vaiotech

Kiwi Warmer

User Manual for
Kiwi Warmer Rowi
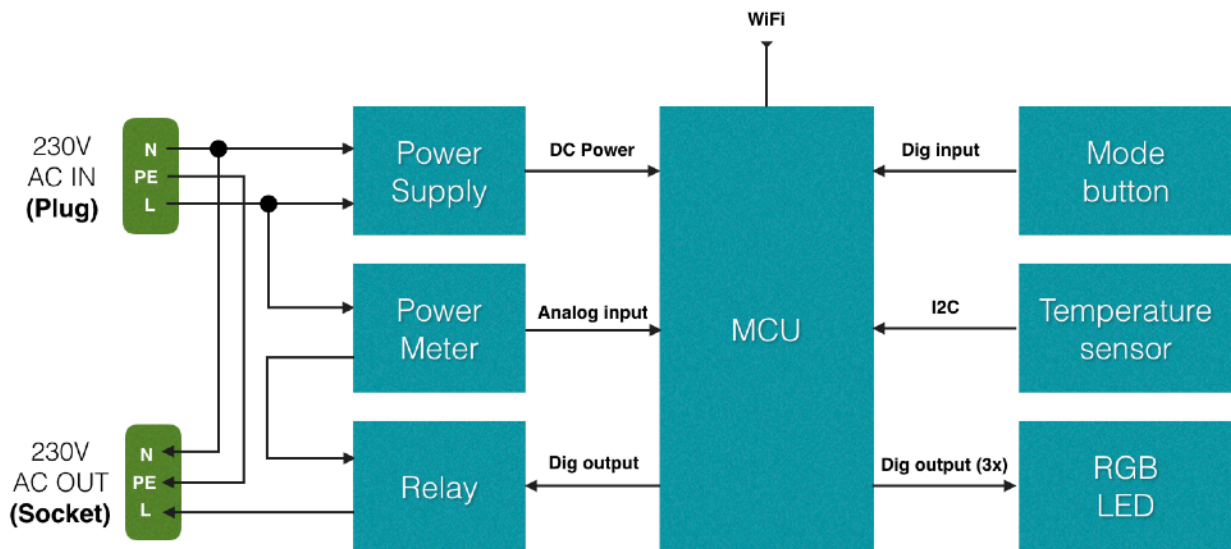
Rowi V2.0
Manual V2.1
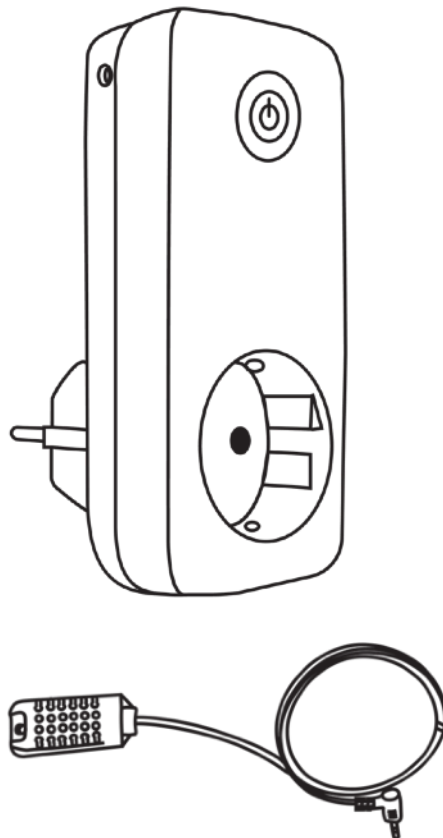
CONTENT

TECHNICAL SPECIFICATIONS

Block diagram

Characteristic	Value
Maximum Power Rating	10A/16A, 220-240V~, 50Hz
Temperature Sensor Range	-40 °C to 125 °C
Temperature Sensor Accuracy	±0.5 °C in the range between 0 and 45 °C
Humidity Sensor Range	0% to 100% RH
Humidity Sensor Accuracy	±3.0%RH at 50%RH
Energy Sensor Accuracy	±10mA according to Sensor Manufacturer
IP Class	IP20
WiFi Network	Wi-Fi: 2.4 GHz 802.11b/g/n
WiFi Authentication	WEP, WPA, WPA2
Mobile App	iOS and Android (only officially supported versions by Apple and Google)

