Plat'Home
TECHNOLOGY to serve you.

OpenBlocks IoT VX1
Data Acquisition Guide

Ver. 2.0.0

Plat'Home Co., Ltd.

■ About trademarks

- Company names, product names and other names in this document may be trademarks or registered trademarks of each company.
- Other proper names such as product names in this document are trademarks or registered trademarks of each company.

■ Before use

- It is prohibited to reprint the contents of this document in whole or in part without prior consent.
- The contents of this document are subject to change without notice.
- Although we make our best efforts to ensure the accuracy of this document, please contact our support center if you find typographical errors or other mistakes.
  The latest version of this document can be downloaded from our website.
- Note in advance that this device is not assumed to be used in in fields with fatal dangers.
- Note in advance that we bear no responsibility for any damages and lost earnings resulting from operation of this device.

Notes on Use

Meaning of symbols

The following categories of symbols explain the hazard level in terms of injury and material damage that may occur if instructions are not observed. Please thoroughly understand them before reading this manual.

⚠ DANGER	This symbol indicates that the possibility of death or serious injury is imminent when the product is handled improperly.
⚠ WARNING	This symbol indicates the possibility of death or serious injury when the product is handled improperly.
⚠ CAUTION	This symbol indicates a potentially hazardous situation that may result in minor injury and/or material damage when the product is handled improperly.

Meaning of pictures

The following categories of pictures explain instructions to follow. Please thoroughly understand them before reading this manual.

⊘ PROHIBITED	This indicates prohibited actions.
❗ MANDATORY	This indicates mandatory actions that must be followed.

Handling this device, SIM card *3, AC adapter *1, SD card *1 (common information)

⚠ DANGER	⊘	Do not use or place the product in areas of high temperatures (near open flames, near a heating appliance, in direct sunlight or in a car during hot weather etc.) It may cause modification or failure of the device, or leakage, overheating, ignition or explosion of the built-in battery. Moreover, a part of the case may become hot and cause burns or other injury.
	⊘	Please do not attempt to disassemble, alter or directly solder the device. It may result in fire, injury, electric shock, or equipment damage. It may also cause leakage, overheating, explosion or ignition of the built-in battery*1. Modification of the device is a violation of the radio law and will be penalized.
	⊘	Do not get the device wet. Leaving the device in wet condition after water or other liquid gets inside the device may cause overheating, electric shock, fire, injury or damage to the device. Please pay attention to the handling and the place of use.
⚠ DANGER	❗	Please do not use other AC adapters than those supplied with this device or those specified*2. Also do not use the supplied AC adapter*2 with other products. It may cause overheating, ignition or failure of the AC adapter*2.
⚠ WARNING	⊘	Do not place the device and/or the AC adapter*2 in a cooking appliance (e.g. microwave oven), a high pressure container (e.g. pressure cooker) or on top of an induction cooker (IH cooker.) It may cause leakage, overheating, explosion or ignition of the built-in battery and/or overheating, smoke, ignition or failure of the device or the AC adapter*2.
	⊘	Do not attempt to drop, throw or subject the device to any other severe impact or force. It may cause leakage, overheating, explosion, ignition, fire, electric shock or failure of the built-in battery.
	⊘	Do not let liquid such as water or conductive materials (e.g. a pencil lead or a piece of metal) touch external I/O port, plug of AC adapter*1, USB charging console cable*3 or plug of micro USB cable*2. Also, do not allow them enter into the device. They may cause fire or failure due to a short circuit.
	❗	Make sure to turn off the device beforehand when it is placed in locations subject to flammable gases such as propane gas or gasoline, or dust particles (like a gas station.) Gases may ignite. It may cause explosion or fire when it is used in locations subject to flammable gases such as propane gas or gasoline, or dust particles.
	❗	If you notice anything unusual such as noise, smoke or odor while using, charging or storing the device, take the following steps. 1. Turn off the device. 2. Unplug all the power cords. Unplug the AC adapter*2, holding the adapter body. Using the device in abnormal state may cause fire, electric shock, etc.
	❗	When putting the battery in the device*1, make sure to put the positive (+) and negative (-) ends of it in appropriate direction as it is shown. Putting it in the wrong direction may cause explosion, leakage or fire.

⚠ CAUTION	⊘	Do not place it on unstable surfaces such as wobbling table or inclined surface. It may drop and cause injury or failure.
	⊘	Hold the plug when you disconnect the device from a power supply device, and do not pull the cord. Pulling the cord may damage the cord or the port and cause fire or electric shock.

Handling the device

The specifications of the built-in battery of the device is as follows*1 :

Note	Type of battery
BR1225	Lithium coin cell

⚠ WARNING	⊘	Do not put it into fire. It may cause leakage, explosion or ignition of the built-in battery*2.
	⊘	Do not put foreign substances such as liquid (e.g. water), piece of metal or anything flammable in the SIM card slot*3 or micro SD card slot*4 of the device. It may cause fire, burns, injury or electric shock.
	❗	Make sure the device is turned off or is in flight mode when boarding an airplane. As use of the device in airplanes is limited, please follow the instructions of each airline. It can have a detrimental effect on electronic devices on airplanes. Committing a prohibited act while using the device on an airplane may be punished by law.
	❗	Follow the instructions of each healthcare facility for using the device in it. Turn off the device in locations where its usage is prohibited. It can have a detrimental effect on electronic devices or electronic medical equipment of healthcare facility.
	❗	Turn off the device near the electronic devices using high-precision control or weak signals. It can have a detrimental effect on the operation of electronic devices. * Examples of electronic devices which require extra attention Hearing aids, implantable cardiac pacemakers, implantable cardioverter defibrillators and other medical electric devices, fire alarms, automatic doors and other automatic control devices.
⚠ CAUTION	⊘	Please do not use it in case it has a detrimental effect on an electronic device in a vehicle. Using the device in an automobile could impair safe driving for some type of vehicles by having detrimental effect on its electronic device.
	⊘	Do not place magnetic cards or some other products near the device. Magnetic data on bank cards, credit cards, telephone cards, floppy disks, etc may be lost.
	⊘	Use specified batteries only.*2 There are risks of leakage, explosion or fire.
⚠ CAUTION	❗	Do not charge or disassemble a battery*1 after use or throw it into fire. There are risks of leakage, explosion or fire. Please dispose batteries*1 in accordance with your local government regulations.

Handling the AC adapter*2

⚠ WARNING	⊘	Do not cover or wrap the device with cloth, quilt or blanket. It may cause fire or failure because the heat does not dissipate.
	⊘	Use only with specified power source and voltage. Using with other power source or voltage may cause fire or failure. AC adapter: 100 VAC to 240 VAC (household AC power outlets only) Do not use transformers on the market for international travels. It may cause fire, electric shock or failure.
	⊘	Do not use it in case the cord of the AC adapter is damaged. It may cause fire, burns or electric shock.
	⊘	Do not touch the AC adapter when you hear thunder. It may cause electric shock.
	⊘	Do not plug or unplug the AC adapter or touch the port with a wet hand. It may cause electric shock or failure.
	❗	In case dust is adhering to the plug, unplug it from the outlet while holding the AC adapter, and wipe it with a dry cloth. It may cause fire.
	❗	Make sure the plug and terminal of AC adapter do not contact conductive materials (e.g. a pencil lead or a piece of metal) when plugging the AC adapter into the outlet, and make sure it is firmly plugged. Such contact may cause fire, burns or failure due to electric shock or a short circuit.
	❗	Plug or unplug the AC adapter straight and level, without applying excess force. Not doing so may result in fire, burns, injury or electric shock.
	❗	Unplug the AC adapter from the outlet while holding the AC adapter body when not using it over a long period of time. Not doing so may result in electric shock, fire or failure.
	❗	Immediately unplug it from the outlet while holding the AC adapter in case liquid such as water gets inside of it. Not doing so may result in electric shock, smoke or fire.

⚠ CAUTION	⊘	Do not attempt to subject the device to severe impact or force such as letting your foot catch the cord. It may cause injury or failure.
	⊘	Be careful not to let a part of the body such as a hand or a finger touch the plug. It may cause burns, electric shock, injury or failure.
	❗	Unplug the AC adapter from the outlet while holding the adapter body, and do not pull the cord. Pulling the cord may damage it and cause fire or electric shock.

*1 applies to OpenBlocks IoT BX0 / OpenBlocks IoT EX1
*2 applies when using the AC adapter
*3 applies to all but OpenBlocks IoT BX0
*4 applies to OpenBlocks IoT EX1

Precautions on handling Bluetooth®/Wi-Fi (Wireless LAN)

- Bluetooth® and Wi-Fi (wireless LAN) functions of the device use frequencies in the range of 2.4GHz.

  [The actual product]

  Bluetooth® function: 2.4 FH1/XX8

  The device uses 2.4GHz band. FH1 uses FH-SS modulation method, and its interference range is approximately within 10m. XX8 uses another modulation method, and its interference range is approximately within 80m.

  Wi-Fi (wireless LAN) function: 2.4 DS4 / OF4

  The device uses 2.4GHz band. It uses DS-SS method and OFDM method as its modulation methods. Its interference range is approximately within 40m.

  It uses the entire bandwidth from 2,400MHz to 2,483.5MHz, and it can avoid bandwidth of moving body identification device.

- The bandwidth of this device is also used by industrial / scientific / medical devices such as microwave oven, in-house radio station e.g. in factory production lines (radio stations which require a license) for moving body identification or specific low-power radio station (radio stations which do not require a license.)

(1). Make sure there is no in-house radio station for moving body identification or specific low-power radio station operating nearby before using this product.

(2). In case radio wave of this product interfered with an in-house radio station for moving body identification, immediately stop transmitting radio wave and contact the following address to consult us for necessary measures to avoid the interference (e.g. placing partitions.)

(3). Also, if there are other troubles, such as radio wave of the product interfered with a specific low-power radio station, please contact the following address.
Contact address : Plat' Home Co., Ltd. TEL: +81-3-5213-4372 E-Mail : support@plathome.co.jp

The device can use W52 channel in 5GHz bandwidth. The Radio Act prohibits using W52 outdoor.

Usage of Bluetooth®/Wi-Fi (wireless LAN) functions of the device may be limited in some countries / regions. Please check the local laws and regulations when using it outside Japan.

Other reminders

- The device is class B Information Technology Equipment. Even though the device is designed to be used in a domestic environment, it may cause harmful interference to receivers of radio or TV if they are close to the device. Install and use the device according to the instruction manual.
- This product is designed on the assumption that it will be used in Japan.
  Using the product outside Japan shall be at the customer's own risk.

Table of Contents

Chapter 1 Introduction

This document describes the data acquisition function in the OpenBlocks IoT VX1. A client device in which a web browser can be used (such as PC, smartphone, or tablet) is required for this setup. For description of the web user interface (called Web UI), see "OpenBlocks IoT VX1 Web UI Setup Guide."

