Plat'Home
TECHNOLOGY to serve you.

OpenBlocks IoT VX1
Web UI Setup Guide

Ver. 2.0.0

Plat'Home Co., Ltd.

■ About trademarks

- Linux is a trademark or registered trademark of Mr. Linus Torvalds in the U.S. and other countries.
- Firefox is a registered trademark of Mozilla Foundation in the U.S. and other countries.
- Google Chrome is a registered trademark of Google Inc.
- Internet Explorer is a registered trademark or trademark of U.S. Microsoft Corporation in the U.S. and other countries.
- NTT DOCOMO is a registered trademark of Nippon Telegraph and Telephone Corporation.
- SoftBank and its name and logo are registered trademarks or trademarks of SoftBank Group Corp. in Japan and other countries.
- au (KDDI) is a registered trademark or trademark of KDDI CORPORATION.
- 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.

⚠ CAUTION	⊘	Use specified batteries only.*2 There are risks of leakage, explosion or fire.
	❗	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 9
1-1. Contents of VX1 Package 9
1-2. Name of Each Section (VX1 Main Unit) 10
1-3. Status Indicator 12
Chapter 2 Before Use 13
2-1. About the SIM 13
2-2. Installation of OpenBlocks IoT Family 13
2-3. Preparing a Web Client 14
Chapter 3 Basic Initial Setup of Web UI 16
3-1. License Screen 17
3-2. Administrator Account (Web UI Administrator Account) Settings 17
3-3. Network Settings Screen 18
3-3-1. Mobile Router Configuration 19
3-3-2. Server Configuration 23
3-3-3. Advanced Settings of Wi-Fi AP Mode (CH setting and International Use) 25
3-4. Internal Clock Setting 26
3-5. Applying Setting Items by Rebooting the System 28
3-6. Administrator Login Screen 29
3-7. Dashboard Screen 29
Chapter 4 SMS Control 30
4-1. SMS Control Startup Settings 30
4-2. SMS Control Commands 31
4-3. Sending Multiple Commands with SMS 31
4-4. Registering an SMS User-Defined Script 32
4-5. Direct Execution of SMS Control Commands 33
Chapter 5 Items Related to Bluetooth Device 34
5-1. Starting the Bluetooth Service 35
5-2. Paring with the Bluetooth Device 37
5-3. Editing Registered Devices and Memo 38
5-4. Data Acquisition Settings 39
5-5. Linkage between PD Exchange, Applications, and Devices 40
5-6. Checking the Collection Log 41
5-7. Checking Sensor Data 42
5-8. Exporting or Importing BLE Device Setting Information 43
Chapter 6 Serial Communication Redirection Function 45

6-1. Serial Communication Redirection Function in the SPP Device 45
6-2. RS-232C Serial Communication Redirection Function..... 49
Chapter 7 Reference by Setting Item 50
7-1. Displaying and Hiding the Service Control and Extension Functions 50
7-2. Function assignment to the FUNC switch..... 51
7-3. Process Status Display Function 52
7-4. Storage Alert Function 53
7-5. Setting the Root Password 54
7-6. Filter Permission..... 55
7-7. SSH Key Exchange 56
7-8. Changing the Web Administrator Password..... 58
7-9. WEB User 58
7-10. File Management 59
7-11. Displaying the Software License..... 60
7-12. Checking the Main Unit Serial Number 61
7-13. Dynamic DNS..... 62
7-14. Adding Static Routing..... 63
7-15. Communication Check..... 63
7-16. Network Status Check..... 64
7-17. Backing up and Restoring Configuration..... 65
7-18. Updating System Software..... 66
7-19. Register EnOcean device 67
7-20. SMS Transmit 68
7-21. Using Node-RED..... 69
7-22. SSH Revers tunnel..... 70
7-23. Support Information 71

Chapter 1 Introduction

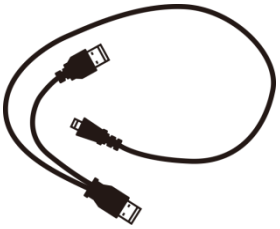
This document describes how to set up the OpenBlocks IoT VX1 on the Web user interface (called Web UI below). A client device in which a web browser can be used (such as PC, smartphone, or tablet) is required for this setup.