COMMUNICATION PROTOCOLS

Kiwi Warmer Rowi supports two communication protocols: HTTP(S) and MQTT. The HTTP(S) protocol can be used to communicate with the Smart Plug within a local WiFi network using RESET API. MQTT is a state-of-the art communication protocol for IoT devices. Each Kiwi Warmer Rowi device publishes sensor data to an MQTT topic within an AWS-based cloud backend, from which it can be accessed via an MQTT client using MQTT subscribe mechanisms. The below diagrams describe the two different communication options.
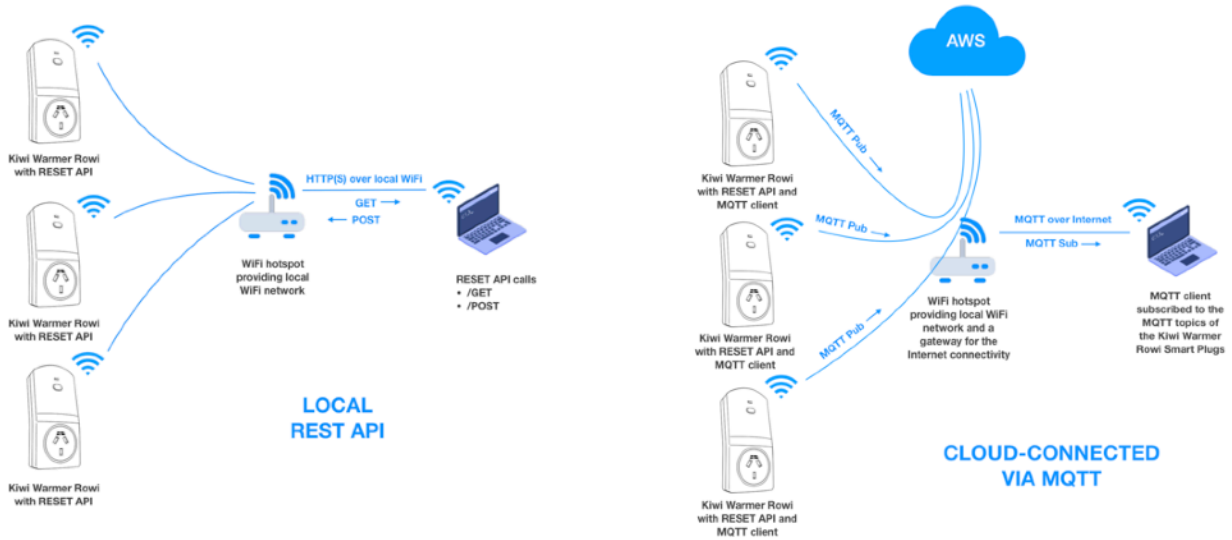
HTTPS-specific

Rowi devices are equipped with Vaiotech's SSL certificates. Compared with HTTP, HTTPS is a secure communication protocol. However, it consumes much more computational resources, which is reflected in slower response times when calling REST API commands. Also, due to high resource requirements, Rowi can accommodate only one HTTPS connection at a time. It is advisable to use HTTPS whenever possible. However, for applications that require higher performance regarding response times and that are running in isolated WiFi networks that are protected from information security threats through other means, HTTP protocol might be a better option.

Each Rowi device is pre-programmed with an SSL certificate signed by Vaiotech and associated with the following domain name: ***.kw.rowi.vaiotech.nz**. Vaiotech can also provide the CA and the client certificates in the .PEM or .DER format on request to install in client's environment and to integrate Rowi devices in the corporate networks. The certificates are valid for 12 months and can be updated using the build-in firmware upgrade feature of Rowi (OTAP - Over The Air Programming).

MQTT-specific

Rowi devices that are configured for MQTT, periodically submit device and sensor data to an AWS-hosted cloud server from which it can be accessed using an MQTT client, for instance MQTTX (https://mqttx.app). Since the communication between the cloud server and the client is encrypted, you will need a set of the following certificates that can be provided by Vaiotech on request: CA Certificate, Client Certificate and Client Key File.