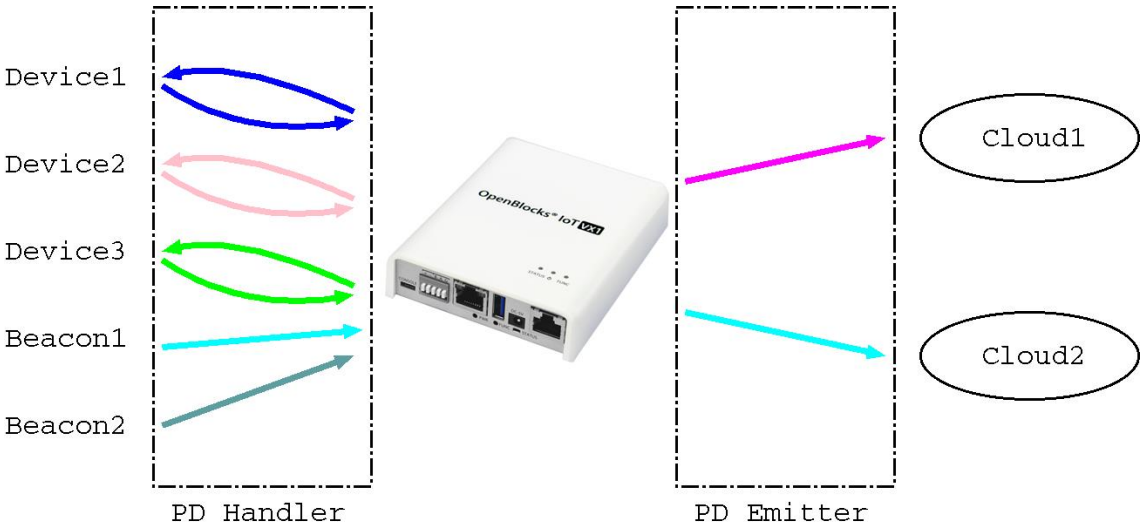
"OpenBlocks IoT VX1 Web UI Setup Guide" can be downloaded from the following URL:

http://openblocks.plathome.co.jp/common/pdf/obsiot_webui_setup_guide.pdf

Chapter 2 Data Acquisition Function

The data acquisition function of the Web UI in the OpenBlocks IoT VX1 supports beacons and some of BLE sensor devices. For supported sensor device and other products, see our website.

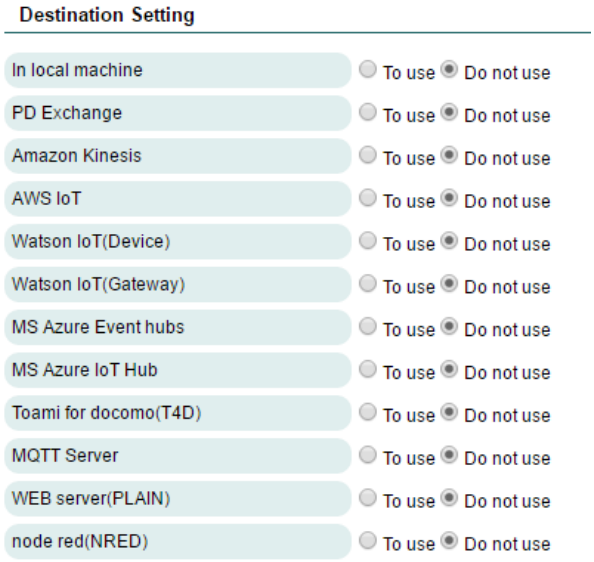
The acquisition function acquires data from each device or other product and sends the information to the cloud or other destination.
Because data is saved in the OpenBlocks IoT VX1 as temporary buffer, data is safely sent. This is because data can be resent even if a network failure or other problem occurs.



2-1. Data Acquisition Settings

When you enable data acquisition at [Service] ⇒ [Basic] tab on Web UI, the [Acquisition settings] tab appears.
You can set up data acquisition on this tab.

2-1-1. Destination Settings



The initial destination settings are as shown in the left screenshot.

Here, specify the settings for the cloud to which beacons or data in each device is uploaded.

When you select [To use] for each item, the settings associated with that item appear. These settings are described below.

You can specify up to two destinations except for "Main unit (local)."

● In local machine

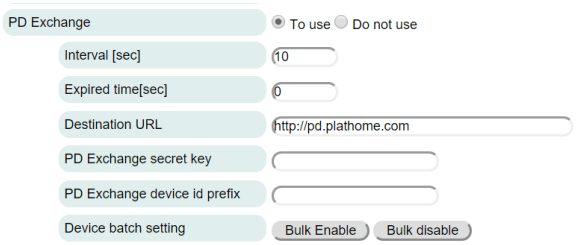
These settings are used to check if sensor data and beacon data is imported in the main unit normally.

This function is used only when the PD Handler is used.

Device batch setting:

You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

●PD Exchange



These settings are used to send sensor data and beacon data to PD Exchange.

Interval [sec]:

Specify the time interval between completion of transmission and start of transmission in seconds.

Expired time [sec]:

Specify the time to retain data if PD Emitter cannot send it.

If you specify 0, data is retained until completely sent.

Destination URL:

Specify the URL of destination PD Exchange.

PD Exchange secret key:

Specify the secret key for the connection destination PD Exchange account.

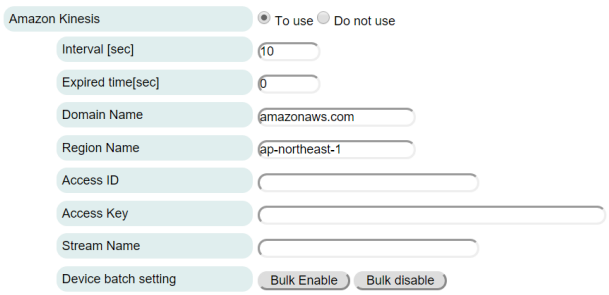
PD Exchange device id prefix:

Specify the device ID prefix for the connection destination PD Exchange account.

Device batch setting:

You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

● Amazon Kinesis



These settings are used to send sensor data and beacon data to Amazon Kinesis (called Kinesis below).

Interval [sec]:

Specify the time interval between completion of transmission and start of transmission in seconds.

Expired time [sec]:

Specify the time to retain data if PD Emitter cannot send it.

If you specify 0, data is retained until completely sent.

Domain Name:

Specify the domain name of destination Kinesis.

Normally, you do not have to change this item.

Region Name:

Specify the region name of destination Kinesis.

Access ID:

Specify the access ID of destination Kinesis.

Access Key:

Specify the access key of destination Kinesis.

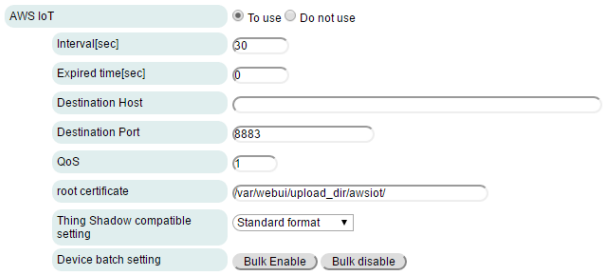
Stream Name:

Specify the stream name of destination Kinesis.

Device batch setting:

You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

●AWS IoT



These settings are used to send sensor data and beacon data to AWSIoT.

Interval [sec]:

Specify the time interval between completion of transmission and start of transmission in seconds.

Expired time [sec]:

Specify the time to retain data if PD Emitter cannot send it.

If you specify 0, data is retained until completely sent.

Destination Host:

Specify the host name (FQDN) of the destination AWSIoT.

Destination Port:

Specify the destination port number. Normally, you do not have to change from "8883".

QoS:

Specify the QoS when sending data to AWSIoT. The specification range is from 0 to 2.

root certificate:

Specify the root certificate file to connect for the distination AWSIoT.

Thing Shadow compatible setting:

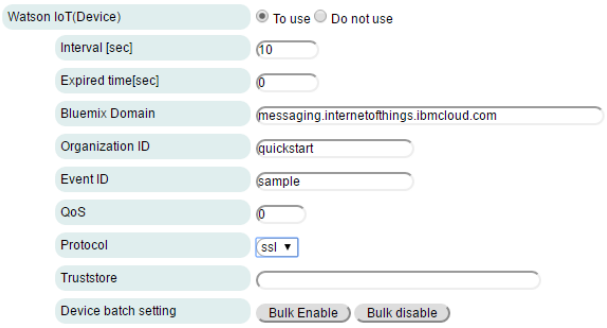
You can select format of the payload whether AWS IoT standard format or Thing Shadow compatible format that has been used in the FW 1.x previous.

Device batch setting:

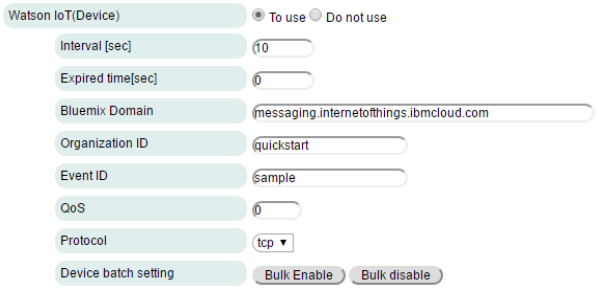
You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

* Upload the root certificate file at [System] ⇒ [File Management] tab on the Web UI.

●Watson IoT (Device)



*Sample



These settings are used to send sensor data or beacon data to IBM Watson IoT for device.

Interval [sec]:

Specify the time interval between completion of transmission and start of transmission in seconds.

Expired time [sec]:

Specify the time to retain data if PD Emitter cannot send it.

If you specify 0, data is retained until completely sent.

Domain Name:

Specify the Internet domain name of destination Watson IoT for device.

Organization ID:

Specify the organization ID of destination Watson IoT for device.

To use quickstart, specify quickstart.

Event ID:

Specify the event ID of destination Watson IoT for device.

QoS:

Specify the QoS when sending data to Watson IoT for device.

The specification range is from 0 to 2.

*To use quickstart, specify 0.

Protocol:

Select the transfer protocol ether TCP or SSL for the destination Watson IoT for device.

Truststore:

Specify the truststore file to connect for the destination Watson IoT for device with SSL protocol.

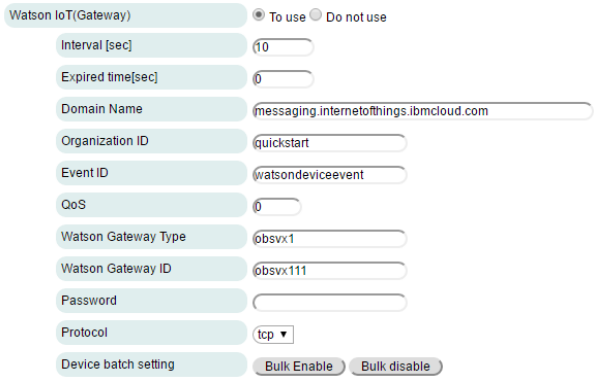
Device batch setting:

You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

* Upload the truststore file at [System] ⇒ [File Management] tab on the Web UI.

●Watson IoT (Gateway)

*Sample



These settings are used to send sensor data or beacon data to IBM Watson IoT for gateway.

