterprise Security

From firmware 1.4, Cassia Bluetooth gateway supports 802.1x. It means from firmware 1.4 the user can use WPA2 enterprise Wi-Fi AP as the uplink.

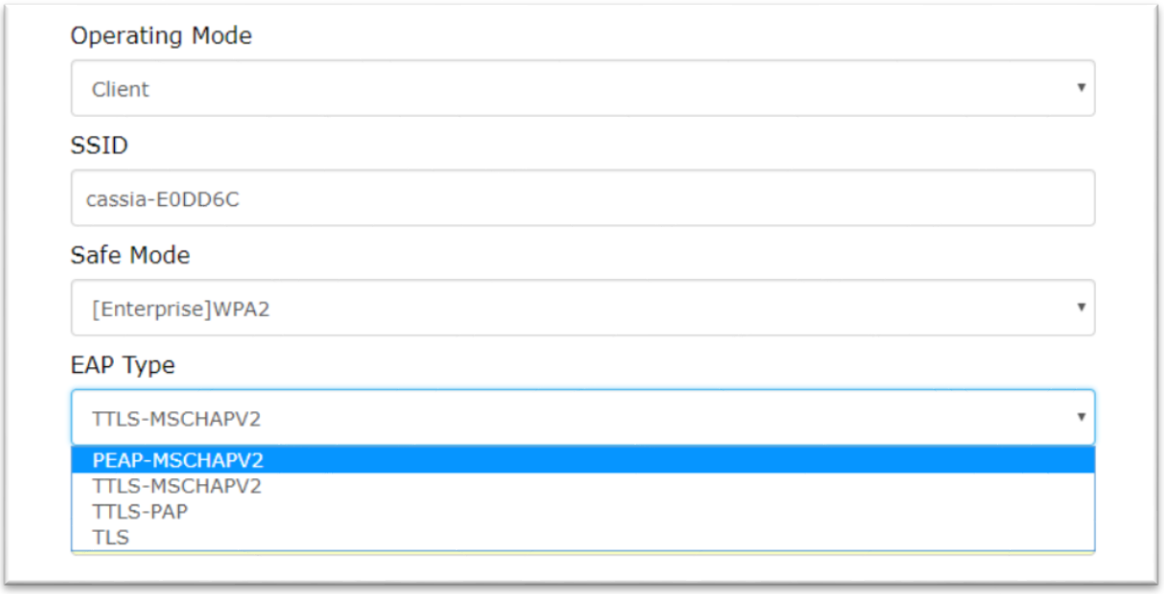
NOTE

- In 1.4 GA firmware, a character return is required for CA certificate, Client Certificate, and Private Key (please check below snapshots). In 1.4.1 GA and 2.0 GA firmware, the character return is optional.
- In 1.4 GA and 1.4.1 GA firmware, please reboot the gateway after updating the CA certificate, Client Certificate, or Private Key. In 2.0 GA firmware, we will fix this issue.
- Only the PEM certificate file format is supported.
- For private keys, Cassia has tested des, des3, seed, and aes. Camellia is not supported.

The user needs to set the Wi-Fi operation mode to “Client”, set the “Safe Mode” and “EAP Type” based on the Wi-Fi AP configuration, and provide required inputs. Then, Cassia Bluetooth gateway will connect to the Wi-Fi AP with WPA2 enterprise enabled.

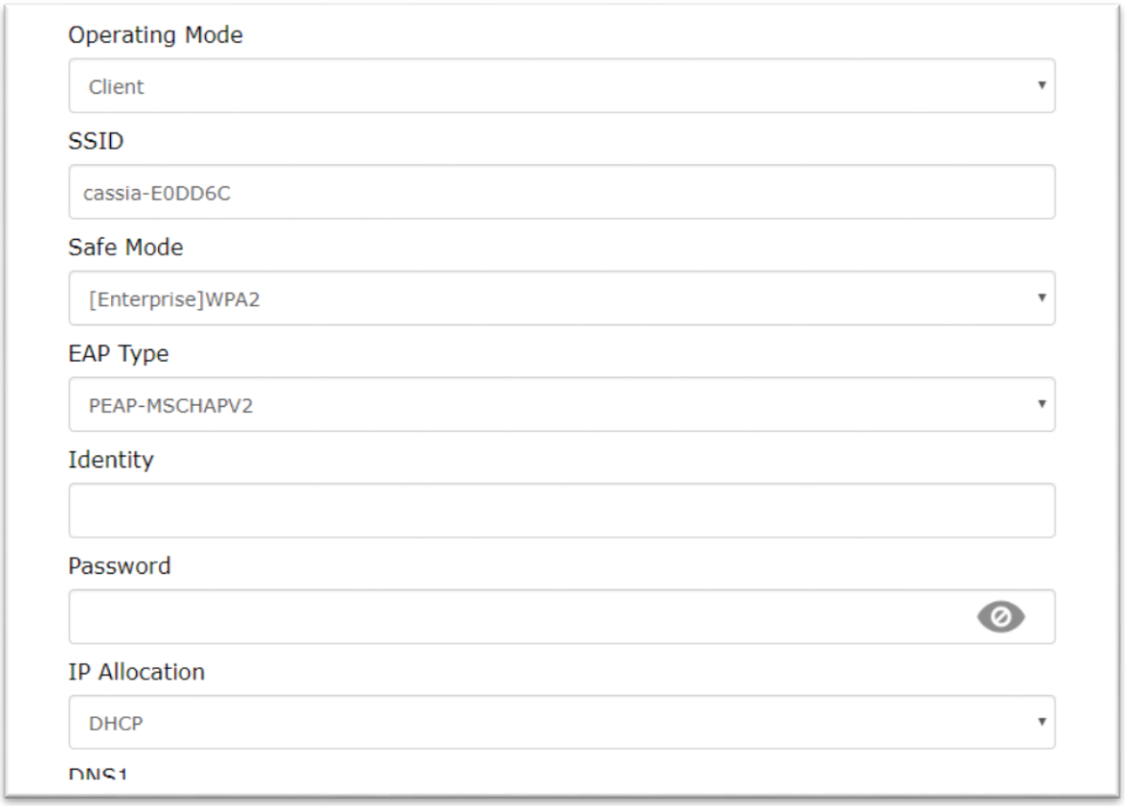
➢ **Safe Mode: [Enterprise] WPA2 or [Enterprise] WPA[TKIP]+WPA2[AES]**

When setting “Safe Mode” to [Enterprise] WPA2 or [Enterprise] WPA[TKIP]+WPA2[AES], the user should select “EAP Type”.



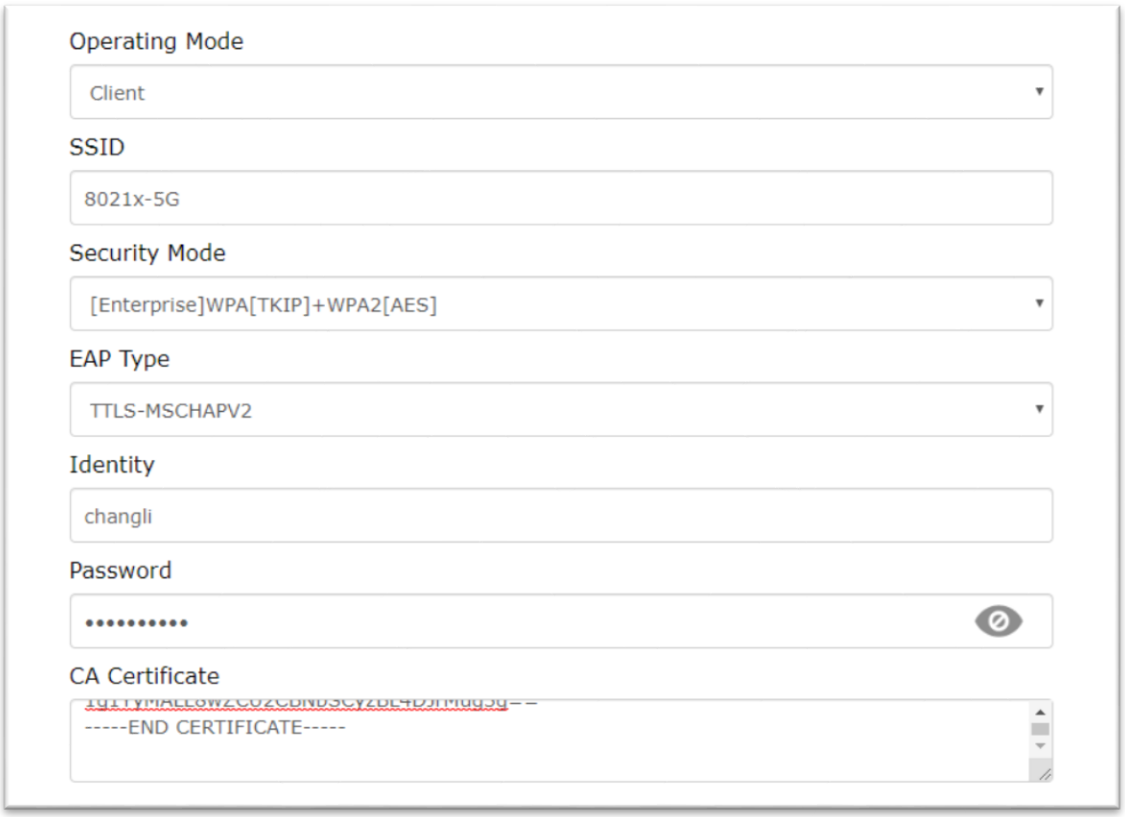
- EPA Type: PEAP-MSCHAPV2

The user should provide Identify and Password, besides SSID, IP, and DNS options. Below is an example.