The address of the MQTT URL is **a1n1imofwtibil-ats.iot.us-east-1.amazonaws.com** and the port is **8883.** Once connected, you will need to subscribe to an MQTT topic that is constructed according to the following format: **kw_family_rowi/pub/<SECRET4>/<MAC>/<SECRET3>/<SECRET5>/**

Secret #3 will be generated during setup procedure described in the chapter "DEVICE CONFIGURATION". Secrets #4 and #5 as well as the MQTT authentication certificates will be shared via email on request (to request, please send an email to support@kiwi-warmer.nz).

Below screenshot shows an example of a working MQTT Client configuration using MQTTX:

* Name	AWSIoT
* Client ID	mqttx_66b12ba2
* Host	mqtts:// a1n1imofwtibil-ats.iot.us-east-1.amazonaws.com
* Port	8883
Username	
Password	
SSL/TLS	● true ○ false
* Certificate	○ CA signed server ● Self signed
SSL Secure	🟢 ⓘ

Certificates

* CA File	Downloads/AmazonRootCA1.pem
Client Certificate File	Desktop/dc8d1e69e9-certificate.pem.crt
Client key file	/Desktop/dc8d1e69e9-certificate.private.crt

DEVICE STATES

Kiwi Warmer Rowi is equipped with an RGB LED that is used to indicate the device status. Rowi can operate in eight different modes that are explained below.
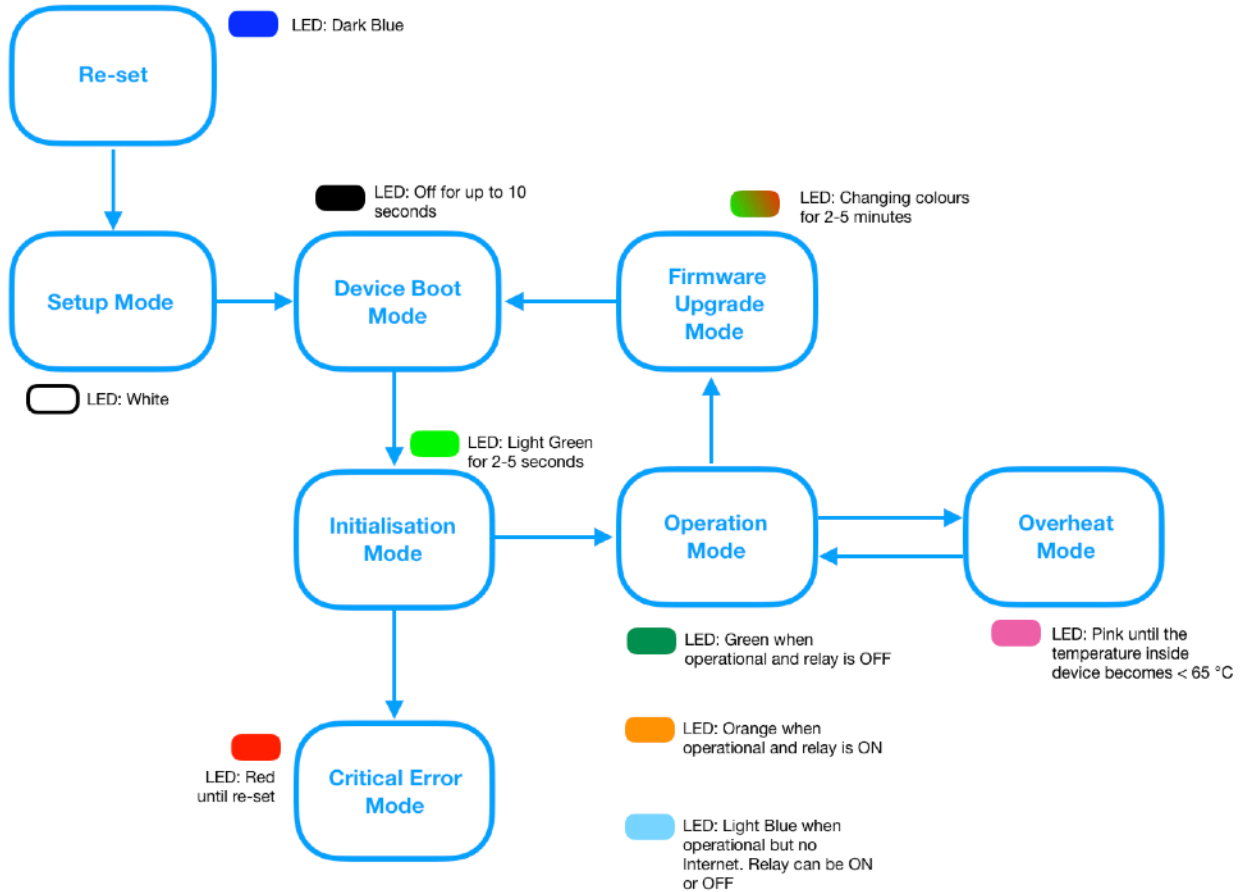
Please note that, that even though the device is in the Operation Mode and shows the correct LED status, the REST API may need up to 2 minutes to become fully accessible. Sending the /ping command via REST API after the device moves into the Operation Mode speeds up the process and makes the API accessible immediately.