1-1. Contents of VX1 Package

The standard configuration of the OpenBlocks IoT VX1 is as shown below.

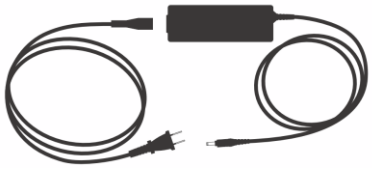
BX1 main unit x 1

USB console cable for debug x 1

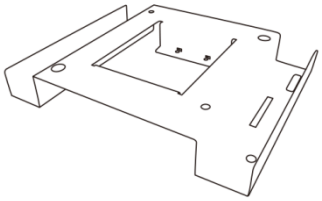


User's Guide x 1

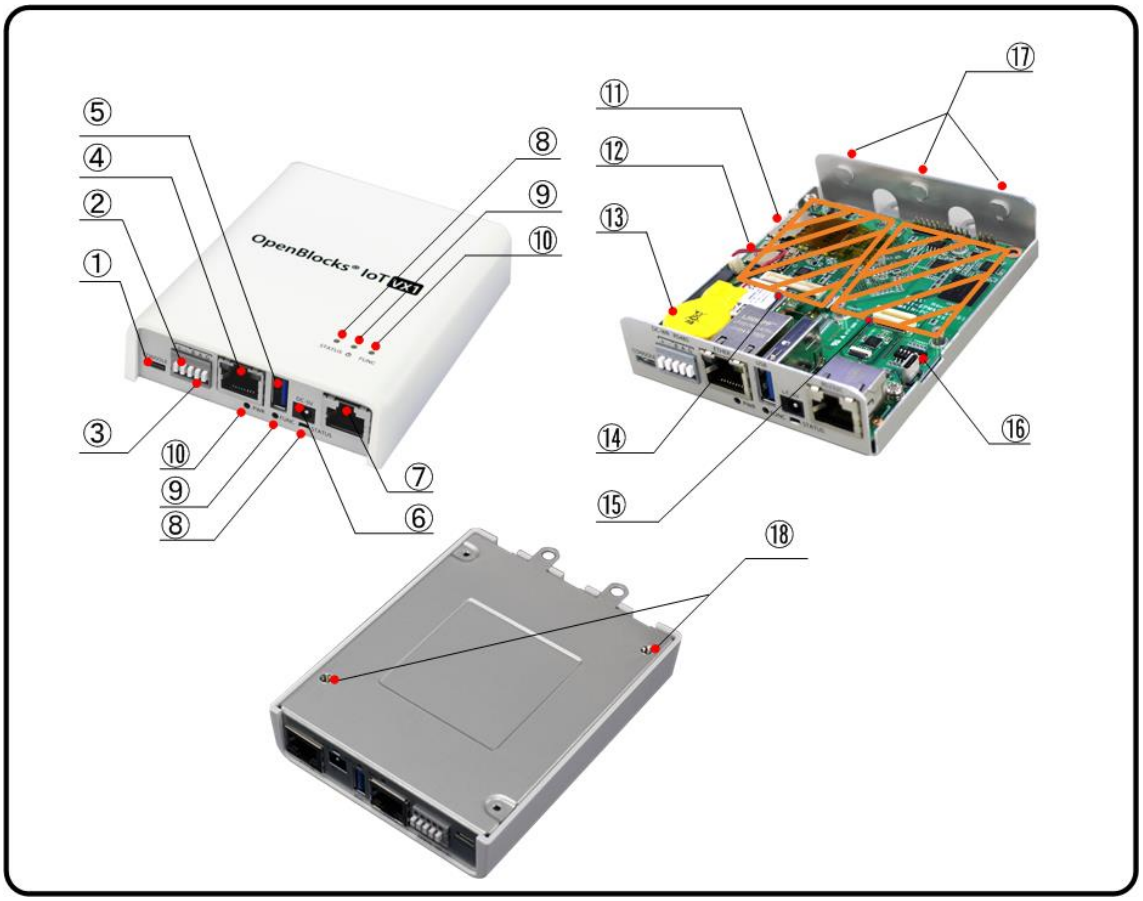
AC adapter x 1



Bracket x1



1-2. Name of Each Section (VX1 Main Unit)