Interval [sec]:

Specify the time interval between completion of transmission and start of transmission in seconds.

Expired time [sec]:

Specify the time to retain data if PD Emitter cannot send it.

If you specify 0, data is retained until completely sent.

Domain Name:

Specify the Internet domain name of destination Watson IoT for gateway.

Organization ID:

Specify the organization ID of destination Watson IoT for gateway.

To use quickstart, specify quickstart.

Event ID:

Specify the event ID of destination Watson IoT for gateway.

QoS:

Specify the QoS when sending data to Watson IoT for gateway.

The specification range is from 0 to 2.

*To use quickstart, specify 0.

Watson Gateway Type:

Specify the gateway type of destination Watson IoT for gateway.

Watson Gateway ID:

Specify the gateway ID of destination Watson IoT for gateway. It does not duplicate with other gateway that use the same destination.

Password:

Specify the password for the destination Watson IoT for gateway.

Protocol:

Select the transfer protocol ether TCP or SSL for the destination Watson IoT for gateway.

Server public certificate:

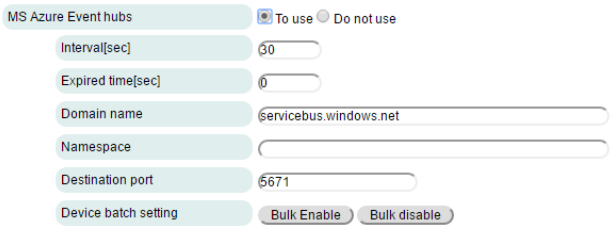
Specify the server public certificate file to connect for the destination Watson IoT for gateway with SSL protocol.

Device batch setting:

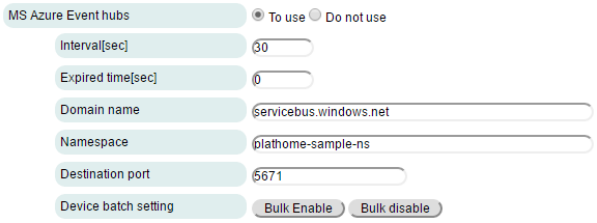
You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

* Upload the server public certificate file at [System] ⇒ [File Management] tab on the Web UI

●MS Azure Event hubs



*Sample



These settings are used to send sensor data and beacon data to the Microsoft Azure Event hubs.

Interval [sec]:

Specify the time interval between completion of transmission and start of transmission in seconds.

Expired time [sec]:

Specify the time to retain data if PD Emitter cannot send it.

If you specify 0, data is retained until completely sent.

Domain name:

Specify the Internet domain name of destination Event hubs.

Namespace:

Specify the Namespace of destination Event hubs.

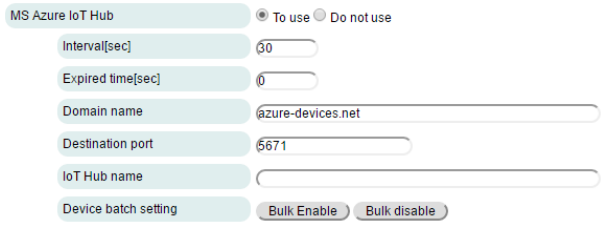
Destination port:

Specify the port number used to connect to the destination Event hubs. Normally, you do not have to change from "5671".

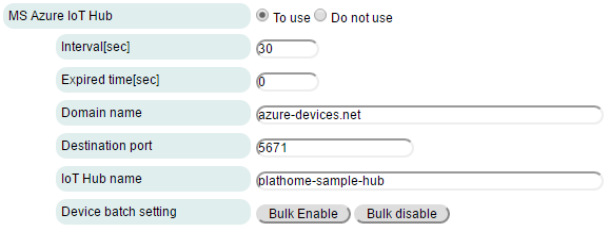
Device batch setting:

You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

●MS Azure IoT Hub



*Sample



These settings are used to send sensor data and beacon data to the Microsoft Azure IoT Hub.

Interval [sec]:

Specify the time interval between completion of transmission and start of transmission in seconds.

Expired time [sec]:

Specify the time to retain data if PD Emitter cannot send it.

If you specify 0, data is retained until completely sent.

Domain name:

Specify the Internet domain name of destination IoT Hub.

Destination port:

Specify the port number used to connect to the destination IoT Hub. Normally, you do not have to change from "5671".

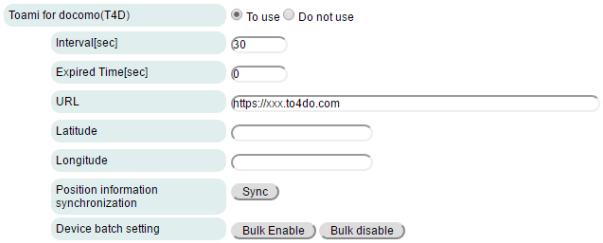
IoT Hub name:

Specify the IoT Hub name of destination.

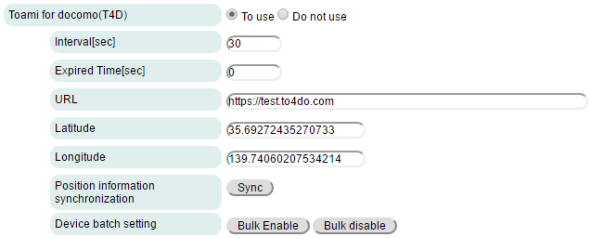
Device batch setting:

You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

●Toami for docomo (T4D)



*Sample



These settings are used to send sensor data and beacon data to the Toami for docomo that provided by NTT docomo.

Interval [sec]:

Specify the time interval between completion of transmission and start of transmission in seconds.

Expired time [sec]:

Specify the time to retain data if PD Emitter cannot send it.

If you specify 0, data is retained until completely sent.

URL:

Specify the URL of destination Toami for docomo.

Latitude:

Specify the the latitude of the location to be added to the payload.

Longitude:

Specify the the longitude of the location to be added to the payload.

Position information synchronization:

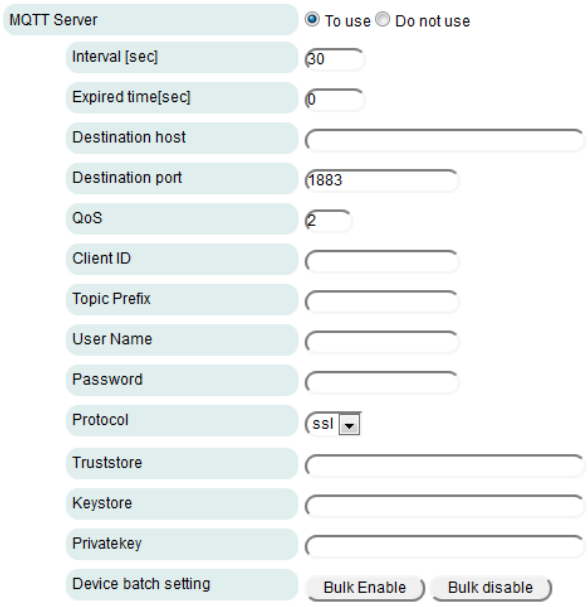
Copy the location information that specified by [System] ⇒ [Basic] tab to above columns.

Device batch setting:

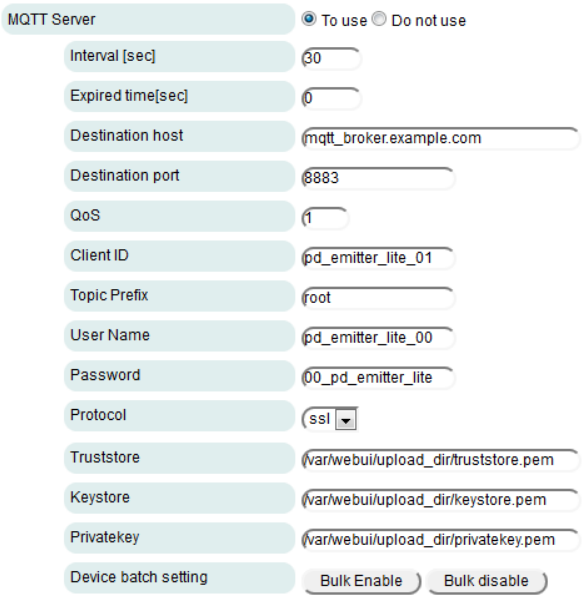
You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

* In Toami for docomo, you must make the conversion of data to be transmitted. Will appear the Key conversion tab after the save button selected in the settings that you want to use the Toami for docomo, please set from the Key conversion tab. See chapter 2-2.

●MQTT Server



*Sample



These settings are used to send sensor data and beacon data to the MQTT server you built by yourself.

Interval [sec]:

Specify the time interval between completion of transmission and start of transmission in seconds.

Expired time [sec]:

Specify the time to retain data if PD Emitter cannot send it.

If you specify 0, data is retained until completely sent.

Destination host:

Specify the FQDN or IP address of the destination MQTT server.

Destination port:

Specify the port number used to connect to the destination MQTT server. Normally, you do not have to change "1883".

QoS:

Specify the QoS when sending data to the MQTT server. The specification range is from 0 to 2.

Client ID:

Specify the client ID when sending data to the MQTT server. It does not duplicate with other publisher or subscriber that use the same MQTT server.

Topic Prefix:

Specify the topic prefix when sending data to the MQTT server. Configure the topic using the unique ID (MQTT) you set with beacon or sensor transmission settings as the suffix. The prefix and the suffix are separated with a slash (/) and sent.

User Name:

Specify the user name of destination MQTT server.

Password:

Specify the password of destination MQTT server.

Protocol:

Select the transfer protocol ether TCP or SSL for the destination MQTT server.

Truststore:

Specify the Truststore file to connect for the destination MQTT server with SSL protocol, if nessary.

Keystore:

Specify the Keystore file to connect for the destination MQTT server with SSL protocol, if nessary.

Privatekey:

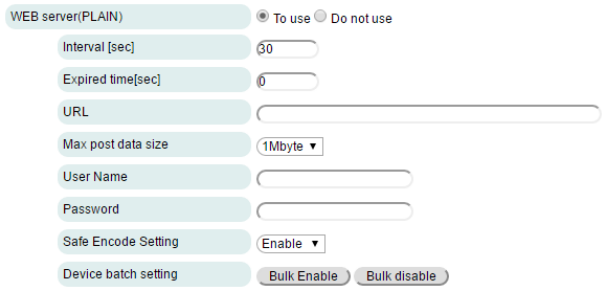
Specify the privatekey file to connect for the destination MQTT server with SSL protocol, if nessary.

Device batch setting:

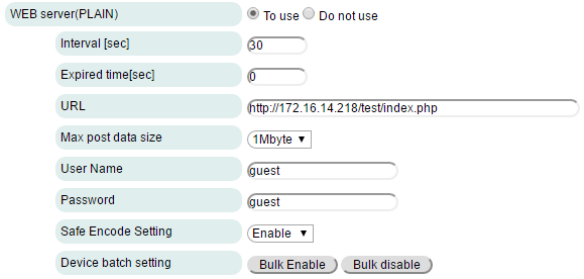
You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

* Upload the truststore file or keystoref, privatekey file at [System] ⇒ [File Management] tab on the Web UI

● WEB server (PLAIN)



*Sample



These settings are used to send sensor data and beacon data to the web server you built by yourself.