Mode	Colour	Description
Re-set	Dark Blue	Factory mode. The device is not set up and is not operational. It cannot receive commands, but it is ready to be set up with the mobile app. To re-set the device: 1. Unplug Rowi 2. Long-press the MODE button on the front side of the device and while pressed plug-in again 3. Wait until the LED starts to glow Dark Blue and then release the MODE button
Setup	White	The device is in the setup mode. It is either already paired or is waiting to be paired with the mobile app. If the setup attempt was not successful, Rowi leaves this mode after 2 minutes and goes back to the previous mode.
Device Boot	LED is OFF	The mode Rowi is in while booting. This is the first mode after the device is powered on and when it is already set up. The Boot process can take up to 10 seconds.
Initialisation	Light Green	During the initialisation stage, the device checks internal settings, the integrity of the flash memory and if the internal temperature sensor is operating correctly. The Initialisation takes up to 5 seconds.
Operation	Dark Green Orange Light Blue	This is the main mode in which the device spends most of the time. Dark Green LED indicates that the device is operational but the relay is switched off. Orange means, the device is operational and the relay is switched on. Light Blue LED indicates that the device has no internet connectivity at the moment (this applies only to the devices that were configured for the Internet and/or MQTT connectivity).
Firmware Upgrade	Changing colours	Firmware upgrade initiated by the user. This process can take 2-5 minutes and is indicated by changing colours of the RGB LED.

DEVICE CONFIGURATION

Kiwi Warmer Rowi can be configured using a mobile app provided by Vaiotech. The mobile app is available for iOS and Android-based phones and the download and installation instructions will be provided via email after the shipment of the Rowi devices.

Step 1: Connect to 2.4 GHz WiFi network
The Rowi devices require a 2.4 GHz WiFi connection. Before starting the mobile app, make sure you've connected your mobile phone with a 2.4 GHz WiFi network, the same network your Rowi devices need to be connected with. Also, have your WiFi password ready as it will be required for the device configuration.

Step 2: Download the mobile app
Scan the QR code with the mobile phone and you should be automatically navigated to the Apple or Google Store where you can download the mobile app called "Kiwi Warmer Eco".

Step 3: Start the mobile app and initiate pairing
The mobile app requires Location Services to be able to be paired with the Rowi devices via WiFi. Please allow the mobile app using Location Services when asked upon the first start. After the mobile app has been started, you will be presented with general safety instructions for Kiwi Warmer Products, which need to be confirmed. After confirming the safety instructions, navigate to the Settings screen using the "Hamburger" icon located in the bottom right corner and select [Settings]. In the Settings screen, click on the button [Add New Appliance] and follow the the instructions of the Pairing Dialog.