No.	Name	Description
①	USB serial console port	Micro USB typeB
②	Wide-range power supply terminal block	10 to 48 VDC supported.
③	RS-485 (half-duplex) terminal block	
④	Ethernet port	10Base-T/100Base-TX/1000Base-T Auto-MDX compatible
⑤	USB host mode port	A-Type / USB3.0
⑥	Dedicated AC adaptor input	5 VDC
⑦	RS-232C port	RJ-45. The connector to connect the D-Sub9 pin is optionally available. A general straight network cable can be used for

No.	Name	Description
		connection.
⑧	Status indicator	The LED lights up or flashes in seven colors.
⑨	Power switch	Power on and boot the OS. Shutdown the OS and power off, if during operation.
⑩	FUNC switch	OS specified function will work.. See also section 7-2.
⑪	SIM slot	Slot which you insert the SIM into. * The shape of the supported SIM is mini-SIM (2FF) (standards generally called standard SIM).
⑫	SD card slot	Use the SD card for file exchange, log storage or other purpose because the SD card cannot ensure sufficient reliability for system operation.
⑬	RTC battery holder	Coin type lithium battery (CR2032) connected.
⑭	Expansion slot 1	Expansion slot for mobile adaptor card for mobile line. Attach the mobile adaptor card that supports your carrier. In principle, this is a factory option.
⑮	Expansion slot 2	Expansion slot for EnOcean, Wi-SUN module and so on.
⑯	DIP switch	Normally, do not change these settings. They are configured at the factory.
⑰	External antenna mounting hole	Filled in the image.
⑱	Braket mounting hole	

* To insert the SIM, reverse the VX1 main unit and insert the SIM until the end of the SIM slot. Likewise, reverse the VX1 main unit when removing the SIM.

1-3. Status Indicator

The status indicator of this device displays the statuses with the LED in seven colors.
The table below shows how the indicator shows each status.

Status	Color	Lighting state	Remark
BIOS starting up	Yellow	On	When the startup of the BIOS is complete, migrate to OS starting up status.
OS starting up	Yellow	On	When the OS starts up is complete, radio reception check for the mobile line starts. * The LED flashes in green if the SIM is not inserted.
When the SIM slot is not in use	Green	Flash	Normal operation if the SIM is not in use, or wait for checking the status of radio field.
Mobile line radio field: Strong	White	Flash	Radio field strength of -87 dBm or more in 3G line. For 4G line, corresponds to the display of the antenna two or three of the mobile phone.
Mobile line radio field: Middle	Light blue	Flash	Radio field strength of -88 to -108 dBm in 3G line. For 4G line, corresponds to the display of the antenna one or two of the mobile phone.
Mobile line radio field: Weak	Blue	Flash	Radio field strength: -109 to -112 dBm in 3G line. For 4G line, corresponds to the display of the antenna zero or one of the mobile phone. * Communication may be retried many times with this radio field strength. Therefore, use the medium or strong radio field strength when using the mobile line as much as possible.
Mobile line radio field: No service	Purple	Flash	Radio field strength of -113 dBm or less in 3G line. For 4G line, indicating that it is out of service.
During process any function which assigned FUNC switch.	Yellow	Flash	It will be the status indicator and flash alternately in mobile line or SIM slot when not in use.
During OS shutdown	Yellow	On	You must hold down the INIT switch until the LED goes out.

* Radio status indication of 4G line is different for each mobile module.

Chapter 2 Before Use

2-1. About the SIM

The OpenBlocks IoT VX1 supports mini-SIM (2FF) as the SIM shape. When using the micro-SIM or nano-SIM, use the adaptor that can fix the SIM with the fall prevention film or adhesion tape. For reference, repair is charged if the SIM slot is corrupted when the SIM adaptor is used.