Interval [sec]:

Specify the time interval between completion of transmission and start of transmission in seconds.

Expired time [sec]:

Specify the time to retain data if PD Emitter cannot send it.

If you specify 0, data is retained until completely sent.

URL:

Specify the URL of destination web server.

Max post data size:

Select the maximum data size for one POST method. Select from 1 to 4 Mbyte.

User Name:

Specify the user name used when the web server performs basic authentication.

Password:

Specify the password used when the web server performs basic authentication.

Safe Encode Setting:

Enable the URL safe encoding for payload and add the Content-type to header of HTTP.

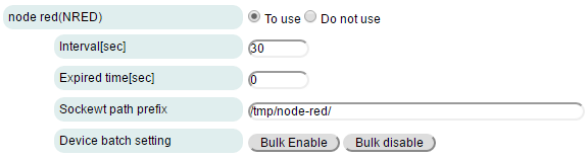
Device batch setting:

You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

* Use the POST method to send data to the web server. At this time, put multiple data items together in the Records variable and send them as following.

{“Records”:[{DATA1},{DATA2},{DATA3},…{DATAn}]}

● node red (NRED)



These settings are used to send sensor data and beacon data to the Unix domain socket of Node-RED, which is built in local.

Interval [sec]:

Specify the time interval between completion of transmission and start of transmission in seconds.

Expired time [sec]:

Specify the time to retain data if PD Emitter cannot send it.

If you specify 0, data is retained until completely sent.

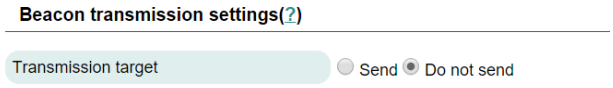
Socket path prefix:

Specify the pathname prefixe of the Unix domain socket.

Device batch setting:

You can enable/disable the destination settings for each target for which [Send] is selected as the beacon and device transmission target settings in batch.

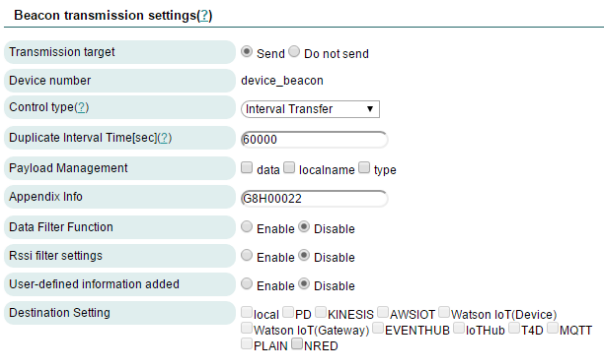
2-1-2. Beacon Transmission Settings



The initial destination settings are as shown in the left screenshot.

Here, select [Send] to send beacon data to the cloud or other destination.

Note) The beacon that you are transmitted by the device information transmission settings, as described below, this section does not apply.



When you select [Send], each item appears as shown in the left screenshot.

Device number:

Number managed on the Web UI in the OpenBlocks IoT VX1. This number cannot be changed.

Control type:

Select how to manage beacon data from the following options. For each method, see "Beacon Duplicate Control Algorithm" below.

- Interval transfer
- Entry point transfer
- In/out status transfer

Duplicate Interval Time [ms]:

Specify the control time for each control type in milliseconds.

Payload Management:

Select whether to append each type of information in beacon when passing beacon data to PD Emitter.

data: Advertisement data (hexadecimal)

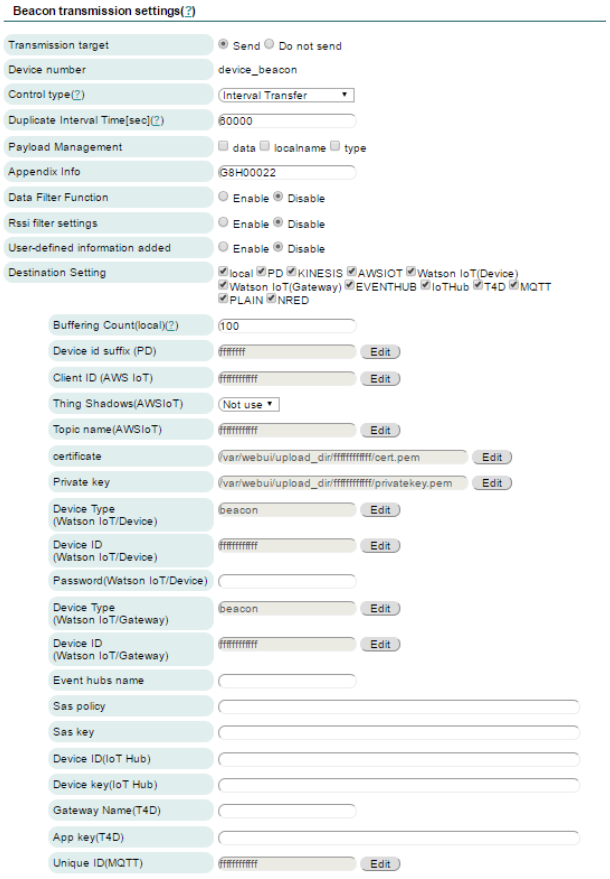
localname: Device name

type: Data type

Appendix Info:

Specify information to be appended such as the source OpenBlocks IoT Family when

*Sample



sending beacon data to each cloud.

*The default is the serial number of the main unit.

Data Filter Function: (data prefix)

Specify the filter to select the beacon to be sent. When you enter a filter condition in [Data Prefix] in hexadecimal format, the advertisement information in the beacon is compared with forward match and only matched data is sent to the destination.

*You can register multiple conditions with the [Add] button.

*To set the data filter, filter the device seeing data in the log in this device (local). The filter applies to logs in this device (local) as well.

User-defined information added: (additional information setting)

You can add pairs of key name and value to data passed to PD Emitter.

*You can register up to five pairs with the [Add] button.

Destination Setting:

The check boxes corresponding to the destinations for which "Use" is selected become selectable.

Data is sent to the cloud and other destinations whose check boxes are selected.

Buffering Count (local):

Save advertisement data from surrounding devices in the main unit. The maximum count is 10,000.

Device id suffix (PD):

Specify the device ID suffix when sending data to PD Exchange.

Client ID (AWSIoT):

Specify the client ID when sending data to

AWSIoT. It does not duplicate with other client ID that use the same destination. When Thing Shadows is used, the client ID is Thing Name.

Thing Shadows (AWSIoT):

Select whether to use Thing Shadows when sending data to AWSIoT.

Topic name (AWSIoT):

Specify the topic when sending data to AWSIoT. When Thing Shadows is used, the topic is automatically generated using the client ID as Thing Name.

Certificate (AWSIoT):

Specify the device certificate file used when sending data to AWSIoT.

Privatekey (AWSIoT):

Specify the privatekey file for the device used when sending data to AWSIoT.

Device type (Watoson IoT/Device):

Specify the device type when sending data to Watoson IoT for device.

Device ID (Watoson IoT/Device):

Specify the device ID when sending data to Watoson IoT for device.

Password (Watoson IoT/Device):

Specify the device type when sending data to Watoson IoT for device, if necessary.

Device type (Watoson IoT/Gateway):

Specify the device type when sending data to Watoson IoT for gateway.

Device ID (Watoson IoT/Gateway):

Specify the device ID when sending data to Watoson IoT for gateway.

Event hubs name (EVENTHUB):

Specify the Event hubs name when sending data to Event hubs.

Sas policy (EVENTHUB):

Specify the SAS policy when sending data to Event hubs.

Sas key (EVENTHUB):

Specify the SAS key when sending data to Event hubs.

Device ID (IoT Hub):

Specify the Device ID when sending data to IoT Hub.

Device key (IoT Hub):

Specify the Device key when sending data to IoT Hub.

Gateway Name (T4D):

Specify the Gateway name when sending data to Toami for docomo.

App key (T4D):

Specify the App key when sending data to Toami for docomo.

Unique ID (MQTT):

Specify the unique ID when sending data to the MQTT server. The unique ID is treated as the topic suffix. The topic prefix is set to the MQTT server. The prefix and the suffix are separated with a slash (/) and sent.

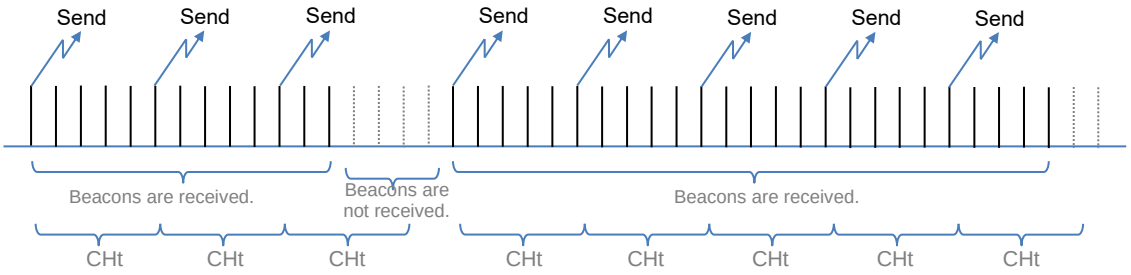
*Information linked with cloud settings can be edited with the Edit button.

*Upload the certificate file and privatekey file from [System] ⇒ [File management] tab.

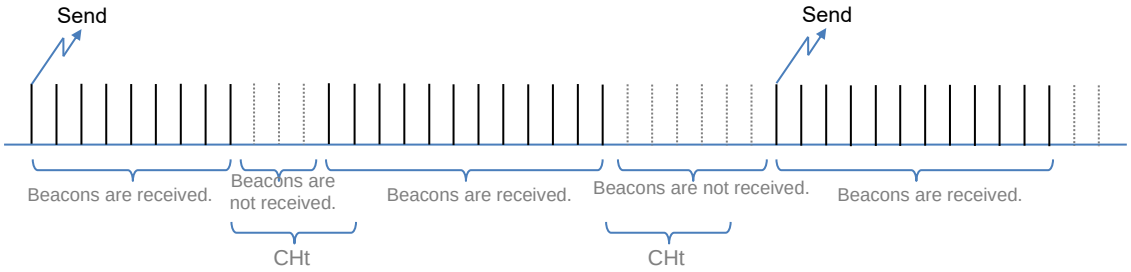
Beacon duplicate control algorithm

Settings assumed for this description
Beacon transmission interval = 1 second
Duplicate control time interval (CHt) = 5 seconds

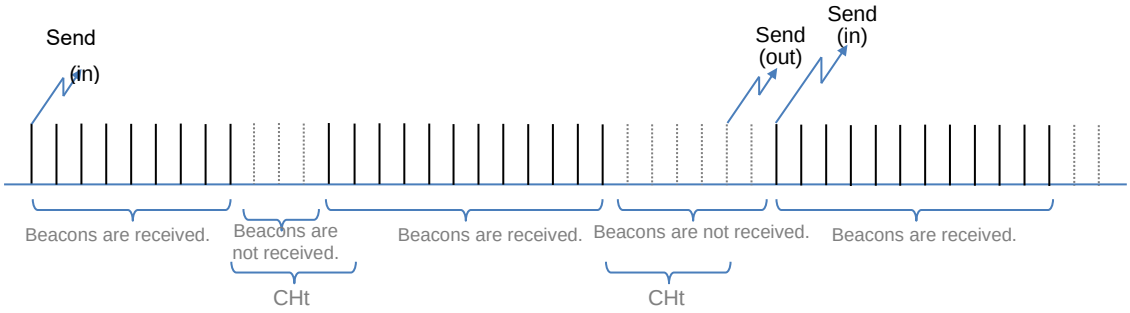
① Interval transfer
Data is sent to the transmission program at specified intervals while beacon is received.