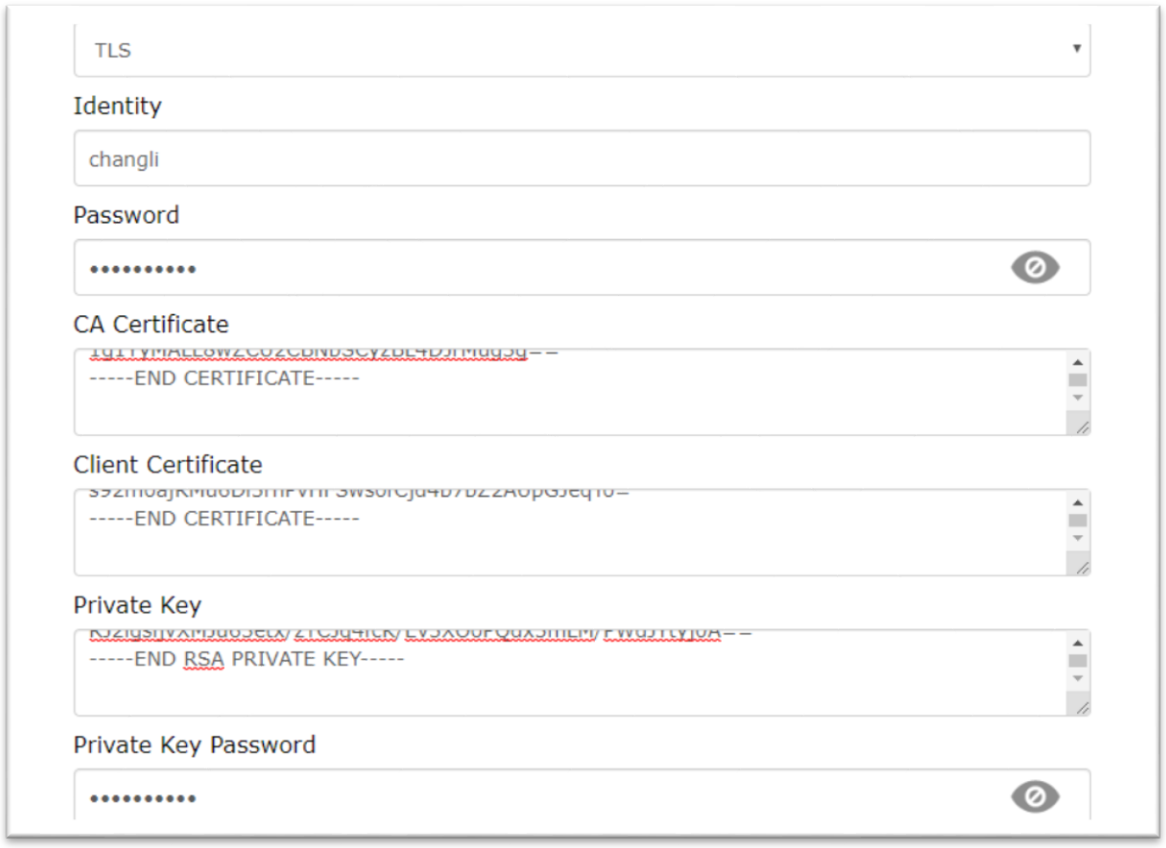
- EPA Type: TTLS-MSCHAPV2 or TTLS-PAP

The user should provide Identify, Password, and CA Certificate, besides SSID, IP, and DNS options. Below is an example.



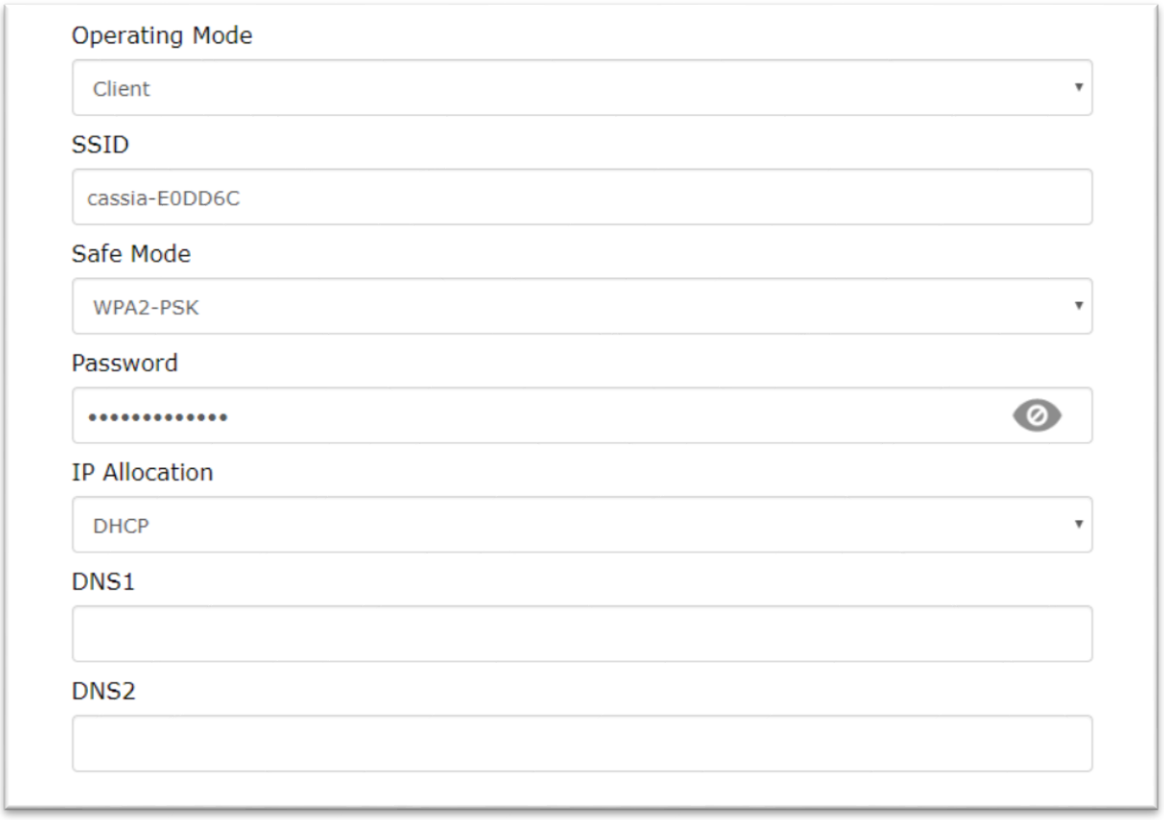
- EPA Type: TLS

The user should provide Identify, Password, CA Certificate, Client Certificate, Private Key, and Private Key Password, besides SSID, IP, and DNS options. Below is an example.



➢ **Safe Mode: WPA2-PSK or WPA[TKIP]+WPA2[AES]**

When setting “Safe Mode” to WPA2-PSK or WPA[TKIP]+WPA2[AES], the Cassia gateway behavior is the same as firmware v1.3. The user should configure SSID, Password, IP, and DNS options. Below is an example.



➢ **Safe Mode: None**

If a password is not needed, the user should set “Safe Mode” to None. In this case, only SSID and IP should be configured. Below is an example.

Below is an example of self-signed certificate and keys.

- ca.crt is CA Certificate
- client.key is Private Key
- client.crt is Client Certificate
- The password set in step 6 is Private Key Password