2-2. Installation of OpenBlocks IoT Family

The OpenBlocks IoT VX1 using the supplied AC adapter to connect as following.
* Power operation in other than the supplied AC adapter or a wide range power input will be unsupported, Please note.

The status indicator lights up or flash when the device becomes ready for use.
(The display color differs depending on the status at that time.)

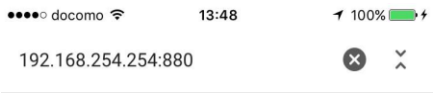
2-3. Preparing a Web Client

A web client is required to access the Web UI for this device.

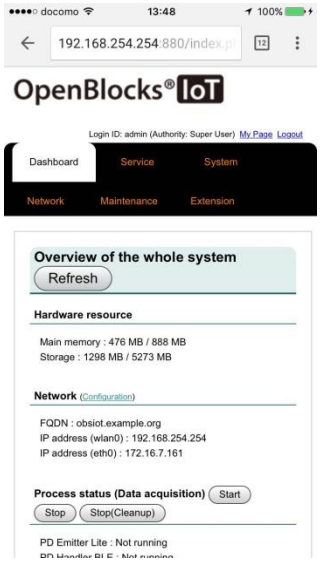
The PC, tablet, or smartphone that can be connected to Wi-Fi can be used as a web client. Select the access point (SSID) of this device as the Wi-Fi setting for the web client and connect it.

The right screenshot shows the smartphone screen where the SSID(iotfamily_"the serial number of the main unit") of this device is selected from the Wi-Fi SSID list. You can connect to Wi-Fi by entering the default password at shipment: openblocks.

Once you connect to Wi-Fi, access the following address using the web browser:



When the SSID is selected



Web screen

* The serial number of the main unit is shown on the back of the housing.

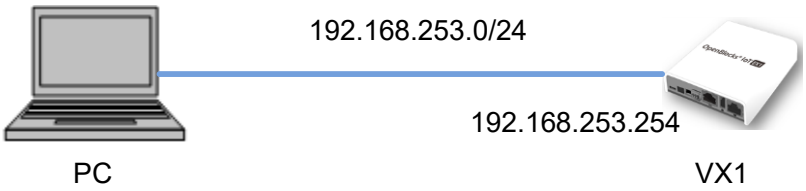
- Connections with HTTP
  http://192.168.254.254:880

- Connections with HTTPS
  https://192.168.254.254:4430

Immediately after running with this product, access in Wi-Fi are subject to authentication error. It will be connected by performing a re-connection after a few tens of seconds.

This product has a wired interface is supported. To use a wired network for connection and perform initial setup, specify the IP address of your PC to access the 192.168.253.0 network and access the following address using the web browser:

http://192.168.253.254:880 or https://192.168.253.254:4330.



* The web browsers supported as the web client on the PC are the latest versions of Google Chrome and Firefox. Internet Explorer is not supported.

Chapter 3 Basic Initial Setup of Web UI

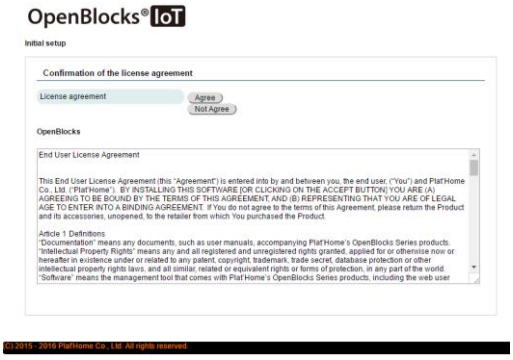
This document uses the web screen on the PC for description purposes, moreover Both the pc and the smartphone can be used to access the WEB GUI for the setup.

The procedures in Sections 3.1 to 3.3 are necessary only when the device is in initial default condition. In other cases, refer to the procedures written in Section 3.4 and beyond. The part until Section 3.3 describes the minimum necessary procedures for initial setup of this device as well as mobile router settings and the minimum network settings for the standalone server.