Pairing dialog.
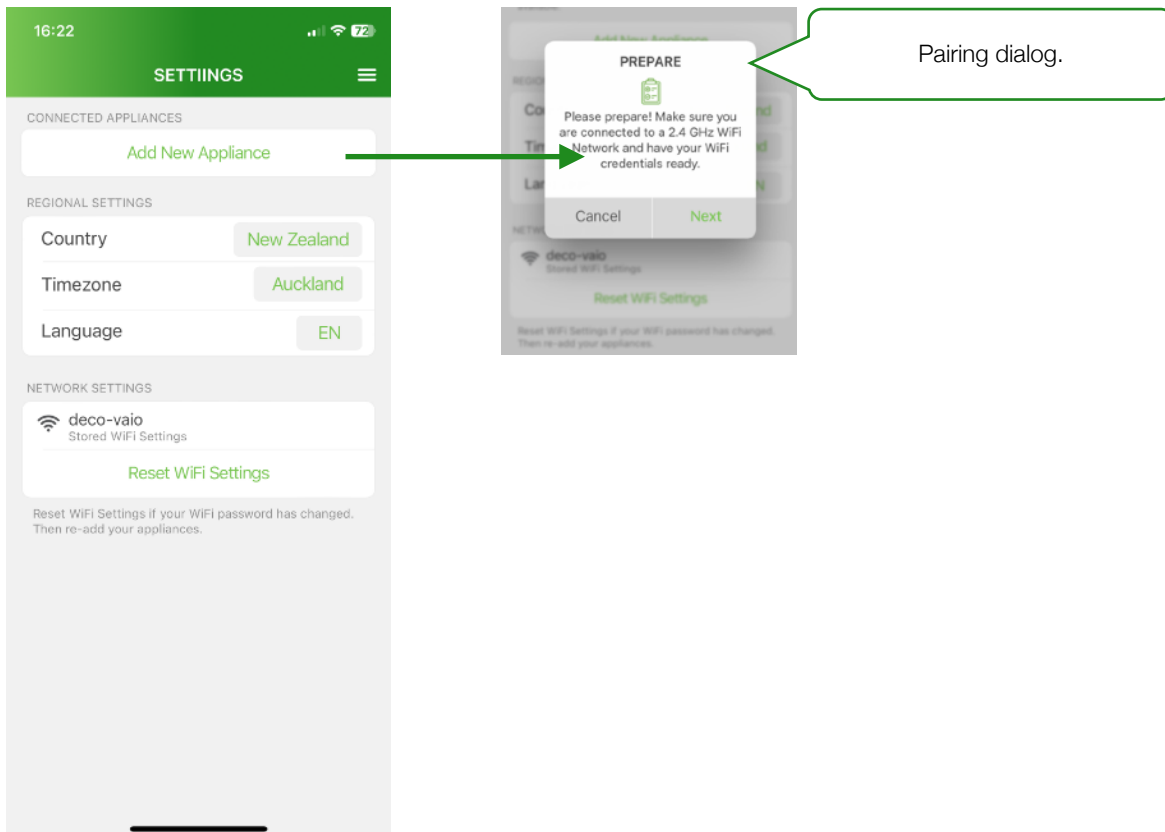
Step 4: Configure device

After successful pairing, a Configuration Screen "Manage Rowi" will be presented.

Exits the setup mode without saving the changes. If the device was reset to factory settings before, it goes back to factory settings after clicking on [Cancel].

MAC address and IP address of the device.

Function for sending device configuration and device secrets via email.

Save settings in the device. After saving the settings the device leaves the setup mode and goes into the operations mode.

Section for device settings.

Device secrets that are required for secure HTTPS (secret1), and secure MQTT connection (secret3). Secret 2 is for future use.

Step 4a: Select connectivity options

Configure the connectivity options based on your requirements. HTTP and HTTPS protocols are used to communicate with Rowi within the local WiFi network. When choosing HTTP, you can also specify the TCP port the Rowi device should be listening to. The default port for the HTTP connections is 80. When MQTT is activated, Rowi will send device and sensor data to an MQTT topic whose format is specified in the section "Communication Protocols / MQTT-Specific" of this manual. Please note that MQTT requires Internet connectivity. Don't select MQTT if your WiFi network is not connected to the Internet. This may negatively impact the performance and the responsiveness of Rowi.