Openssl command example:

```
openssl genrsa -des3 -out ca.key 2048
openssl req -new -x509 -key ca.key -out ca.crt -days 3650
openssl genrsa -des3 -out server.key 2048
openssl req -new -key server.key -out server.csr
openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out server.crt
openssl genrsa -des3 -out client.key 2048
openssl req -new -key client.key -out client.csr
openssl x509 -req -days 3650 -in client.csr -CA ca.crt -CAkey ca.key -
CAcreateserial -out client.crt
```

ca.crt example:

```
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgIJANeiouNsNcHlMA0GCSqGSIb3DQEBCwUAMFExCzAJBgNV
BAYTAlhYMRUwEwYDVQQHDAxEZWZhdWx0IENpdHkxHDAaBgNVBAoME0Rl ZmF1bHQg
Q29tcGFueSBMdGQxDTALBgNVBAMMBHRlc3QwHhcNMTgxMDMwMTA0NjQ5WhcNMjgx
MDI3MTA0NjQ5WjBRMQswCQYDVQQGEwJYWDEVMBMGA1UEBwwMRGVmYXVsdCBDaXR5
MRwwGgYDVQQKDBNEZWZhdWx0IENvbXBhbnkgTHRkMQ0wCwYDVQQDDARO ZXNOMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAymWBDuwiacayEuFG1BtvJF3Z
qu0OzyOExNh2cyuNx+rxgcyOCECkvDqXAvOOIpV5+C7SO39j5i3y6lIv6q8HbtQd
J04Fxjb//RJsPDG9GtK+RnC/p81Xi2o3AUJ6K8eLPhwsikt1nQaXCetT03JZKMQm
3cSqu2nyjJWowpHTr7cVTk8S6mZJBiLMPX6YOCTae1cR98JB1WfquRe9e/XJQAOw
/iq/51LAtHmee+x8eaai8/516bHsuVppYYIhqg4YNATeqsGTOB1QNrwjXekPx4KY
X3YmAP9EXBqApKts4ACIGcPLig81vKgd6hChTc6eK2yXW0dTuOMtkwTP+KOGiwID
AQABo1AwTjAdBgNVHQ4EFgQUXHdieYTw3ZOWAGLJDRRF6SOFIpswHwYDVR0jBBgw
FoAUXHdieYTw3ZOWAGLJDRRF6SOFIpswDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAs3r/C51AJcpUxPvUT4XSVycMNH79gSYwbLsoBRC0r7YK04enIZ7r
fi6IOD13R6Qbp0ergt80QrBmGLI1nCPyqft0pUfCPaZEGrQhCo58r8NSQyCnSm67
mqzBrs3JI1vZixi/0rU1vaq51FaJq6HaKiN0gJDuJPC1XX5Fern+/cGsBpFCzfG9
c/ouim3PB03M6UG+FBSX9UDpf/pTRfWnRzgmbITH5nMv/tXHKoNCQcCRYqkSgQ6L
kmncU8ajvWV0kJdztrtdsxHatcx1LaD79jd7hpETMjo0dpYuBRz7zs2K5SELw9QU
1g1YyMALL8wZCU2CBNbSCyzBL4DJrMug3g==
   -----END CERTIFICATE-----
```

client.key example:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-CBC,5F85A1BB8701F03D
```

```
mvWLF1iRfec8MCstf2Yceswff89kQMP2DtTG831AG3kJYWwDYUuK1vKmO5S44IAp
zbZuDZ1NUIc7dVoRNWj8qGhh7wJpkQVAfbFE1GmDQzwIaU+TKQ1E7rEwU5/cZAJH
DzLSV1Hz8jDSjwl218LuOpCb31KDyVsdKFsRzM+Dyx8D+Jby3xtjA2QI4xx4bJha
SZnJOGA8AhiwSDGseTpPWFtGRuDwzVmzaYNBomCuiEbqAmaozxcRVvNH5HVchskS
XSs05hkZOsm9I3nVf2jyb2mdL1fXA1O146OgjvGu4sZ1+342iT9mw84h03kDEDdP
sMHcrTMYidSO9CMCi6nZ2R7Z+zpXd0xwzQd8m0JuCpLwlRBYSk4ZJ6rq9Y6s7TJg
waronF6sC15tmVGSORZAzdc544BI7mhBd3yLSRcwOnfZmnRRM5g/nS2m3vVBs5d4
rmG3YII9J+5erOuZw19GSkljvAzqhL4N+axCggqjDtTLtS6avd1wlyMgqUuchz/k
O08TvMiHnwEnNkIBSd1LOSAnWojr9P2XBYdfx66r2XDdN7PtAc0tA5gT/kawtLd7
caFLOULFuh46gIzUcji6pD+PiKWINEP98KTKPYtLwG7/O4YHHcP34lyJGQOCU6NU
9AmO1T5lvvfMxTmMzsePTkZARbQsAS6uqzpoTk10BuRAOz0hQ+5Vc+7G8IZ3uuOO
HUOAlfV8/e8pRxTzWpodhOcyh36fqPBAPcqeXg1RhOu0yApLh+SwYu2a1g1NMu+i
IAwanpQE9LYx8/e66ML6+Y4hyrgI/mwcCv5yYfUevBZbj1rP5f5qrddqZXm6qFv8
JFltcXtYy2GTTATC/TV1j4wnU1zSiPO5Z/4UZtK+eaEQQwXXzO1SW/3HHrg6Uexj
krfZF/sJ41GUyejLEgxomOOnbjctwqzMNFxv5I/4XI9vCIBW/tglqV7CZGDoi6ui
jg9Sd191CQMtUn11+PO/SlKA21Q7lbga+ggsdEESpUSlswvvJlk+flqHnzv5H4O6
z1DXH8FLRtCK5GEo5bPp10+bYU1PgZQL0jRf2/h6UzVBz3zm/vSmOl6Uec+Cj8qb
bg2lrVXthrDaOwU8FuJVbS33HHc5e0eNOAkHOyaxorDeS+ha6ranLAtS9MC+PgqG
SUOCBRYQGO5DXaTHic/724cLWjoDeJ/u+KUuPfaJkaU3bEZq+5+Gso8UVt8hSlnx
ppy4FvSSB8Tsg095P8lmZBSp2qt9+sy0sBxiHW/7XayP66gQAUFuBESkioCamlEz
VdAOiC1KrDQunR3z3/nNFtHMehFurQkyYgICq5EuqUhF3i6ILDyTSLHiEtf19JeG
ZxtRb/Vk2JUOHZ/UmGNWVI5Z9i953ltTfRrnH7+fGQVpIMhIZug+OGmyJi3flLQe
Q/vpUpMtPFdFSaz+eIbOOtI8XJoMuWwKDMhJdNHfqkOls3BZZUvoQUC1umwAq9ov
CmeYXxJT3HXBRzGFL9UjJ47jM8JDEtOOqDpkXJLGhiAh8Ty8bHQKEfWgsYdkvxsY
RJ2igsijvXMJu63etx/zTCJq4fcK/Ev5XOoPQdx5mLM/PWdJYtyj0A==
    -----END RSA PRIVATE KEY-----
```

client.crt example:

```
-----BEGIN CERTIFICATE-----
MIIDHDCCAgQCCQCMtSyQfdk92zANBgkqhkiG9w0BAQsFADBRMQswCQYDVQQGEwJY
WDEVMBMGA1UEBwwMRGVmYXVsdCBDaXR5MRwwGgYDVQQKDBNEZWZhdWx0IENvbXBh
bnkgTHRkMQ0wCwYDVQQDDAROZXNOMB4XDTE4MTEwMTAyMTMyOVoXDTI4MTAyOTAy
MTMyOVowTzELMAkGA1UEBhMCWFgxFTATBgNVBAcMDERlZmF1bHQgQ2l0eTEcMBoG
A1UECgwTRGVmYXVsdCBDb21wYW55IEx0ZDELMAkGA1UEAwwCdHQwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDDPrVoQCFUXBgA807fkgrkYdF+ozeO3CGI
GJRxa3YsGVZ9TIcRe9L/oOkiOyomQbqRRGFcbULqmPyBAymtZoAkNOGGXP7nrco4
NOQA7dVPC6ueZi+gYWCuMOkKO8D8JVZnMZfctbymYLWNvIN8+TqAGV49+rSPU1wd
56eh26YJ4Wnq5gY1jPG9I233Tyq05Br6hFv79ZIOFSsqwK3rGd2447bh3yMb4ah2
qm+He78hK2XwV6X2M7UyUUTYwIo4Ohcc4k7edTK/thxqyUK3aCHQEUKK8ruF/BI7
dufVtHOk0srSLNJ3svsRh6VK5Rwi1CezABkknBQjcpWChcJcG81VAgMBAAEwDQYJ
KoZIhvcNAQELBQADggEBAAfAnL6vIYh/IjlbdUMMSsdvWiAYIiSyWrLyz3ZeGs4u
1UaagR4evVNPTq7ToAbvtaDd0PTPoJkfVxVN65Rc/TtlwnkGh+GmQhk5twjEMUrs
7vDBkdYDOv3ZqHSpeFCDTwn1rO6HpV2h+it7EqhVlpyYow2QA1VMVgNJr7fBWMsY
AJsIepors/nGjBm57cQKMcmU8T6O5mYFGpaVlpM/q+1rm/zl7pmo4ghit1fiVlRi
HS0YB9ZbjVdwMbazf4m07h8x5vE8CzId9bD6ByWebANcOoy8z6fTSLUaifLU11D6
s92moajRMu6D15rnPvHFSwsofCjd4b7bZ2AUpGJeqTo=
    -----END CERTIFICATE-----
```

Appendix D: EU WEEE Directive

Waste Electrical and Electronic Equipment (WEEE) symbol on the Cassia Bluetooth gateway and/or accompanying documents means that used electrical and electronic equipment (WEEE) should not be mixed with general household waste. Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling.

If you wish to discard electrical and electronic equipment (EEE) in the European Union, please contact your dealer or supplier for further information. Penalties may be applicable for incorrect disposal of this waste, in accordance with your national legislation.

Appendix E: Configurable MQTT TLS Certificates for Gateway-AC Communication

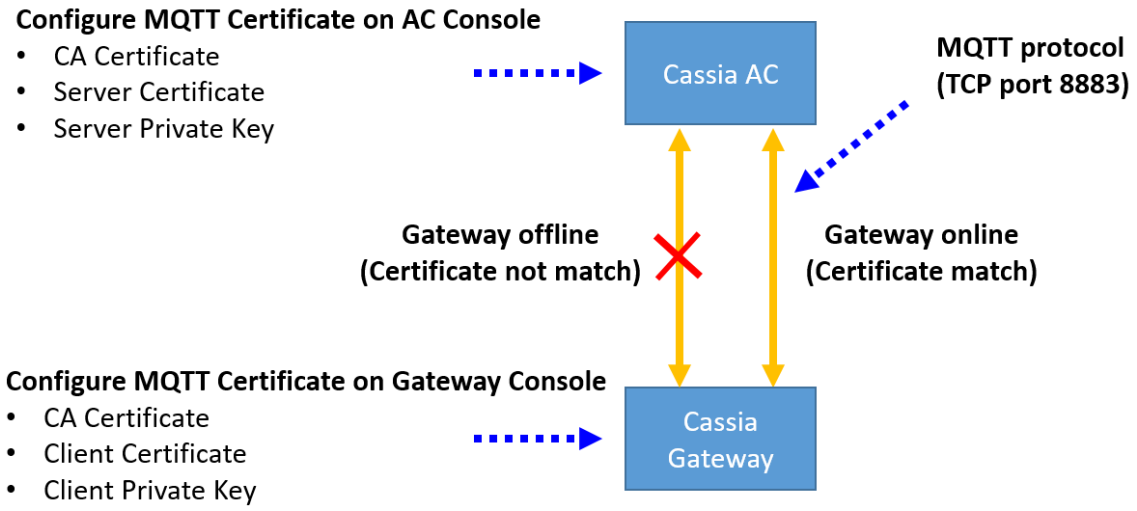
1. Overview

To further improve the communication security between Cassia IoT Access Controller (AC) and Cassia Bluetooth gateway, Cassia supports configurable MQTT TLS certificates for gateway and AC communication from firmware 2.0.

The user can generate their MQTT certificate and load it in AC and gateway console. If the loaded certificate doesn't match or expired, the gateway can't connect to the AC. The certificate can be a CA certificate or a self-signed certificate. Cassia gateway always uses the secured MQTT to communicate with AC, no matter if the default or custom certificate is used.

NOTE

- Only PEM certificate file format is supported
- Don't support private keys with passphrase protected
- Don't support certificate revoke



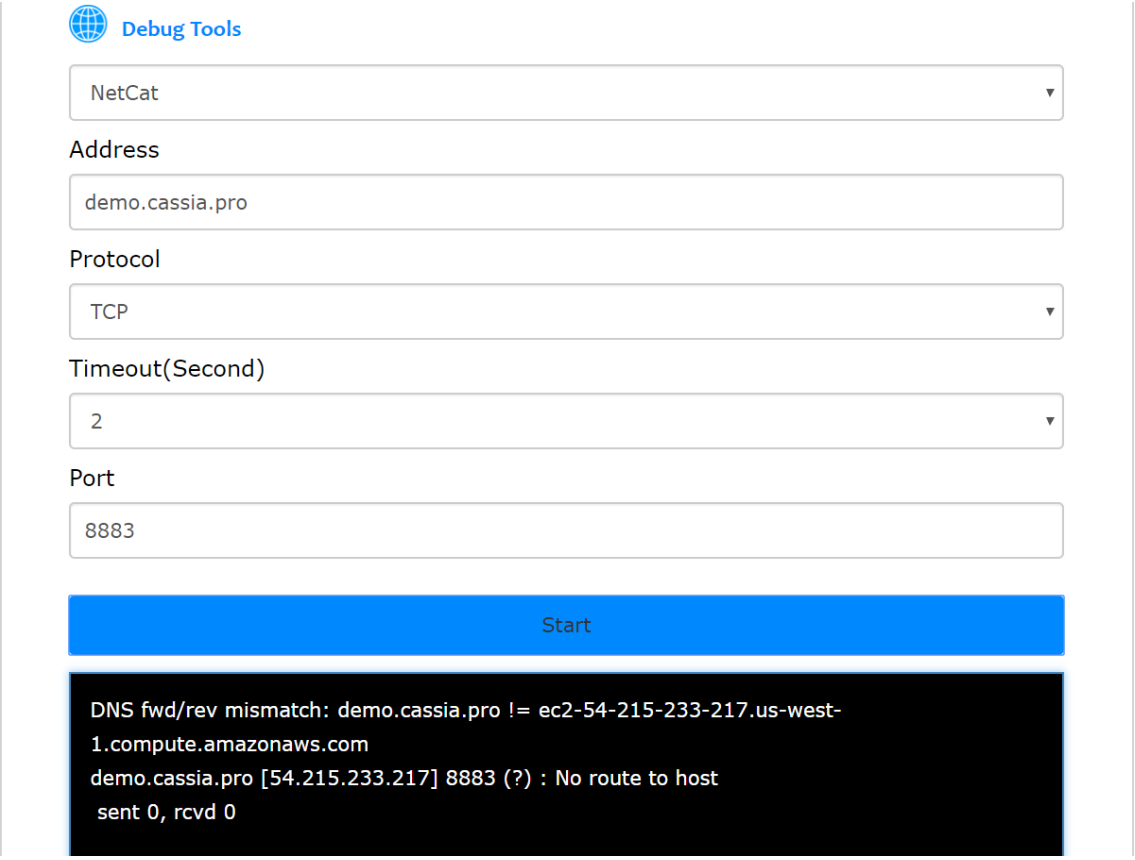
2. AC Configuration

2.1. Open TCP port 8883 on AC Host

TCP port 8883 is used by MQTT protocol between Cassia AC and Cassia Bluetooth gateway.

The user can use NetCat to check if TCP port 8883 is enabled on AC and reachable from the gateway. Please login gateway's local console, select Other page, and run NetCat like below.

TCP port 8883 has been opened on VMware AC. If the user wants to open TCP port 8883 for Cassia-hosted AC, please contact Cassia support.