Attension)

Setting the administrator account in Section 3.2, which has been carried out in this chapter is important for security. Therefore, please set the made such a password difficult to crack.

3-1. License Screen

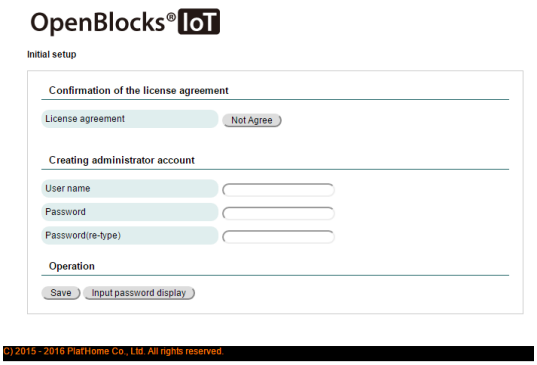


The license contract screen for this device appears immediately after shipment before this device is set up.

You may use this device only after agreeing to this license.

Scroll the screen, check the contents of the contract, and select [Agree] to go to the next screen.

3-2. Administrator Account (Web UI Administrator Account) Settings



When you agree to the license contract, the screen to enter the Web UI administrator account and password opens.

Caution) Administrator account

Be careful not to enter a wrong user name for the administrator because this cannot be changed later. Note that this account has the privilege to change the password of the root user.

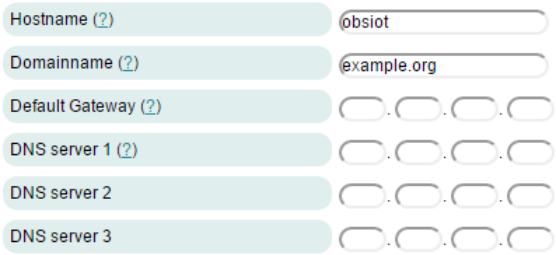
Specify account information and click the [Save] button. The first configuration information is written. When the configuration is written, the screens in sections 3.1. and 3.2. no longer appear from the next access. The administrator login screen first appears when you access the web.

3-3. Network Settings Screen

You must perform the minimum settings on the network settings screen to use OpenBlocks IoT.

You can select configuration using this device as the mobile router and configuration using this device as the server device without using the mobile line when setting up the network.

There is a field to enter this device name at the top of the [Basic] tab on the network settings screen as shown in the screenshot below.



Hostname:

Name of this device as server.

Domainname:

Network domain name which this device belongs to.

Default Gateway:

You do not have to specify this item when dynamically acquiring the IP with DHCP.

DNS server 1 - 3:

You do not have to specify these items when dynamically acquiring the IP with DHCP.

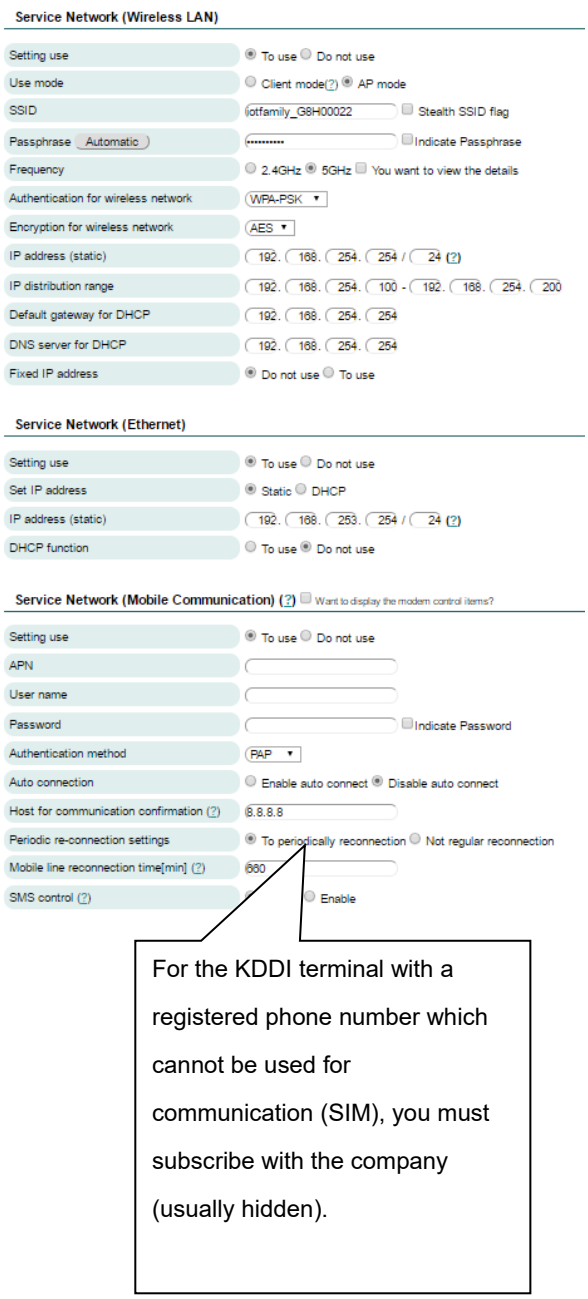
Specify at least one DNS server when specification is required. It is recommended to specify two or more servers.