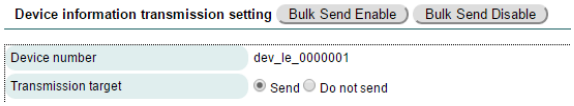
② Entry point transfer
Data is sent to the transmission program when beacon is received.
(Even if beacon is not temporarily received within the CHt time, it is not regarded as exit.)



③ In/out status transfer
Data is sent to the transmission program with the IN/OUT flag when beacon enters and exits.
(Even if beacon is not temporarily received within the CHt time, it is not regarded as exit.)



2-1-3. Device Information Transmission Setting

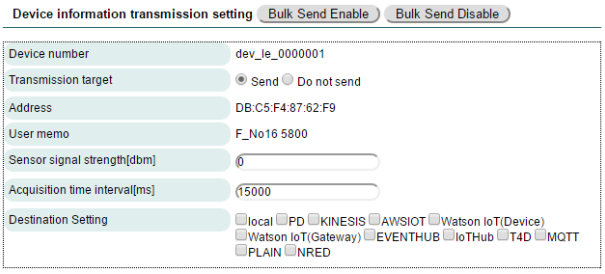


If the registered BLE device exists, the initial status is as shown in the left screenshot.

*This is when a BLE device is registered.

You can specify device transmission settings in detail by selecting [Send] in [Transmission target] for each device.

*You can control transmission targets of all the registered devices with the [Enable transmission target in batch] or [Disable transmission target in batch] button.



When you select [Send], each item appears as shown in the left screenshot.

Device number:

Number managed on the Web UI in the OpenBlocks IoT Family. This number cannot be changed.

Address:

Displays the Bluetooth address of the registered device.

User memo:

Displays note information set in the registered device.

Sensor signal strength [dbm]:

Enter the desired signal strength if your sensor model supports specification of signal strength.

If the specified signal strength is not available, an approximate value or default value is set.

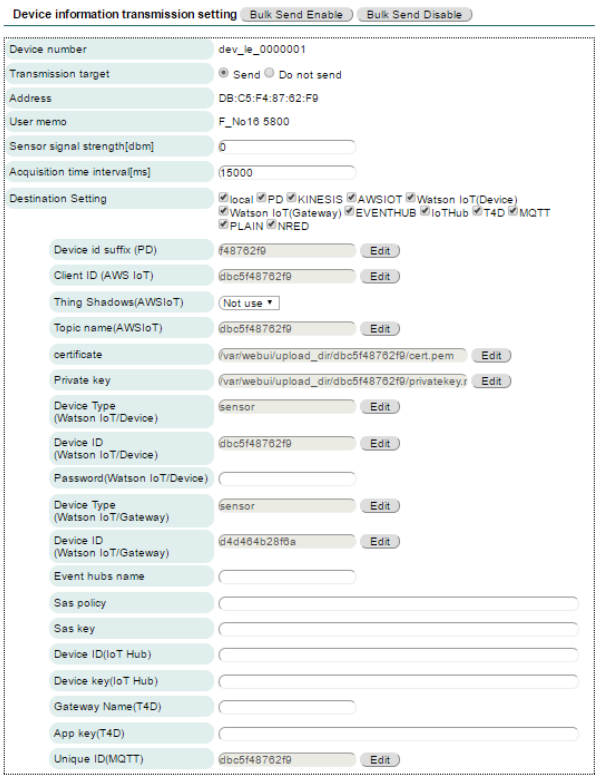
Acquisition time interval [ms]:

Specify the time interval to acquire data from the sensor with a number in milliseconds.

Destination Setting:

The check boxes corresponding to the destinations for which "Use" is selected become selectable.

*Sample



Data is sent to the cloud and other destinations whose check boxes are selected.

Device id suffix (PD):

Specify the device ID suffix when sending data to PD Exchange.

Client ID (AWSIoT):

Specify the client ID when sending data to AWSIoT. It does not duplicate with other client ID that use the same destination. When Thing Shadows is used, the client ID is Thing Name.

Thing Shadows (AWSIoT):

Select whether to use Thing Shadows when sending data to AWSIoT.

Topic name (AWSIoT):

Specify the topic when sending data to AWSIoT. When Thing Shadows is used, the topic is automatically generated using the client ID as Thing Name.

Certificate (AWSIoT):

Specify the device certificate file used when sending data to AWSIoT.

Privatekey (AWSIoT):

Specify the privatekey file for the device used when sending data to AWSIoT.

Device type (Watson IoT/Device):

Specify the device type when sending data to Watson IoT for device.

Device (Watson IoT/Device):

Specify the device ID when sending data to Watson IoT for device.

Password (Watoson IoT/Device):

Specify the device type when sending data to Watoson IoT for device, if necessary.

Device type (Watoson IoT/Gateway):

Specify the device type when sending data to Watoson IoT for gateway.

Device ID (Watoson IoT/Gateway):
Specify the device ID when sending data to Watoson IoT for gateway.

Event hubs name (EVENTHUB):
Specify the Event hubs name when sending data to Event hubs.

Sas policy (EVENTHUB):
Specify the SAS policy when sending data to Event hubs.

Sas key (EVENTHUB):
Specify the SAS key when sending data to Event hubs.

Device ID (IoT Hub):
Specify the Device ID when sending data to IoT Hub.

Device key (IoT Hub):
Specify the Device key when sending data to IoT Hub.

Gateway Name (T4D):
Specify the Gateway name when sending data to Toami for docomo.

App key (T4D):
Specify the App key when sending data to Toami for docomo.

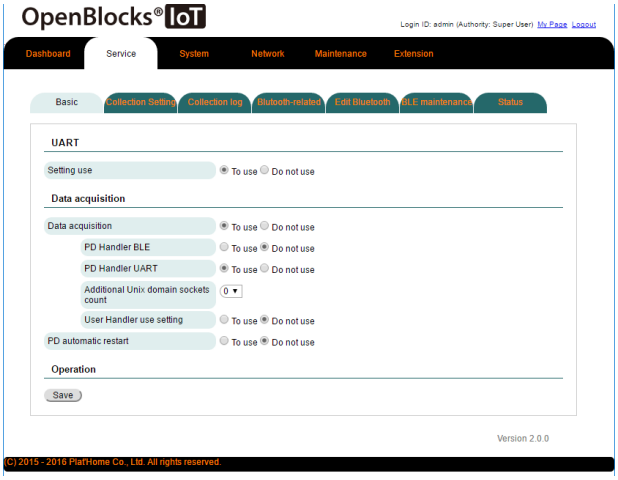
Unique ID (MQTT):
Specify the unique ID when sending data to the MQTT server. The unique ID is treated as the topic suffix. The topic prefix is set to the MQTT server. The prefix and the suffix are separated with a slash (/) and sent.

*Information linked with cloud settings can be edited with the Edit button. It is recommended to use the same settings when replacing the device due to failure or other reason to handle the new device in the same way as the old device. (For the failed device, change [Transmission target] to [Do not send].)

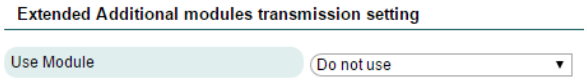
*Upload the certificate file and privatekey file from [System] ⇒ [File management] tab.

2-1-4. Extended Additional modules transmission setting

In the WEB UI version 1.0.8 or later, will be displayed this function, if extended additional modules that either EnOcean module or Wi-SUN module or FCL Specific small power wireless module (MBH7SLZ01) has been mounted on the OpenBlocks IoT EX1. This function gets the device information from extended additional module by the PD Handler UART.



In order to use the extended additional modules, you need to enable the UART Setting and the PD Handler UART in the [Service] ⇒ [Basic] tab.



In the initial state is selected to [Do not use].
If you want to get the data from the module, please select the target module in the [Service] ⇒ [Collection Setting] tab.

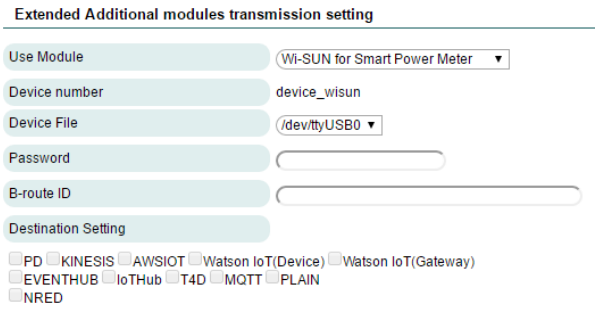
*FCL Specific small power wireless module (MBH7SLZ01) is domestic product of Japan by the Fujitsu Component to use the 920MHz band. For implementation of this module is a beta version, be careful in your use.

● Wi-SUN Module

It corresponds to the acquisition of the amount of electric power by B-route. In the case of the amount of electric power of acquisition in the B route, select the [Wi-SUN (B-route)] in the use module column. It should be noted that, for the communication other than B-route is not currently supported 2016/4.

*For more information about the contents of the data to be transmitted to the PD Emitter, it will be the value corresponding to the particular key.

*The B-route, is a feature that consumer is to get the data from Smart Meter. The Smart Meter, is a power meter that has a communication function.



In the case of the acquisition of the amount of power by the B-route, please set a password and B-route ID sent from the electric power company.

Device File:

Select the device file for the extended additional modules.

(In normal, it will be the file at the bottom of the list.)

Password:

Specify the password for the connection to the Smart Meter.

B-route ID:

Specify the B-route ID for connection to the Smart Meter.

*B-route ID begins with ‘00’.