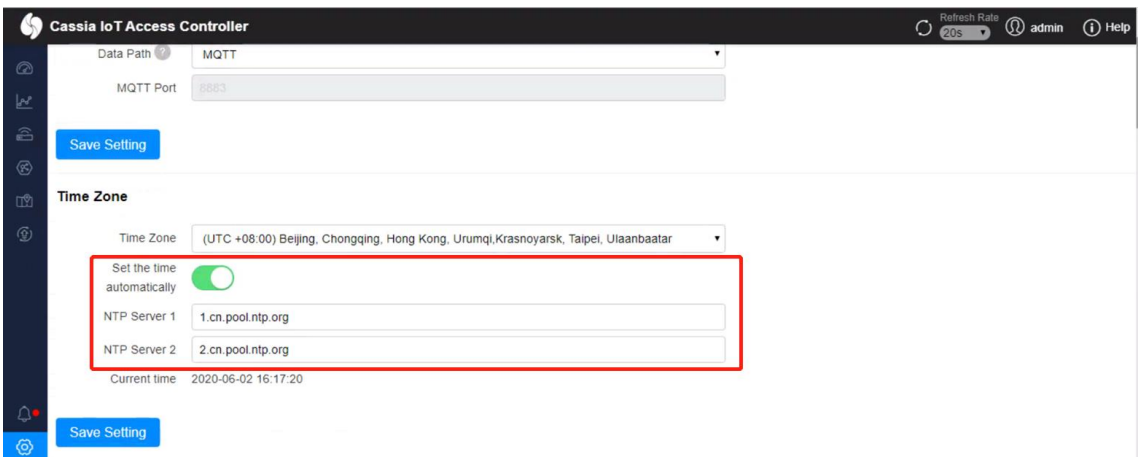


2.3. Configure AC Time

Please skip this step if the AC is running on the cloud, e.g. Azure or AWS because the time of the host server is always correct.

If the AC is not running on the cloud, it is recommended to switch on “Set the time automatically” and set your own NTP time servers on the AC setting page.

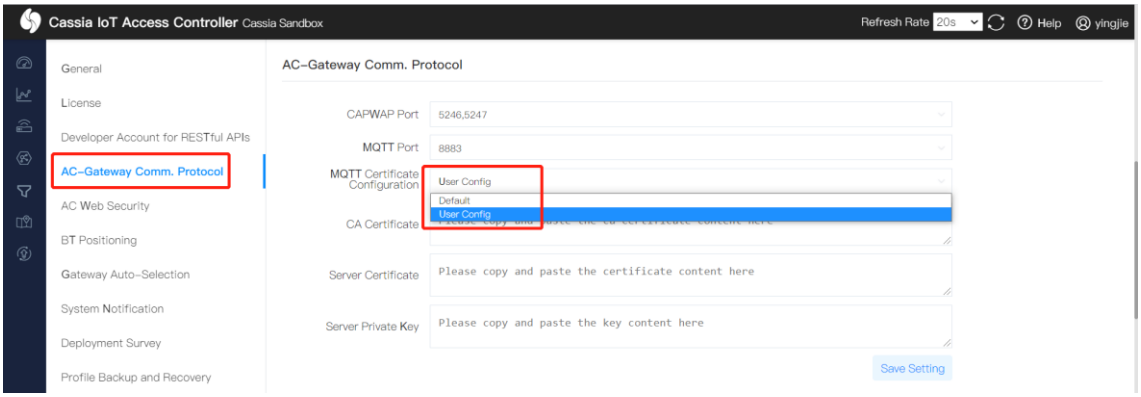
The AC time will be used for certificate validation. If the AC time is not configured correctly, the gateway can’t connect to the AC.



2.4. Configure MQTT Certificate

On the AC Settings page, please change MQTT Certificate Configuration from Default to User Config. Then, please fill in the CA Certificate, Server Certificate, and Server Private Key.

Default means using the default certificate provided by Cassia. The gateway and AC communication is still protected.

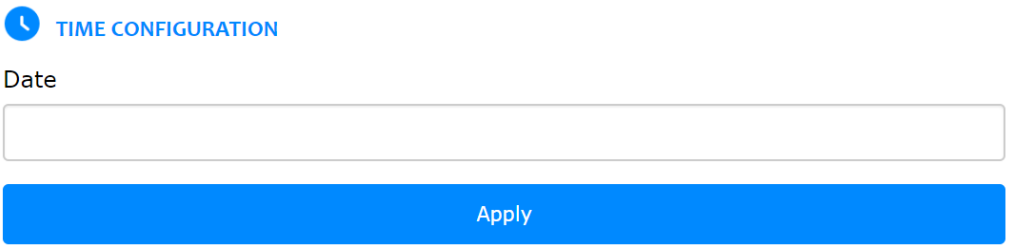


3. Gateway Configuration

3.1. Configure Gateway Date

Please configure the correct local date in the gateway's local console Other tab. After connected to AC, the gateway will get the correct time from AC automatically.

The local date will be used for certificate validation. If the date is not configured correctly, the gateway can't connect to the AC. The default gateway local time is 1970-01-02, 00:00:00.



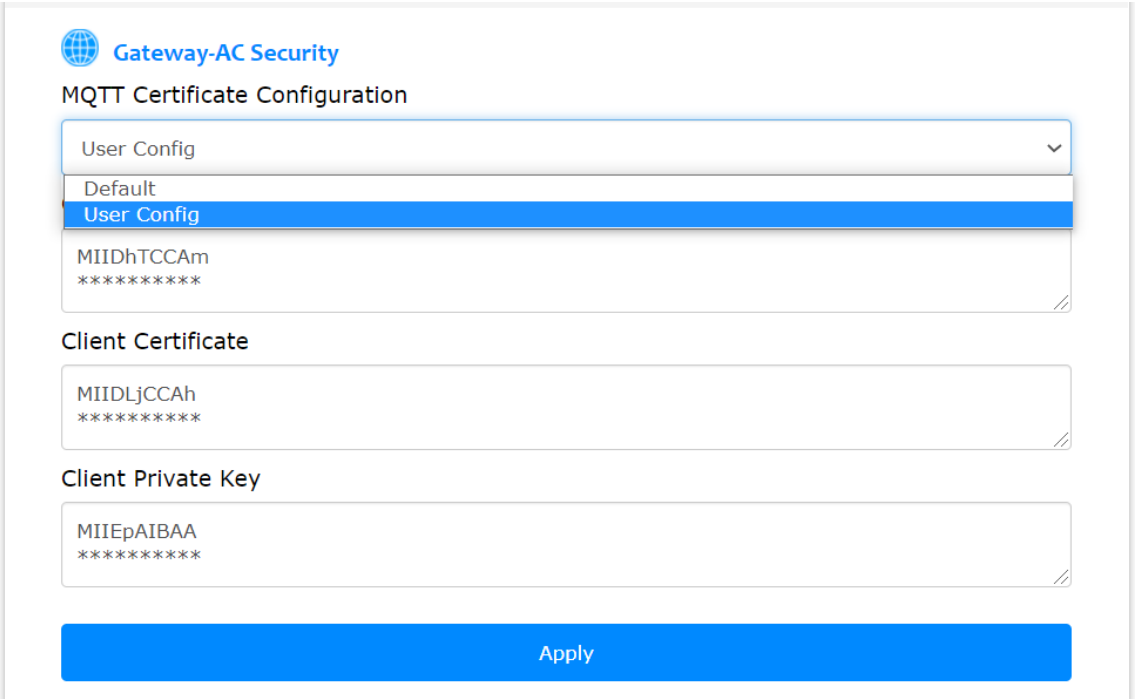
3.2. Configure MQTT Certificate

Please fill in MQTT certificates in the gateway Other tab. Please change Certificate Configuration to User Config, and then fill in the CA Certificate, Client Certificate, and Client Private Key.

NOTE

- The AC and gateways should use the same CA certificate.
- Now, we only support bi-directional authentication. It means the gateway will authenticate AC and AC will authenticate gateway too. So, both CA certificate, client

certificate, and client private key should be provided on the gateway side.



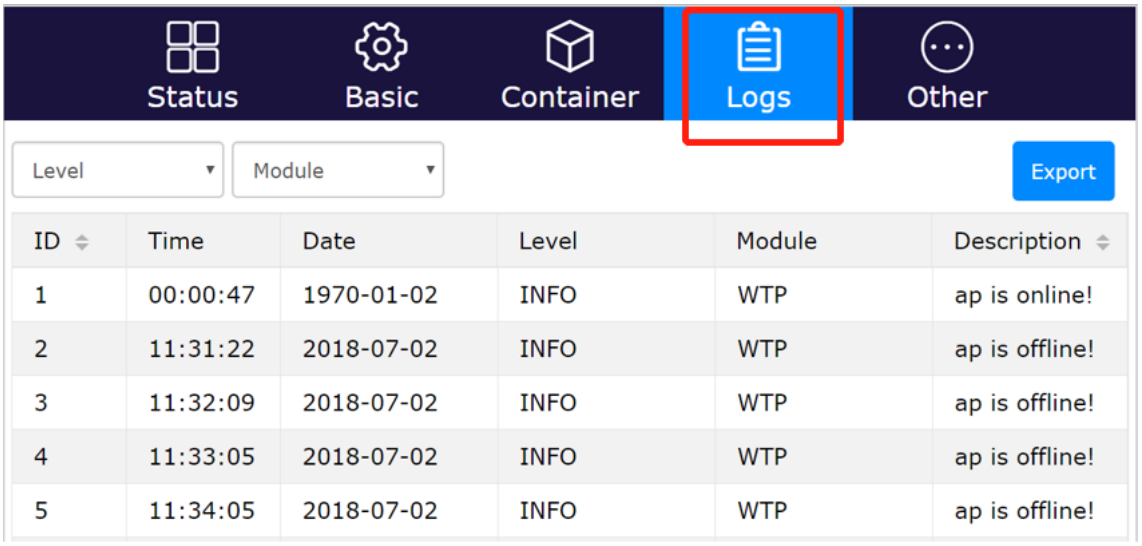
Now, the gateway will connect to the AC automatically.

4. Trouble Shooting and Tips

The AC and gateway console will check the integrity & validity of the certificate and private key. Please check chapter E.1 for the format requirement. If the local date and time are not configured correctly (see chapter E.2.3 and E.3.1), the validity check will fail too.

If the gateway can't connect to the AC, please double-check if you load the correct certificate and private key. The user can set the Certificate Configuration back to Default to exclude any other issues, e.g. transport issue.

The user can find TLS error logs in the gateway console Log tab.



5. Certificate and Private Key Examples

Below is an example of self-signed certificate and keys.

- ca.crt is CA certificate
- server.crt is the server certificate
- server.key is server private key
- client.crt is the client certificate
- client.key is client private key
- Don't support private key with passphrase protected, e.g. don't add "-des3" in step 3 and step 6

Openssl command example:

```
openssl genrsa -des3 -out ca.key 2048
openssl req -new -x509 -key ca.key -out ca.crt -days 3650 // generate CA certificate
openssl genrsa -out server.key 2048        // generate server private key
openssl req -new -key server.key -out server.csr
openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -
out server.crt        // generate server certificate
openssl genrsa -out client.key 2048        // generate client private key
openssl req -new -key client.key -out client.csr
openssl x509 -req -days 3650 -in client.csr -CA ca.crt -CAkey ca.key -CAcreateserial -
out client.crt        // generate client certificate
```

ca.crt example:

```
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIJALSD+kQkX3FuMA0GCSqGSIb3DQEBCwUAMFIxCzAJBgNV
BAYTAkFVMRMwEQYDVQQIDApTb211LVN0YXR1MSEwHwYDVQQKDBhJbnRlcm5ldCBX
aWRnaXRzIFB0eSBMdGQxCzAJBgNVBAMMAmRkMB4XDTE5MDUwNTAzMDk0N1oXDTIw
MDUwNDAzMDk0N1owUjELMAkGA1UEBhMCQVUxEzARBgNVBAgMC1NvbWUtU3RhdGUx
```

```
ITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IExOZDELMAkGA1UEAwwCZGQw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDP+fPO92U1IHrIBvXHM5kP
wB25McMpRu3CUz9SnbC/LNi8uaSZI0glevlnsU/mckVeKDizWEX6ZrtPfokN8yH2
JmwaG16AAo6jmtmam9VjVWjZeXB7bGxIi9/obl/viD9efrLamNbpldBeZEFB0ia0
p6xcCh+0Vo+268xbWdiHGnwFaFcUMhaQ0hIuHdujWguSzMLYXqATGjhZSvdkSCe+
ieUcc+y4SZTP1H+xD78MwyBxGSxMxSo6ANRjcQNIJedn2eF36dcLbVSz0EEyR2Xs
EQYBVkAyv4mFR2uFOn/j+3LR+uqEI5vAGkKw5p15D9d9em2Ym/O5IhosO0xTzBnF
AgMBAAGjUDBOMB0GA1UdDgQWBBT5SOcADFP2P/DhdcGZRD7H96BtuTAfBgNVHSME
GDAWgBT5SOcADFP2P/DhdcGZRD7H96BtuTAMBgNVHRMEBTADAQH/MA0GCSqGSIb3
DQEBCwUAA4IBAQAfnXfC/1MOROwv0KL8uyROtY2V1hvTjIoc1D/5zHGY7IOgLCyz
3ZRyvb3VGvVR+MPi8PHkp4X1mud/n8uVRDF+qTYvQnhxS2HF7ABxwC4Fz0JmIYAn
KYcLBgB4sUXHa8kqZiPcW8YOGnXuT1kiYTGodfNOK6T3pXPy08Inh3IcySqwgjmh
cGppJQC86LugeLFN81B/EzQSMPpG1fyxHwlyqmsm7LNryYqr5QoS2CUc6qlc3Hc0
pu+Q15kCapJ7TS71V5hOqEtHD7XuWfhYbltAQpexw5M6udECVa3TEUWBmq86Oq6/
n0aFHK5hb2J2NhpuPAKQIUbBn7UXTd3pw1RP
    -----END CERTIFICATE-----
```

client.key example:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvlwkLoVBJ3a/HPQ+7mcM4YuDls6txnmmV6WMhZ7BGPw+6P3Z
XzzDHRPkx8OAUSfzxUThmegNt1t6fCorESGvc9di0aFWvJB9xVQQdiocPIuZ+8Sb
Gj9m2dsmhCgn++7kea/Eusat0kVYUVnm8cMaN4/2xvrli1n4+bKZ+hGb7gV6IOuJ
XDelfRRFFANXKSBBgLSqkLxXWBT4I7DC6Cjdp9jidAmRqmuHG3923xTzkhVbBtiG
bq04SB3kfb6L139nB1O2z0V/+oHOG+CkuJQ94ZF/EmfLzipv6jSY/fCMSKzcGCQZ
3j/gbEsQYAG6v/PZ1S5XE+A1nKQ87qzMrsG2HwIDAQABAoIBACWVNYOFxY5QEH1b
74zMBawGCm3c0kxMOj41rh+3bzJKovUHIUJ/UZpNEi8qdwwO0j8RUWU8fnDD+9PF
04jnWKeLT7RJoUFLWbl61mEuATMm8LjXYTP2boz2io0vDG3eBXfM7w9dKHZKQJyX
H1R/C48KulMgt+8iTVinHWVU0q9UR9+f8PTMxUThkVHh+F+BoMBhcKpXAJZruBWc
oXyBlTF5T4Lt7neszHVkY6qx7E7yxVC7XY82zBExJPIu8/AzELONHT9F0DhioBJs
iBPu18HK6fdLXPZDMhZX3CB0cvYSwRni5cCVLpqIcQJ5oJ6F+ZRu2xB2rPJlHBAw
I/iDJsECgYEA9IUaY7elUliz9GdrmHynh4po70AZEo0viiaywwlTyEsz2ho20jDq
Svm03aemUod8sDdDwp/ajmcL3thhC3thFCVB1ZbSmq13DD269SDUK+fnr4roiv56
BVZnSdASa8rZim3qpDin7NblGVpEAiRax7Vmuy0Bi6bbhBxmF9/vL/8CgYEAx0wW
JWkaU5WR/d1MTIsnRA/u/3CJukkkbOnOZP1W9YbG7MQAWEh40tToyhqdAWC4MxS8
jAq5q10AGA83v7qIeRiFr6u8VBL02yUaxjzRvpaL10frv/VCDEA7B0YSxFd8y4xt
lK4kXOzjJ5OqyO11BS00iUIGbIacN1Jcd4AneeECgYAL9TpuJ/wAw+/BAxHC+k2j
FkS9dpADVMdP5UaWvV8ci3j0sJV/v/6lPgL3WAyNOq0BXSKGMRUaI7Xz5vcP/a+o
sY2/qUmRYOxSf+5VsI5Pu16cOhnXOkyzWB9i/7b26Ius9mUkNNUZgwTfMYfj5u09
mQR2IORTdQyFMHJZtozW9wKBgDO5YpIJCiUhT4eUlMXU47b9b6jqG0S20PZXZBK+
x7vnY991KyW+gWUujtBNQexmnsfbHOg3rGJ2O50C7hQbpGnRXHjwWGt1lAkAQ0ep
50HQrrCL4Pqr+51UWj2UCTDeB+yIILSS0aswa/AMmimVv2Y9ikIJWcN22DpfbNIy
94vhAoGAHNA6PAhP72+ze83Jz8ihEvpfIPJ1ekTpAsoE2EvfCtzMp+qtGV32wG3Q
IYNtsvn3/fBQGAMeDBCDjaeFH4ZRY42A+G6RURftDiOzuaCicH+d0IHez2HqY+OO
wC/sPSzYUeL9EST+WsehiUzZ2SSeIZa9qWjoCRdUECsxI9ifQBk=
    -----END RSA PRIVATE KEY-----
```

client.crt example:

```
-----BEGIN CERTIFICATE-----
MIIDKzCCAhMCCQDgCfVlo1FF7TANBgkqhkiG9w0BAQsFADBSMQswCQYDVQQGEwJB
VTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ210
cyBQdHkgTHRkMQswCQYDVQQDDAJkZDAeFw0xOTA1MDUwNzM3NDNaFw0yMDA1MDQw
NzM3NDNaMF0xCzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb211LVN0YXR1MSEwHwYD
VQQKDBhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxFjAUBgNVBAMMDTE5Mi4xNjgu
MC4yNDUwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+XCQuhUEndr8c
9D7uZwzhi4OWzq3GeaZXpYyFnsEY/D7o/dlfPMMdE+THw4BRJ/PFROGZ6A23W3p8
KisRIa9z12LRoVa8kH3FVBB2Khw8i5n7xJsaP2bZ2yaEKCf77uR5r8S6xq3SRVhR
Webxwxo3j/bG+uWLWfj5spn6EZvuBXog64lcN6V9FEUUA1cpIEGAtKqQvFdYFPgj
sMLoKN2n2OJOCZGqa4cbf3bfFPOSFVsG2IZurThIHeR9vovXf2cHU7bPRX/6gfQb
4KS41D3hkX8SZ8vOKm/qNJj98IxIrNwYJBneP+BsSxBgAbq/89nVL1cT4DWcpDzu
rMyuwbYfAgMBAAEwDQYJKoZIhvcNAQELBQADggEBACc9mAkv9ErVQO7v7JrxweoJ
XnYcq4jlHIo9S7x5flTou2C4GVp1231jVRjzxJs3yQOo+Xj8WsePHLpITNZRmYOS
SnAR/AhA3tUejHbfJsDKvsjHPBdG83hJ9MhQ1friyHiWVrMxVoPrPpvynG7mKN/i
FSQlxh9bTwHtTWhBJ5X1bqOnJaz69qaumGvSIIey3IklLKJhs4LC5ADn4HHa2Xfs
pRXC69CfPrYg/grTUPAY3uV/tPdTUDwCwxnvchR4bLgP4gUW6PSNvZ4MxRBx+ulx
f9Z4+5j5cnmDhafUdBtE4Vs809VlfK5hgwvIy2gzZjONBLQvFKqN5duwNvr08EM=
    -----END CERTIFICATE-----
```

Appendix F: Cassia Gateway LED Indicators

X2000 LED (Green)

LED	Function	Status	Description
PWR	Power status	Off	Power off
		Solid on	Power on
SYS	System status	Off	The system didn't start or cannot operate normally
		Solid on	The system is starting, going to reset, or cannot operate normally
		Slow blinking	The system is operating normally
ETH	Ethernet status	Off	No Ethernet link
		On	Ethernet link present
		Blinking	Sending or receiving data
WIFI	Wi-Fi status	Off	Wi-Fi didn't start or is in disable mode
		On	Wi-Fi is operating normally in hotspot or client mode
		Blinking	Sending or receiving data
BT0/1	Bluetooth status	Off	Bluetooth chip didn't start
		Solid on	Bluetooth chip is operating normally
		Fast blinking	Bluetooth connection has been setup
		Slow blinking	Bluetooth scan has been enabled
4G	Cellular modem status	Off	USB cellular modem is not connected to X2000 or cellular modem works abnormally
		Solid on	1: PPPoE cellular modem*: X2000 has connected to a cellular network 2: DHCP cellular modem*: X2000 has connected to the cellular modem. **NOTE**: Does not guarantee cellular network connectivity
		Blinking	1: PPPoE cellular modem*: X2000 is sending or receiving data to a cellular network 2: DHCP cellular modem*: X2000 is sending or receiving data to the cellular modem. **NOTE**: Does not guarantee cellular network connectivity
AC	AC online status	Off	X2000 is offline on AC
		Solid on	X2000 is online on AC