The setting procedures are different in the following sections depending on whether you select 3-3-1. Mobile Router Configuration or 3-3-2. Server Configuration.

The setting screen is the same as the above screenshot. Description of the setting items below it is different.

3-3-1. Mobile Router Configuration

This section describes the setting procedure when using this device as the mobile router.



For the KDDI terminal with a registered phone number which cannot be used for communication (SIM), you must subscribe with the company (usually hidden).

<u>Service Network (Wireless LAN)</u>

Setting use:[*1]

Select [To use].

Use mode:

Select [AP mode].

Frequency:

Select [2.4GHz] or [5GHz].

SSID:

Enter an arbitrary access point name.

To hide the SSID from general users, select the [Stealth SSID flag] check box.

Authentication for wireless network: and **Encryption for wireless network:**

Select an arbitrary mode from the pull-down menu. You can use default settings as is.

Passphrase: (security key)

Specify eight or more characters.

IP address:

Enter the IP address and the number of the bits of netmask of this device for Wi-Fi.

IP distribution range:

Specify the IP address distribution range to operate as the DHCP server.

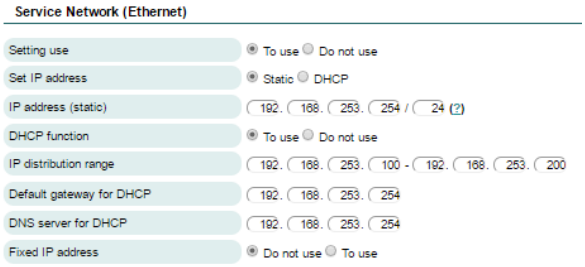
Default gateway for DHCP:

DNS server for DHCP:

Specify the IP addresses of default gateway and DNS notified to the DHCP client.

Fixed IP address(static):

Specify this item for use when distributing the fixed IP.



Service Network (Ethernet)

Setting use:

Select [To use] only when using this network.

Set IP address:

Specify the IP address set to the Ethernet. When you select [Static], the following item appears.

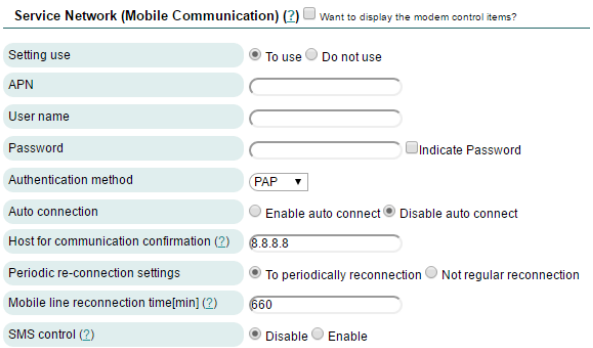
IP address (static):

When using a static address, specify the IP address in this field.