Step 4b: Select the default behaviour of the relay

By activating the setting "Rely ON upon start", your Rowi will automatically switch on the relay upon each boot procedure regardless of the state of the relay before the device was powered off or rebooted.

Step 4c: Select the default behaviour of the relay

Archive Device IP, Device Settings and Device Secrets to an email address by clicking on [Email all Rowi info]. Make sure that after using the Email function, you return back to the mobile app to complete the Device Configuration.

Step 4d: Complete Device Configuration

After all fields within the section DEVICE SETTINGS have been configured, click on the button [Save] and follow the instructions of the mobile app. Rowi shall reboot and automatically connect to the WiFi network. After a successful setup, the LED of your Rowi should glow Green or Orange depending on the Relay ON settings. In case you've configured Rowi for Internet connectivity, but your WiFi network is currently not connected to the Internet, the LED will glow Light Blue.

Re-set to factory settings

In case you need to re-set your device to the factory settings, please follow these instructions:

1. Unplug Rowi
2. Long-press the MODE button on the front side of the device and while pressed plug-in again
2. Wait until the LED starts to glow Dark Blue and then release the MODE button

Please note that during the re-set procedure, Rowi generates a new set of secrets and the previously generated secrets become invalid.

REST API

The RESP API provides a set of commands that can be sent to the Rowi device within the local WiFi network either using HTTP or HTTPS. The commands are divided into two categories: GET (Read) and POST (Write) requests. The GET requests use query string parameters whereas POST requests expect the parameters to be transmitted within the request body in JSON format. All requests sent via HTTPS also require a secret (Secret 1) to be transmitted as an additional parameter for authorisation purposes.

Please note that, that even though the device is in the Operation Mode and shows the correct LED status, the REST API may need up to 2 minutes to become fully accessible. Sending the /ping command via REST API after the device moves into the Operation Mode speeds up the process and makes the API accessible immediately. Please, also note that the command and parameter names are case sensitive!

Overview of RESET API commands

Command	Type	Short description
/ping	GET	Checks if the device is alive and responsive
/getTemperature	GET	Returns device and ambient temperatures
/getRelayStatus	GET	Returns the current status of the relay (on or off)
/getSystemInfo	GET	Returns all settings and vital details about Rowi
/getPowerMeterData	GET	Returns info related to power consumption
/setRelayStatus	POST	Switch on/off relay
/setPermanentRelayStatus	POST	Switch on/off relay and store status in flash memory
/updateFirmwareAndReset	POST	Checks for and installs upgrades
/reboot	POST	Reboot Rowi

ping	
Command	/ping
Type	GET
Description	Checks if the device is alive and responsive
Parameters	-
Return value	{ "rslt": "OK" }
Example HTTP	http://192.168.0.111/ping
Example HTTPS	https://192.168.0.111/ping

getRelayStatus	
Command	/getRelayStatus
Type	GET
Description	Returns the current status of the relay and an info if the setting "Automatically On" is activated.
Parameters	secret for HTTPS

Return value	{
	   "rslt": "OK",
	   "rels": "0",
	   "alon": "0"
	}

Example HTTP	http://192.168.0.111/getRelayStatus
Example HTTPS	https://192.168.0.111/getRelayStatus?secret=lS8qVlcRuVSJPfjc

setRelayStatus	
Command	/setRelayStatus
Type	POST
Description	Sets the status of the relay to "on" or "off". The status remains valid until the next reboot of the device, at which it will be set to the value of the parameter "Automatically On".

Parameters
 	
JSON string in the request body
	data {"on" or "off"}
	secret for HTTPS
	
	For HTTP
	
	{
	   data: "off"
	}
	
	For HTTPS
	
	{
	   data: "off",
	   secret: "lS8qVlcRuVSJPfjc"
	}

Return value	{
	   "rslt": "OK"
	}

Example HTTP	http://192.168.0.111/setRelayStatus
Example HTTPS	https://192.168.0.111/setRelayStatus

getTemperature

Command	/getTemperature
Type	GET
Description	Returns temperature values (temperature inside device and calculated ambient temperature)
Parameters	secret for HTTPS

Return value	```{
	    "rslt": "OK",
	    "temp": "2500",
	    "humi": "6245",
	    "thcn": "1",
	    "thnm": "SHT3x"
	}```

Example HTTP	http://192.168.0.111/getTemperature
Example HTTPS	https://192.168.0.111/getTemperature?secret=IS8qVlcRuVSJPfjc

setPermanentRelayStatus

Command	/setPermanentRelayStatus
Type	POST
Description	Sets the status of the relay to "on" or "off" and stores it in the flash memory. The value set within the command overrides the value of "Automatically On".