Destination Setting:

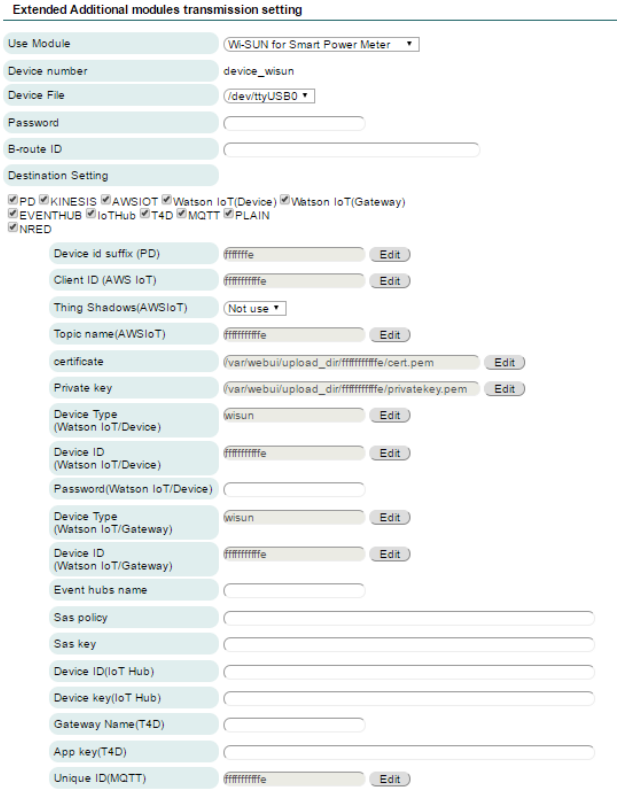
The check boxes corresponding to the destinations for which "Use" is selected become selectable.

Data is sent to the cloud and other destinations whose check boxes are selected.

Device id suffix (PD):

Specify the device ID suffix when sending data to PD Exchange.

*Sample



Client ID (AWSIoT):

Specify the client ID when sending data to AWSIoT. It does not duplicate with other client ID that use the same destination. When Thing Shadows is used, the client ID is Thing Name.

Thing Shadows (AWSIoT):

Select whether to use Thing Shadows when sending data to AWSIoT.

Topic name (AWSIoT):

Specify the topic when sending data to AWSIoT. When Thing Shadows is used, the topic is automatically generated using the client ID as Thing Name.

Certificate (AWSIoT):

Specify the device certificate file used when sending data to AWSIoT.

Privatekey (AWSIoT):

Specify the privatekey file for the device used when sending data to AWSIoT.

Device type (Watson IoT/Device):

Specify the device type when sending data to Watson IoT for device.

Device (Watson IoT/Device):

Specify the device ID when sending data to Watson IoT for device.

Password (Watoson IoT/Device):

Specify the device type when sending data to Watoson IoT for device, if necessary.

Device type (Watoson IoT/Gateway):

Specify the device type when sending data to Watoson IoT for gateway.

Device ID (Watoson IoT/Gateway):

Specify the device ID when sending data to Watoson IoT for gateway.

Event hubs name (EVENTHUB):

Specify the Event hubs name when sending data to Event hubs.

Sas policy (EVENTHUB):

Specify the SAS policy when sending data to Event hubs.

Sas key (EVENTHUB):

Specify the SAS key when sending data to Event hubs.

Device ID (IoT Hub):

Specify the Device ID when sending data to IoT Hub.

Device key (IoT Hub):

Specify the Device key when sending data to IoT Hub.

Gateway Name (T4D):

Specify the Gateway name when sending data to Toami for docomo.

App key (T4D):

Specify the App key when sending data to Toami for docomo.

Unique ID (MQTT):

Specify the unique ID when sending data to the MQTT server. The unique ID is treated as the topic suffix. The topic prefix is set to the MQTT server. The prefix and the suffix are separated with a slash (/) and sent.

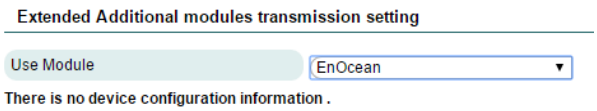
*Information linked with cloud settings can be edited with the Edit button. It is recommended to use the same settings when replacing the device due to failure or other reason to handle the new device in the same way as the old device. (For the failed device, change [Transmission target] to [Do not send].)

*Upload the certificate file and privatekey file from [System] ⇒ [File management] tab.

● EnOcean Module

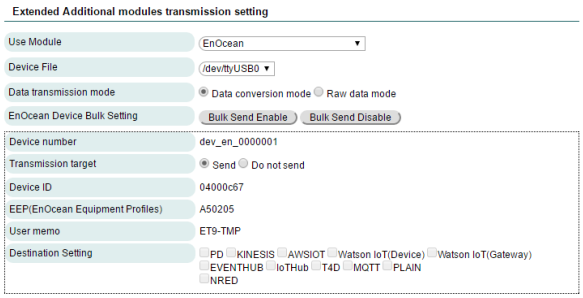
In the case of the data acquisition from EnOcean devices, select the [EnOcean] in the use module column. It gets the data only from registered EnOcean devices. Data from EnOcean devices that are not registered will not be acquired.

*For more information about the contents of the data to be transmitted to the PD Emitter, it will depend on the data transmission mode and the corresponding EEP(EnOcean Equipment Profiles.).



If the EnOcean of the device is not registered, it will be displayed as shown in the figure on the left.

In this case, please register the EnOcean device from [EnOcean Regist] tab.



When the EnOcean device is registered, it will be displayed as shown in the figure on the left.

Device File:

Select the device file for the extended additional modules.

(In normal, it will be the file at the bottom of the list.)

Data transmission mode:

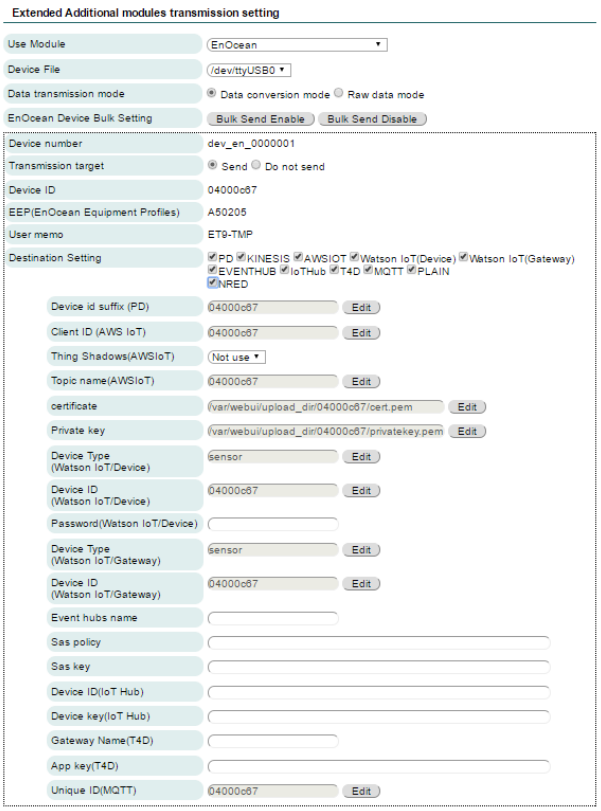
Specify the mode of transmition data to PD Emitter.

Data conversion mode, if the EEP is supported, and sends the data of the analysis to the PD Emitter. If it does not, it will send to convert the received data in hexadecimal to PD Emitter.

Raw data mode, sends it to the PD Emitter to convert the received data in hexadecimal. It dose not depends on EEP support.

EnOcean Device Bulk Setting:

You can select enable/disable destination settings for batch setting of the transmission target setting of all of the EnOcean devices.



Destination Setting:

The check boxes corresponding to the destinations for which "Use" is selected become selectable.

Data is sent to the cloud and other destinations whose check boxes are selected.

Device id suffix (PD):

Specify the device ID suffix when sending data to PD Exchange.

Client ID (AWSIoT):

Specify the client ID when sending data to AWSIoT. It does not duplicate with other client ID that use the same destination. When Thing Shadows is used, the client ID is Thing Name.

Thing Shadows (AWSIoT):

Select whether to use Thing Shadows when sending data to AWSIoT.

Topic name (AWSIoT):

Specify the topic when sending data to AWSIoT. When Thing Shadows is used, the topic is automatically generated using the client ID as Thing Name.

Certificate (AWSIoT):

Specify the device certificate file used when sending data to AWSIoT.

Privatekey (AWSIoT):

Specify the privatekey file for the device used when sending data to AWSIoT.

Device type (Watson IoT/Device):

Specify the device type when sending data to Watson IoT for device.

Device (Watson IoT/Device):

Specify the device ID when sending data to Watson IoT for device.

Password (Watoson IoT/Device):

Specify the device type when sending data to Watoson IoT for device, if necessary.

Device type (Watoson IoT/Gateway):

Specify the device type when sending data to Watoson IoT for gateway.

Device ID (Watoson IoT/Gateway):

Specify the device ID when sending data to Watoson IoT for gateway.

Event hubs name (EVENTHUB):

Specify the Event hubs name when sending data to Event hubs.

Sas policy (EVENTHUB):

Specify the SAS policy when sending data to Event hubs.

Sas key (EVENTHUB):

Specify the SAS key when sending data to Event hubs.

Device ID (IoT Hub):

Specify the Device ID when sending data to IoT Hub.

Device key (IoT Hub):

Specify the Device key when sending data to IoT Hub.

Gateway Name (T4D):

Specify the Gateway name when sending data to Toami for docomo.

App key (T4D):

Specify the App key when sending data to Toami for docomo.

Unique ID (MQTT):

Specify the unique ID when sending data to the MQTT server. The unique ID is treated as the topic suffix. The topic prefix is set to the MQTT server. The prefix and the suffix are separated with a slash (/) and sent.

* Information linked with cloud settings can be edited with the Edit button. It is recommended to use the same settings when replacing the device due to failure or other reason to handle the new device in the same way as the old device. (For the failed device, change [Transmission target] to [Do not send].)
* Upload the certificate file and privatekey file from [System] ⇒ [File management] tab.

● FCL Specific small power wireless module

In the case of performing the data reception at the Specific small power wireless module between each other, and then select the [FCL Specific small power module] in the use module column.

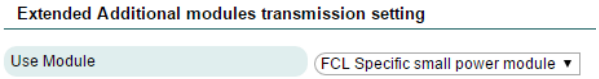
This unit is made with a particular base unit of wireless communication to collect the data, which has received the data from the child unit.

* The contents of the data to be transmitted to the PD Emitter is the data that is base64-encoded data received from the child device.

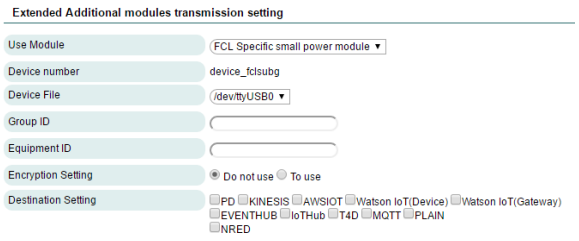
* Specific vendor ID of the Small power wireless module has been fixed. If the same vender ID is exist, it may collision of communication with the target module occur.

In addition, the module for the evaluation is the vendor ID has become a fixed to '0'

* For implementation of this module is a beta version, be careful in your use.



In the case of Specific small power wireless module selected, it will be displayed as shown in the figure on the left.



Device number:

It will be specified automatically. This item is not be changed.

Device File:

Select the device file for the extended additional modules.