DHCP function:

Select [To use] when using the DHCP function as in the service network (wireless LAN).

Setting items are also [Default gateway for DHCP], [DNS server for DHCP], and [Fixed IP address].



Service Network (Mobile Communication)

You do not have to select the [Want to display the modem control items?] check box.

Setting use:

Select [To use].

APN: *This item is not displayed for the KDDI version.

Specify the APN specified by your carrier.

User name:

Specify the user name specified by your carrier.

Password:

Specify the password specified by your carrier.

Authentication method:

Specify the authentication method specified by your carrier.

Auto connection:

When you select [Enable auto connect], the device automatically connects to the mobile line at startup.

Host for communication confirmation:

Specify the host. This device confirms by the host that the mobile line is connected to the Internet or other network.

***Communication is not confirmed when 127.0.0.1 is set to this item.**

Periodic re-connection settings:

A mobile line to set whether to periodically re-connection.

Mobile line reconnection time [min]:

Disconnection and connection is automatically performed when the time specified with this item elapses after the mobile line is connected.

SMS control:

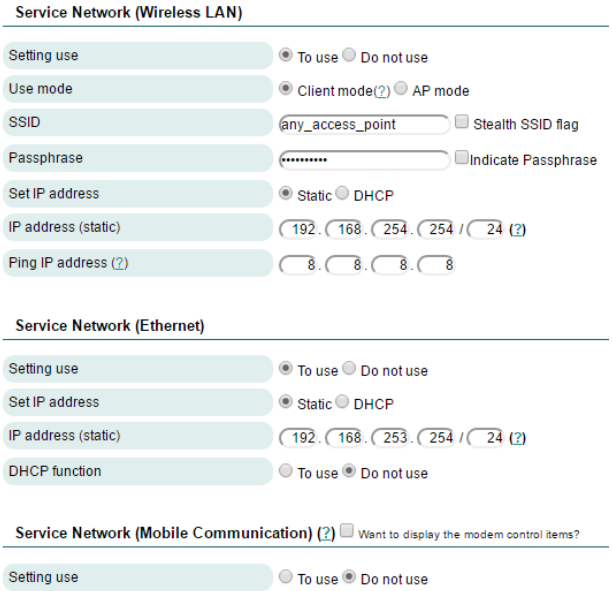
Specify [Disable] here.

After completing the above setup, click the [Save] button.

When you click the [Save] button, the settings are saved and the network settings are applied after reboot. Then, go to 3-4. Internal Clock Setting.

3-3-2. Server Configuration

This section describes the setting procedure when using this device as the standalone server in the network.



Service Network (Wireless LAN)

Setting use:[*1]

Select [To use].

Use mode:

Select [Client mode].

SSID:

Enter the SSID of access point to be connected. To connect to the stealth SSID, select the [Stealth SSID flag] check box.

Set IP address:

Select [Static] or [DHCP].

When you select [DHCP], set up the DHCP server to distribute the fixed IP to this device.

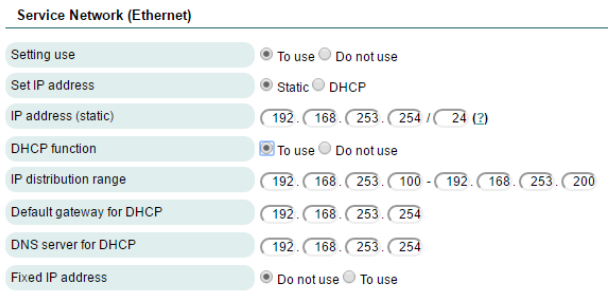
IP address (static):

When the IP address setting is static, enter the IP address.

Ping IP address:

Enter the IP or FQDN of the server to which this device pings to monitor the Wi-Fi connection status.

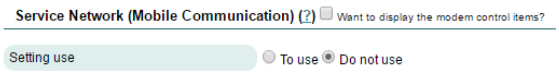
Specify the device that can respond to ping at the upstream of Wi-Fi network.



Service Network (Ethernet)

Select [To use] for [Setting use] only when using these settings. When using a static address, specify the IP address.