Parameters
 	
JSON string in the request body
	data {"on" or "off"}
	secret for HTTPS
	
	For HTTP
	
	``{
	    data: "off"
	}```
	
	For HTTPS
	
	``{
	    data: "off",
	    secret: "IS8qVlcRuVSJPfjc"
	}```

Return value	```{ "rslt": "OK" }```
Example HTTP	http://192.168.0.111/setPermanentRelayStatus
Example HTTPS	https://192.168.0.111/setPermanentRelayStatus

getSystemInfo	
Command	/getSystemInfo
Type	GET
Description	Returns all configuration and system parameters of the Rowi device
Parameters	secret for HTTPS

Return value	<pre>{
	    "rslt": "OK",
	    "devi": "08:D1:F9:19:B3:44",
	    "hhea": "46",
	    "mqon": "1",
	    "alon": "0",
	    "inon": "1",
	    "hwve": "9",
	    "swve": "12843200",
	    "apve": "12848301",
	    "apty": "rowi-pm",
	    "cnin": "1",
	    "cnmq": "1",
	    "nsrv": "1",
	    "ssrv": "1",
	    "rels": "0",
	    "temp": "2950",
	    "humi": "3456",
	    "thcn": "1",
	    "thnm": "CHT8305",
	    "gso2": "0",
	    "gscn": "0",
	    "gsnm": "None",
	    "serr": "0",
	    "devt": "prod"
	}</pre>

Example HTTP	http://192.168.0.111/getSystemInfo
Example HTTPS	https://192.168.0.111/getSystemInfo?secret=IS8qVlcRuVSJPfjc

updateFirmwareAndReset	
Command	/updateFirmwareAndReset
Type	POST
Description	Checks if there is a new firmware version for Rowi available on the vendor's cloud server and if so upgrades Rowi. This process requires internet connectivity and can take up to 5 minutes.

Parameters
 	
JSON string in the request body
	secret for HTTPS
	
	For HTTP
	
	- no parameters required
	
	For HTTPS
	
	{
	   secret: "IS8qVlcRuVSJPfjc"
	}

Return value	{
	  "rslt": "OK"
	}

Example HTTP	http://192.168.0.111/updateFirmwareAndReset
Example HTTPS	https://192.168.0.111/updateFirmwareAndReset

reboot	
Command	/reboot
Type	POST
Description	Reboots Rowi. Use reboot command whenever you need to restart Rowi instead of unplugging and plugging-in again.

Parameters
 	
JSON string in the request body
	secret for HTTPS
	
	For HTTP
	
	- no parameters required
	
	For HTTPS
	
	{
	    secret: "IS8qVlcRuVSJPfjc"
	}

Return value	{
	    "rslt": "OK"
	}

Example HTTP	http://192.168.0.111/reboot
Example HTTPS	https://192.168.0.111/reboot

OVERVIEW OF DEVICE PARAMETERS

The below table explains the different parameters that are returned with the JSON object by the REST command /getSystemInfo and as part of the MQTT message.