* HW models E3372s-153, E3372h-153 and E8372h are DHCP cellular modems. MultiTech models MTCM-LNA3-B03 and MTCM2-L4G1 are PPPoE cellular modems. If you want to know the type of other USB cellular modems, please contact your Cassia sales/support contact

E1000/S2000 LED (Green)

LED	Function	Status	Description
PWR	Power status	Off	Power off
		Solid on	Power on
SYS	System status	Off	The system didn't start or cannot operate normally
		Solid on	The system cannot operate normally
		Fast blinking	The system is starting or going to reset
		Slow blinking	The system is operating normally
ETH	Ethernet status	Off	No Ethernet link

		On	Ethernet link present
		Blinking	Sending or receiving data
WIFI	Wi-Fi status	Off	Wi-Fi didn't start or is in disable mode
		On	Wi-Fi is operating normally in hotspot or client mode
		Blinking	Sending or receiving data
BT1/2	Bluetooth status	Off	Bluetooth chip didn't start
		Solid on	Bluetooth chip is operating normally
		Fast blinking	Bluetooth connection has been setup
		Slow blinking	Bluetooth scan has been enabled

X1000 LED (Blue)

LED	**Function**	**Status**	**Description**
PWR	Power status	Off	Power off
		Solid on	Power on

X1000 LED may keep on blinking if the PoE power supply is not stable. Please try to replace the PoE injector.

Appendix G: China RoHS

本表格依据SJ/T 11364的规定编制
Below table is based on standard SJ/T 11364

产品中有害物质的名称和含量
Hazardous Substances Table

部件名称 (Parts)	有害物质 (Hazardous Substance)					
	铅(Pb)	汞(Hg)	镉(Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚(PBDE)
印刷电路板 (PCB)	×	O	O	O	O	O
外壳 (enclosure)	O	O	O	O	O	O
机械组件 (mechanical sub-assemblies)	O	O	O	O	O	O

o：表示该有害物质在该部件所有均质材料中的含量均在 GB/T 26572 规定的限量要求以下。

(Indicates that this hazardous substance contained in all homogeneous materials of this part is below the limit requirement in GB/T 26572)

×：表示该有害物质至少在该部件的某一均质材料中的含量超出 GB/T 26572 规定的限量要求。
(Indicates that this hazardous substance contained in at least one of the homogeneous materials of this part is above the limit requirement in GB/T 26572)

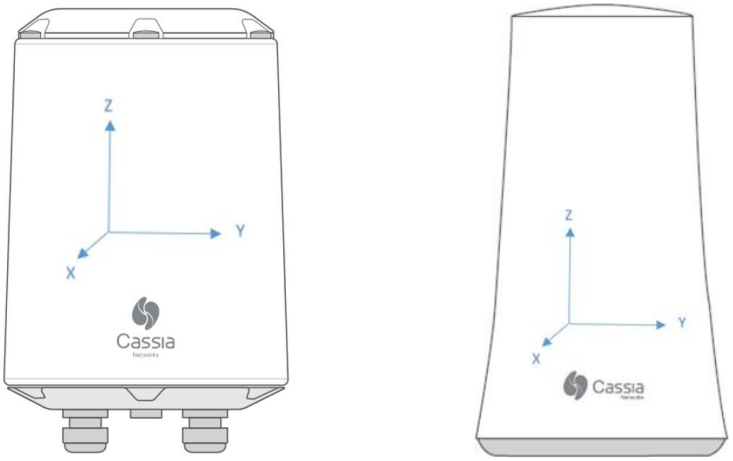
以销售日期为准，本表格显示这些有害物质可能在本公司产品的供应链上找到。
(Subject to the sales date, this table shows that these substances may be found in the supply chain of Cassia products)

除特别标注，根据 GB/T 26572 要求，此标志为针对所涉及产品的环保使用期限标志。
According to GB/T 26572-2011, The Environment-Friendly Use Period (EFUP) for all enclosed products and their parts are per the symbol shown here, unless otherwise marked.

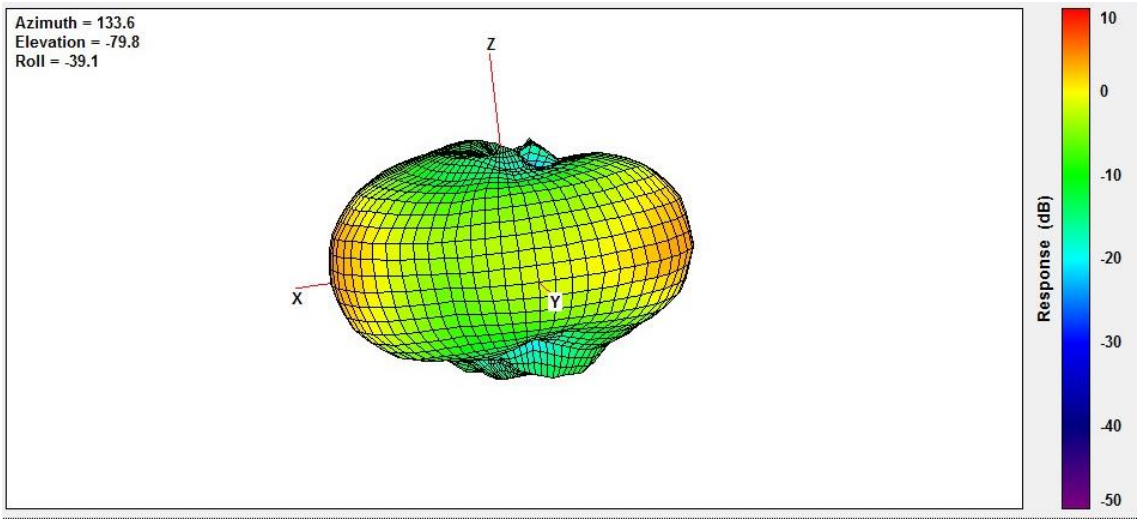
此环保使用期限只适用于产品在产品手册中所规定的条件下工作。
The Environment-Friendly Use Period is valid only when the product is operated under the conditions defined in the product manual.