(In normal, it will be the file at the bottom of the list.)

Group ID:

Enter the common ID for module with each other to carry out the communication to be used.

Input possible values are 1 to 255.

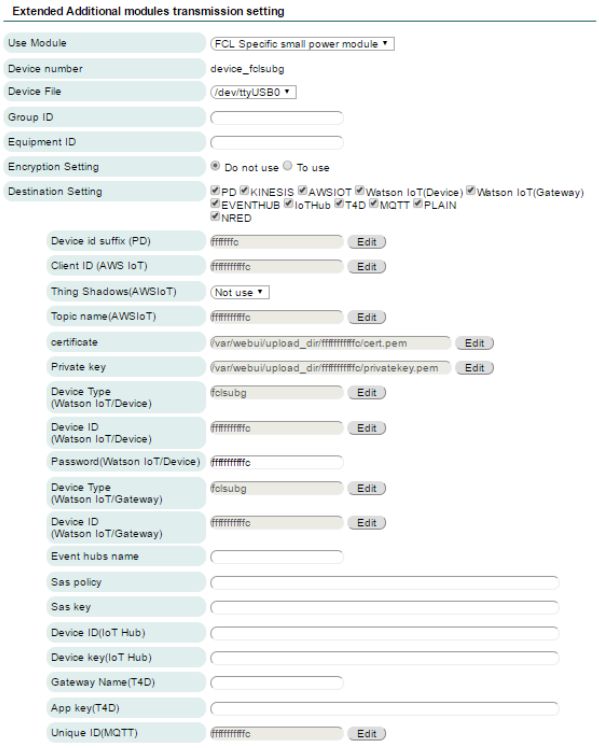
Equipment ID:

Enter the ID of module that is mounted.

Input possible values are 1 to 65533.

Encryption Setting:

Set whether to encrypt communications.



Encryption Key (32chars):

Spedify encryption key. 32 hexadecimal characters (0-9, A-F) to specify.

Destination Setting:

The check boxes corresponding to the destinations for which "Use" is selected become selectable.

Data is sent to the cloud and other destinations whose check boxes are selected.

Device id suffix (PD):

Specify the device ID suffix when sending data to PD Exchange.

Client ID (AWSIoT):

Specify the client ID when sending data to AWSIoT. It does not duplicate with other client ID that use the same destination. When Thing Shadows is used, the client ID is Thing Name.

Thing Shadows (AWSIoT):

Select whether to use Thing Shadows when sending data to AWSIoT.

Topic name (AWSIoT):

Specify the topic when sending data to AWSIoT. When Thing Shadows is used, the topic is automatically generated using the client ID as Thing Name.

Certificate (AWSIoT):

Specify the device certificate file used when sending data to AWSIoT.

Privatekey (AWSIoT):

Specify the privatekey file for the device used when sending data to AWSIoT.

Device type (Watson IoT/Device):

Specify the device type when sending data to Watson IoT for device.

Device (Watson IoT/Device):

Specify the device ID when sending data to Watson IoT for device.

Password (Watoson IoT/Device):

Specify the device type when sending data to Watoson IoT for device, if necessary.

Device type (Watoson IoT/Gateway):

Specify the device type when sending data to Watoson IoT for gateway.

Device ID (Watoson IoT/Gateway):

Specify the device ID when sending data to Watoson IoT for gateway.

Event hubs name (EVENTHUB):

Specify the Event hubs name when sending data to Event hubs.

Sas policy (EVENTHUB):

Specify the SAS policy when sending data to Event hubs.

Sas key (EVENTHUB):

Specify the SAS key when sending data to Event hubs.

Device ID (IoT Hub):

Specify the Device ID when sending data to IoT Hub.

Device key (IoT Hub):

Specify the Device key when sending data to IoT Hub.

Gateway Name (T4D):

Specify the Gateway name when sending data to Toami for docomo.

App key (T4D):

Specify the App key when sending data to Toami for docomo.

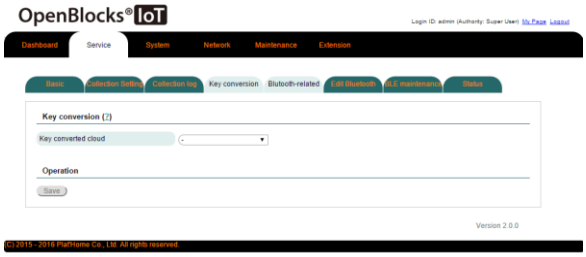
Unique ID (MQTT):

Specify the unique ID when sending data to the MQTT server. The unique ID is treated as the topic suffix. The topic prefix is set to the MQTT server. The prefix and the suffix are separated with a slash (/) and sent.

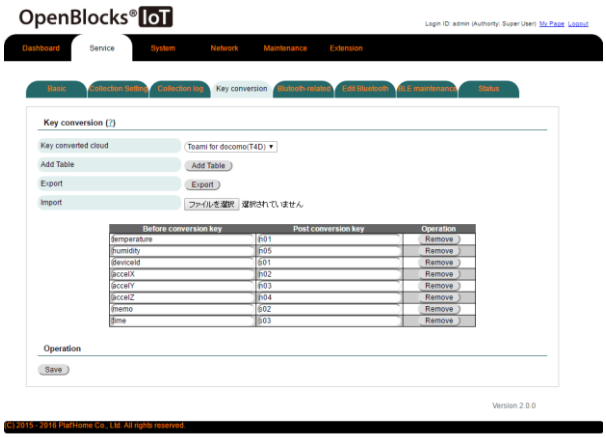
* Information linked with cloud settings can be edited with the Edit button. It is recommended to use the same settings when replacing the device due to failure or other reason to handle the new device in the same way as the old device. (For the failed device, change [Transmission target] to [Do not send].)
* Upload the certificate file and privatekey file from [System] ⇒ [File management] tab.

2-2. Key conversion

If you want to send the data to the Toami for docomo, you must convert key infomation on the payload.



*sample



Key conversion :

Key converted cloud :

Select the cloud for which you want to set the key conversion. In the current situation it will support only "Toami for docomo".

Add Table :

Add a row of tables for the conversion.

Export :

Export the conversion table to the local PC.

Import :

Import the conversion table from the local PC.

Before conversion key :

Specify the JSON key in the payload to be converted from.

Post conversion key :

Specify the JSON key after the conversion corresponding to the pre-conversion key.

Please press the save button after the completion of the conversion information.

In addition, please check the documentation from the following URL for information on JSON key to convert from.

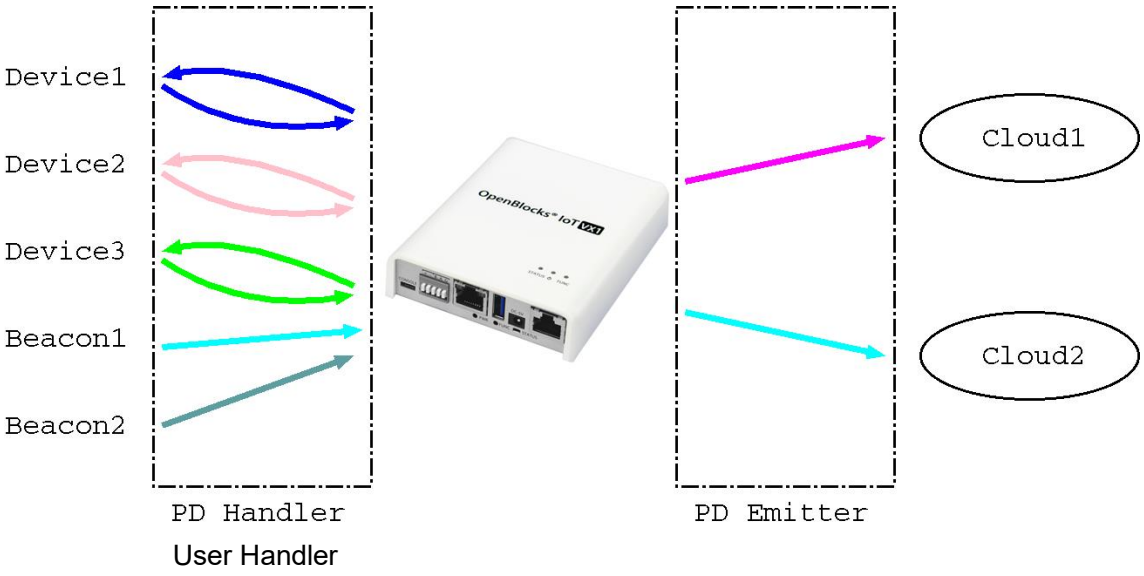
https://docs.google.com/a/plathome.co.jp/document/d/1WR6iy2wpONXX7gFOptZ8NTklzw1yeW58mhIPFGdyqB4/edit?usp=sharing

Chapter 3 Support of Your Own Device Linkage Application

This chapter describes the case when you use your own application to acquire data from each device or other source instead of using the application (PD handler) provided by us in the data acquisition function in the OpenBlocks IoT VX1.

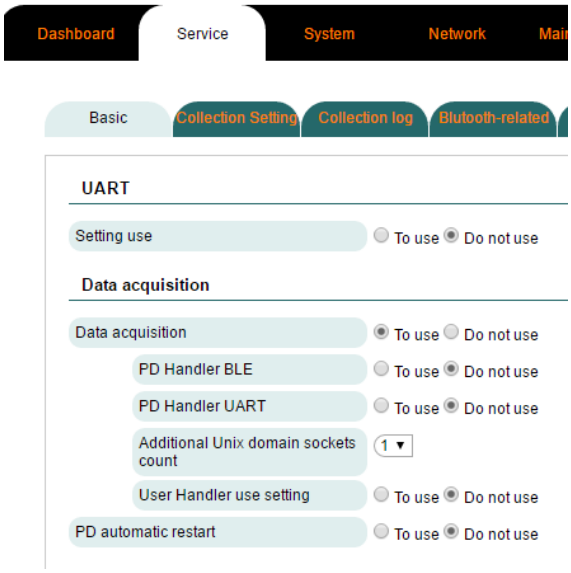
The applications that users to provide their own, is called the **User Handler** in our product.

A configuration image is as shown below.



3-1. WEB UI Settings

Specify the settings at [Service] ⇒ [Basic] tab on the Web UI.

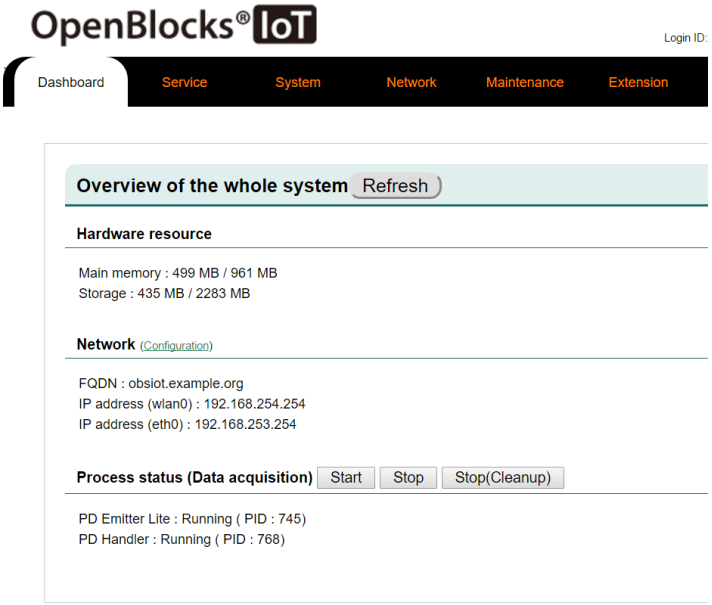


Normally, the following should be displayed when you acquire data.