JSON Key	REST API	MQTT	Meaning	Format
rslt	Yes	No	Command result, either "OK", "ERROR". In case of ERROR, the error message will be delivered via the JSON key "mssg".	"OK" or "ERROR"
devi	Yes	Yes	Unique Device ID	Mac address
hhea	Yes	Yes	Device health. Values under 20% are critical. Device may need to be rebooted.	Percent 1 … 100
mqon	Yes	No	MQTT Protocol is activtated	1 for Yes, 0 for No
alon	Yes	Yes	The relay is automatically switched upon device start and if there are no errors.	1 for Yes, 0 for No
inon	Yes	No	Internet is on or off	1 for Yes, 0 for No
hwve	Yes	Yes	Hardware version of the device	Number 1 … n
swve	Yes	Yes	Base firmware version	Number 1 … n
apve	Yes	Yes	Application version	Number 1 … n
apty	Yes	Yes	Application type	String
cnin	Yes	No	Connected to Internet	1 for Yes, 0 for No
cnmq	Yes	No	Connected to MQTT	1 for Yes, 0 for No
nsrv	Yes	Yes	HTTP Server is running	1 for Yes, 0 for No
ssrv	Yes	Yes	HTTPS Server is running	1 for Yes, 0 for No
rels	Yes	Yes	Relay is switched	1 for Yes, 0 for No
temp	Yes	Yes	Temperature	Number x 100
humi	Yes	Yes	Humidity	Number x 100
serr	Yes	Yes	Critical sensor error. Contact device vendor for further instructions.	1 for Yes, 0 for No
thcn	Yes	Yes	Indicates if the Temperature & Humidity Sensor is connected.	1 for Yes, 0 for No
thnm	Yes	Yes	Type of the connected Temperature & Humidity Sensor.	String
gso2	Yes	Yes	Value of the CO2 sensor	Number
gscn	Yes	Yes	Indicates if the CO2 sensor is connected	1 for Yes, 0 for No

JSON Key	REST API	MQTT	Meaning	Format
gsnm	Yes	Yes	Type of the connected CO2 sensor.	String
volt	Yes	Yes	Voltage in V measured on the power meter.	Number
imad	Yes	Yes	Current in A measured on the power meter.	Number
pmom	Yes	Yes	Power in Wh measured on the power meter.	Number
psmr	Yes	Yes	Summarised Power in Wh measured between two measurements (n and n-1).	Number
ipea	Yes	Yes	Peak Current in A measured since device start.	Number
ppea	Yes	Yes	Peak Power Consumption in Wh measured since device start.	Number

BEST PRACTICE

Performance

To achieve the maximum performance of the Rowi devices, configure them only for those connectivity options that will be used in production operations. For instance, if you know that the WiFi network won't be connected with the Internet, do not activate Internet and MQTT, or if you know that Rowi won't be accessed via HTTPS, don't activate HTTPS. Rowi will periodically try to establish Internet and MQTT connectivity, but always fail, which will unnecessarily consume CPU and memory resources and degrade the responsiveness of the API. Also, the HTTPS server requires relatively large memory allocation which is not worth spending if HTTPS is not used.

If the API access is required immediately after reboot, send the /ping command to speed up the API readiness. Otherwise, by default, the API may need up to 2 minutes to become fully accessible.

Device secrets

If you lose the secrets or/and the IP address of the Rowi device, re-run the configuration procedure using the mobile app without prior re-setting the device to the factory settings. Doing this, Rowi will take all new settings, including the new WiFi credentials (if changed), from the mobile app, but keep the existing secrets. After the end of configuration, the mobile app will display the existing secrets and IP addresses. The same procedure applies if your WiFi settings have changed - re-run the configuration without a prior re-set of the device.

In case your secrets have been compromised, re-set Rowi to the factory settings and re-run the configuration procedure using the mobile app. Re-setting Rowi to the factory settings enforces the generation of the new secrets.

Network

Make sure your WiFi network has sufficient capacity to accommodate new Rowi devices. It is important that the DHCP service of your network doesn't re-assign the IP address that was initially assigned to a Rowi device. Ideally, your network can be configured in such a way that the assigned IP addresses are permanently bound to the MAC addresses of your Rowi devices.

External Sensors

When using external sensors connected via 2.5mm audio connector, make sure that the device is powered on while the sensor is connected. Otherwise, the sensor will not be detected.

Firmware upgrades

Firmware upgrade over the air (OTAP) is one of the most complex procedures within an IoT ecosystem. To make this process as smooth as possible, follow these recommendations:

1) Make sure your WiFi network has a stable internet connectivity
2) Make sure that Rowi is not accessed by any application within your network
3) Run the the command /updateFirmwareAndReset
4) In case the first attempt fails, reboot Rowi by running /reboot command, wait for 2 minutes and execute steps 1 - 3 again