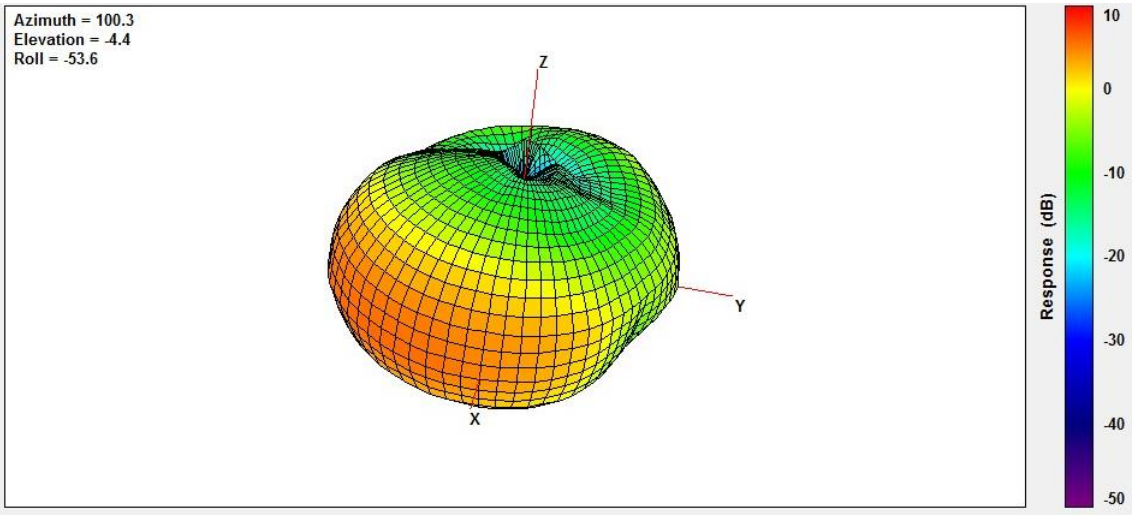
Appendix H: Antenna Radiation Graphs

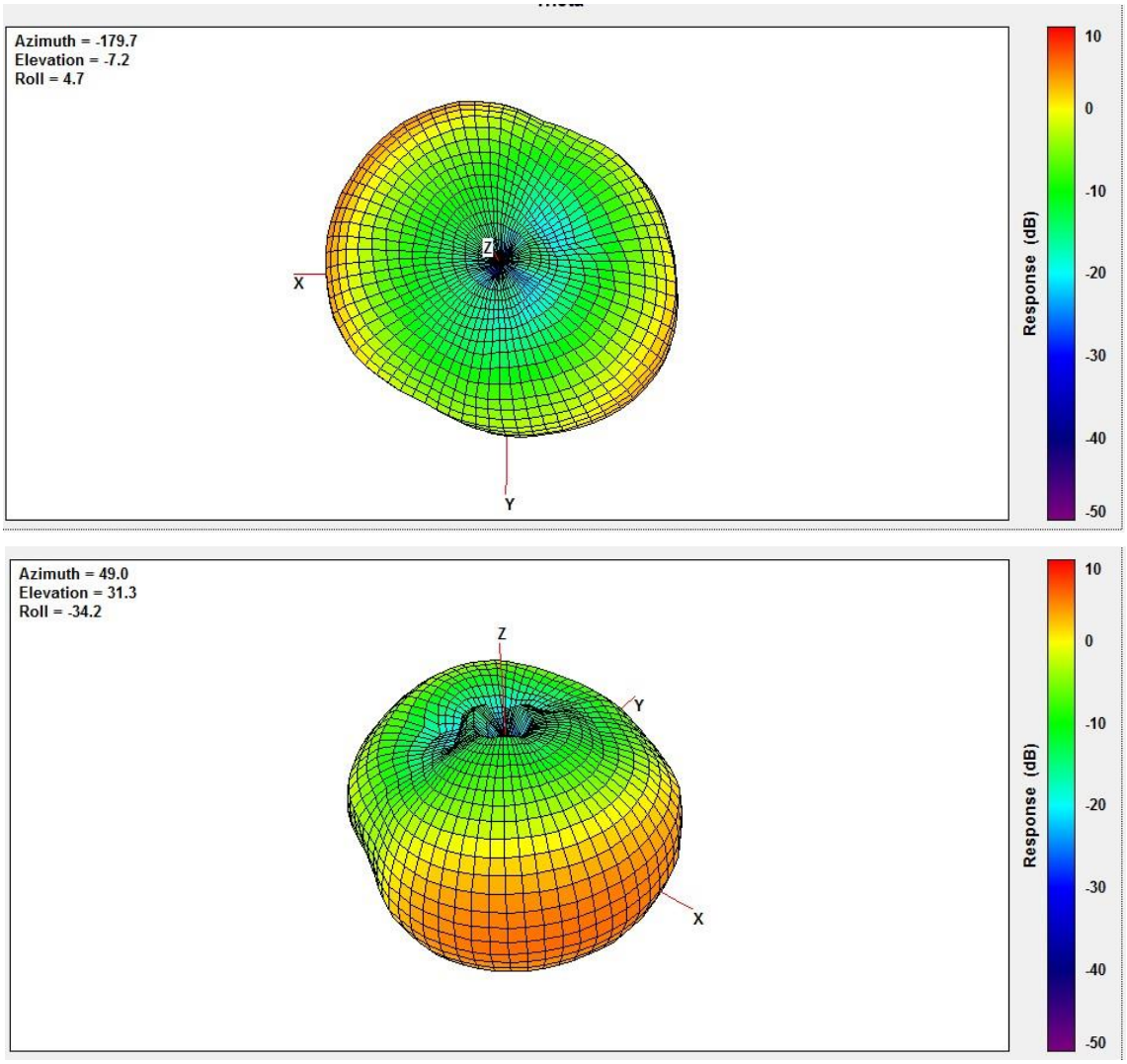
1. X2000 and X1000's Internal Bluetooth Antenna



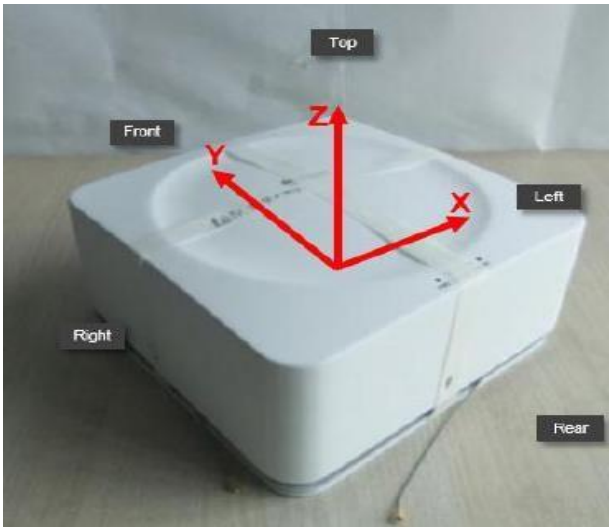
If you place your gateway as depicted in the image above, the images below show the Antenna Gain in 3-D.



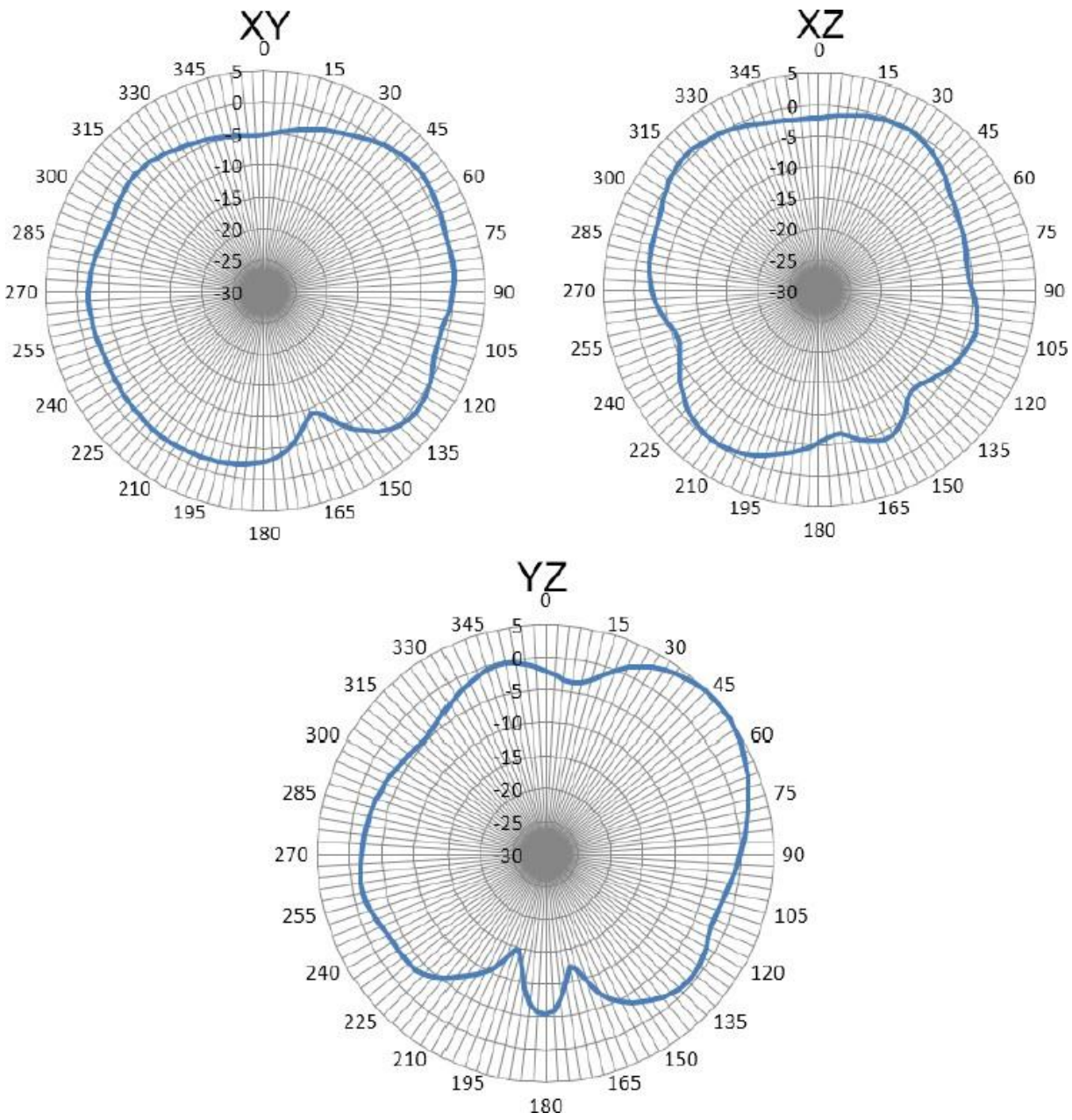




2. **E1000 and S2000's Internal Bluetooth Antenna**



If you place the E1000 and S2000 on a tabletop (shown above), the radiation pattern graph results are shown below.



Appendix I: Accessory Options

Please contact sales@cassianetworks.com for purchase inquiries.

1. Power Adapters and Power Cords

Model Number	Vendor	Description
PT-PSE104GO-30	Procet	PoE injector, input: 100-240 VAC, output IEEE802.3 af/at
AD2412N3L-VI	Artesyn	DC power adapter, input: 90-264 VAC, output 12VDC/24W
CXPST018	Procet	American standard power cord, for PoE injector and DC power adapter
CXPST019	Procet	European standard power cord, for PoE injector and DC power adapter

2. X2000's External Antennas

Antenna	Type	Gain (dBi)	Horizontal Beam Angle (°)	Vertical Beam Angle (°)	Connector
DB24-120V10A	Directional (not MIMO)	10	120	30	N Female
QB24V8A-F	Omni-directional	8	N/A	N/A	N Female
QB24V8A-M	Omni-directional	8	N/A	N/A	N Male

3. X2000's Radio Cables

Antenna	Length (m)	Connector
NJ-2	2	N Male - N Male
NJ-5	5	N Male - N Male
Customized	Customized	Customized

4. X2000's Optional Desktop Stand Kit

For more questions regarding Cassia products, please contact support@cassianetworks.com.