To use your own application to acquire data from devices in this status, as following.

1. Set number of the [Additional Unix domain sockets count].
2. Select [Do not use] for [PD Handler BLE], if not used.
3. Select [Do not use] for [PD Handler UART], if you have any extended additional module but not used.
4. Select [Do not use] for [User Handler use setting at this moment, See chapter 3-3.

When you check the dashboard after saving data, the process status of PD Handler becomes "Stopped" as shown below.

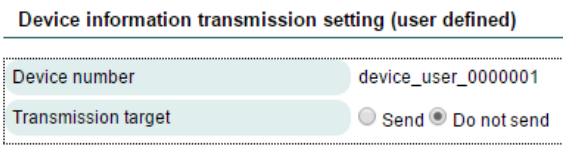


This means that only PD Emitter is operating.

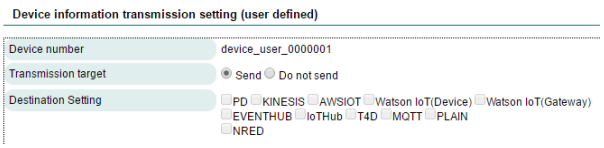
The settings for PD Emitter remain the same as [Service] ⇒ [Collection Settings].

3-2. Device Information Transmission Setting (User Defined)

Specify the settings at [Service] ⇒ [Collection Setting] tab on the Web UI.



If you set the number of the Additional Unix domain sockets count to one or more in the previous section, will be displayed the input items as shown on the left.



When you select [Send], each item appears as shown in the left screenshot.

Device number:

Number managed on the Web UI in the OpenBlocks IoT Family. This number cannot be changed.

Destination Setting:

The check boxes corresponding to the destinations for which "Use" is selected become selectable.

Data is sent to the cloud and other destinations whose check boxes are selected.

Device id suffix (PD):

Specify the device ID suffix when sending data to PD Exchange.

Client ID (AWSIoT):

Specify the client ID when sending data to AWSIoT. It does not duplicate with other client ID that use the same destination. When Thing Shadows is used, the client ID is Thing Name.

Thing Shadows (AWSIoT):

Select whether to use Thing Shadows when sending data to AWSIoT.

Topic name (AWSIoT):

Specify the topic when sending data to AWSIoT. When Thing Shadows is used, the topic is automatically generated using the

*Sample

client ID as Thing Name.

Certificate (AWSIoT):

Specify the device certificate file used when sending data to AWSIoT.

Privatekey (AWSIoT):

Specify the privatekey file for the device used when sending data to AWSIoT.

Device type (Watson IoT/Device):

Specify the device type when sending data to Watson IoT for device.

Device (Watson IoT/Device):

Specify the device ID when sending data to Watson IoT for device.

Password (Watoson IoT/Device):

Specify the device type when sending data to Watoson IoT for device, if necessary.

Device type (Watoson IoT/Gateway):

Specify the device type when sending data to Watoson IoT for gateway.

Device ID (Watoson IoT/Gateway):

Specify the device ID when sending data to Watoson IoT for gateway.

Event hubs name (EVENTHUB):

Specify the Event hubs name when sending data to Event hubs.

Sas policy (EVENTHUB):

Specify the SAS policy when sending data to Event hubs.

Sas key (EVENTHUB):

Specify the SAS key when sending data to Event hubs.

Device ID (IoT Hub):

Specify the Device ID when sending data to IoT Hub.

Device key (IoT Hub):

Specify the Device key when sending data to

IoT Hub.

Gateway Name (T4D):

Specify the Gateway name when sending data to Toami for docomo.

App key (T4D):

Specify the App key when sending data to Toami for docomo.

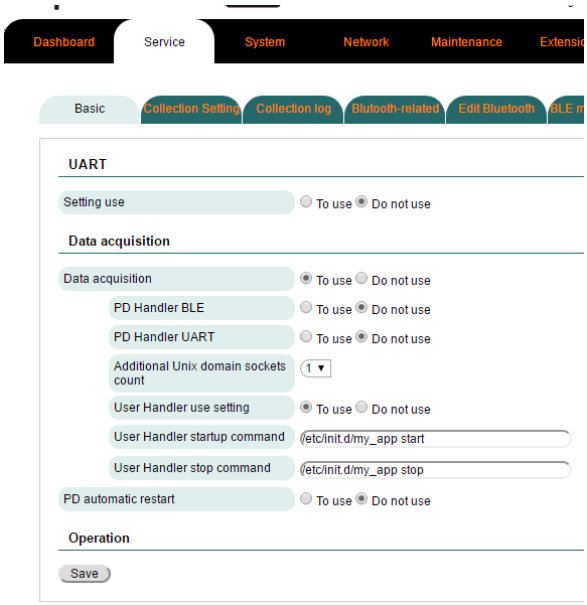
Unique ID (MQTT):

Specify the unique ID when sending data to the MQTT server. The unique ID is treated as the topic suffix. The topic prefix is set to the MQTT server. The prefix and the suffix are separated with a slash (/) and sent.

* Information linked with cloud settings can be edited with the Edit button. It is recommended to use the same settings when replacing the device due to failure or other reason to handle the new device in the same way as the old device. (For the failed device, change [Transmission target] to [Do not send].)
* Upload the certificate file and privatekey file from [System] ⇒ [File management] tab.

3-3. Configure for User Handler

Specify the settings at [Service] ⇒ [Basic] tab on the Web UI.



Configure for User Handler.

User Handler use setting：

Select whether to use the User Handler.

If enable this item, execute the commands which will be described below in linkage with the PD Emitter.

User Handler startup command：

Specify the start-up command for User Handler.

Please note that the User Handler must be a background process such as DAEMON.

Please run covered with a shell script as a wrapper in the case of using a plurality of Handler.

User Handler stop command：

Specify the stop command for User Handler.

Please note that there is a need to stop the background process such as DAEMON.

3-4. Writing Data from Your User Handler into PD Emitter

PD Emitter creates Unix domain sockets in the abstract namespace (abstract) based on the device number you specified on the Web UI. (Unix domain sockets are created for devices for which [Send] is set to [Transmission setting] and the destination is enabled and not local.)
When you write data into this Unix domain socket, written data is sent to the cloud.

The following is a sample where "MessageText" is individually written into the Unix domain socket in PD Emitter.

A sample where data is written from the command line is as shown below.

*When writing data as device_beacon※1

```
# echo -n "MessageText" | socat stdin abstract-connect:/pd_emitter_lite/device_beacon.sock
```

A script sample in PHP is as shown below.

*When writing data as device_beacon

```
<?php
  $socket = stream_socket_client("unix://¥0/pd_emitter_lite/device_beacon.sock", $errno, $errstr);
  if (!$socket) {
    echo "ERROR : " . $errno ." " . $errstr . "¥n" ;
  } else {
    fwrite($socket, "MessageText");
    stream_socket_shutdown($socket, STREAM_SHUT_RDWR);
  }
⇒
```

A script sample in Node.js is as shown below.

*When writing data as device_beacon※2

```
var absocket = require('abstract-socket');
```

※1 The socat command is not installed. Install this command with apt-get install socat.
※2 npm and abstract-socket are not installed. Install them with curl https://npmjs.org/install.sh | sudo sh and npm install abstract-socket.

```
try {
        var absclient = absocket.connect('¥0/pd_emitter_lite/device_beacon.sock', function() {
                console.log('connect ok');
        });
        absclient.write("MessageText ");
        absclient.end();
} catch(e) {
        console.log('fail');
}
process.exit();
```

As shown above, when you write data in the Unix domain socket, the socket becomes the buffer of PD Emitter.
Write data in the Unix domain socket as show above when you control the device or perform other process with your own application.

Chapter 4 Notes

4-1. Data Transmission Amount and Line Speed

If the data rate is slow in comparison with the amount of information acquired from beacons and devices, information accumulates in the buffer in the OpenBlocks IoT Family. Information continues to accumulate unless you improve the data transmission section. So, check buffer data and adjust the interval, acquisition time interval and other settings.
*The buffer file size can be checked at [Service] ⇒ [Status] tab.

4-2. Format when Writing Data into PD Emitter

PD Emitter only supports JSON data when sending data to each cloud.
Up to 4096 bytes can be written into PD Emitter.
Check the message size restriction on each cloud because this restriction is separately set on each cloud.

4-3. Buffer Size of PD Emitter

PD Emitter writes data in the DB as buffer to temporarily accumulate data as transmission buffer. The default upper limit of DB size is 16 Mbyte. If this size is exceeded, new data is discarded and data is no longer received until the DB size drops below 8 Mbyte.

4-4. Retransmission if PD Emitter Encounters an Error

PD Emitter may fail to send data to the cloud depending on the network communication status. The retransmission process starts five minutes after PD Emitter may continue to fail to send data or if an unexpected error occurs.

4-5. Configuration of User Handler

The ability to create a configuration file for the application that you created in the user side is not. If you need to save the configuration file that you created, please use the file upload function.

4-6. Payload Format of the Toami for docomo

Payload format to be transmitted to the Toami for docomo in PD Emitter will be only JSON. If the format of the non-JSON input to the PD Emitter, will result in an error. In addition, payload that caused the error, please note that it is treated as the transmitted data.

4-7. For data transfer method to the Node-RED

Data from the PD Emitter to Node-RED in the local will be via Unix domain sockets. The path of the Unix-domain socket on which the PD Emitter writes in the respective data will be as following.

<Socket path prefix>/<Device Number>.sock

Socket path prefix: ; Specified by [node red(NRED)] section in the [Service] ⇒ [Collection Setting] tab. See section 2-1-1.

Device Number: Indicated in each transmissin settings section in the [Service] ⇒ [Collection Setting] tab.

4-8. For additional beacon device as BLE device

Sensors and beacon device set as the transmission object registered as a BLE device to WEB UI will be treated individually. In this case, in particular beacon device eliminates the dependence of the transmission settings of the beacon. Therefore, control type of beacon transmission setting, no data filter, etc. are applied. In addition, the data to be passed to the PD Emitter of the sensor with a beacon that support is, it will be parsed sensor data. However, in the case of normal beacon to pass the time and device ID, memo information to the PD Emitter.

Plat'Home Co., Ltd.
Nihon Building Kudan Bekkan 3rd floor, Kudan-kita 4-1-3, Chiyoda-ku, Tokyo, 102-0073, Japan