You must specify each item when using the DHCP function.



Service Network (Mobile Communication)

You do not have to select the [Want to display the modem control items?] check box.

Setting use:

Select [Do not use].

* The [Want to display the modem control items?] check box is the function for developer. Therefore, check the Developer's Guide.

After specifying the above necessary items, click the [Save] button and go to 3-4. Internal Clock Setting.

Action if you enter an incorrect SSID and reboot the device

If you register the SSID of nonexistent upstream access point in this section, you can no longer access this device with the general method.
In this case, initialize and restart Openblocks IoT VX1.

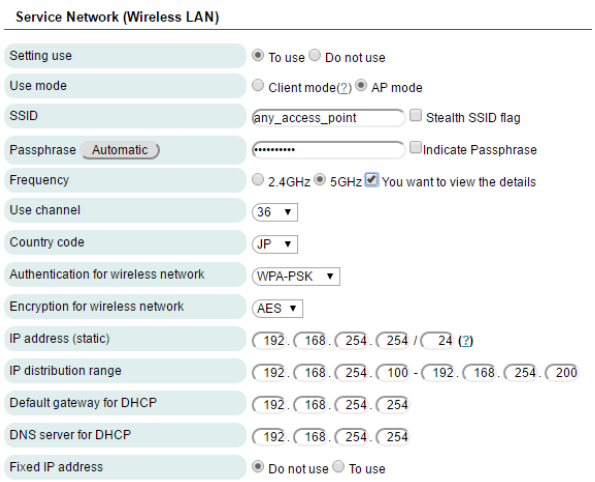
1. Connect PC with USB console cable.
2. Run terminal software in PC to get serial console of Openblocks IoT VX1.
3. Press the power switch of Openblocks IoT VX1 to shutdown.
4. Press the power switch of Openblocks IoT VX1 to boot.
5. Select 'WebUI init boot' at GRUB menu in serial console.
6. This device starts up in the status at shipment.
7. Set up this device again and reboot it.

* If session information of WEB UI remains in the browser, it will remain as it was in the previous state. Therefore, log out and re-access, please set again from the use permission screen.

With the above procedure, you can recover the device.

3-3-3. Advanced Settings of Wi-Fi AP Mode (CH setting and International Use)

You can change the channel to address radio wave interference and specify the country code to use the Wi-Fi AP mode outside Japan.



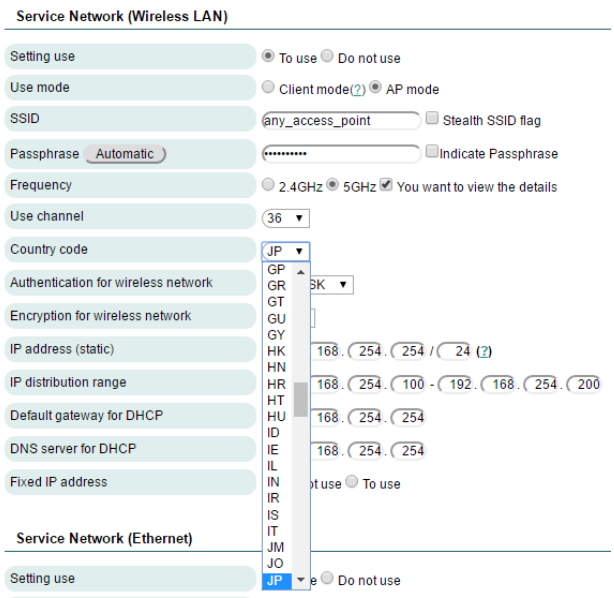
Service Network (Wireless LAN)

Setting use:

Select [AP mode].

When you select [AP mode], the [You want to view the details] check box appears at the right of [Frequency].

When you select this check box, [Use channel] and [Country code] setting items appear.



Use channel:

Select an arbitrary channel from the pull-down menu. To find an empty channel, the apps such as Wi-Fi channel analyzer for smartphone are useful.

Country code:

Specify the country code of the country where you install this device.

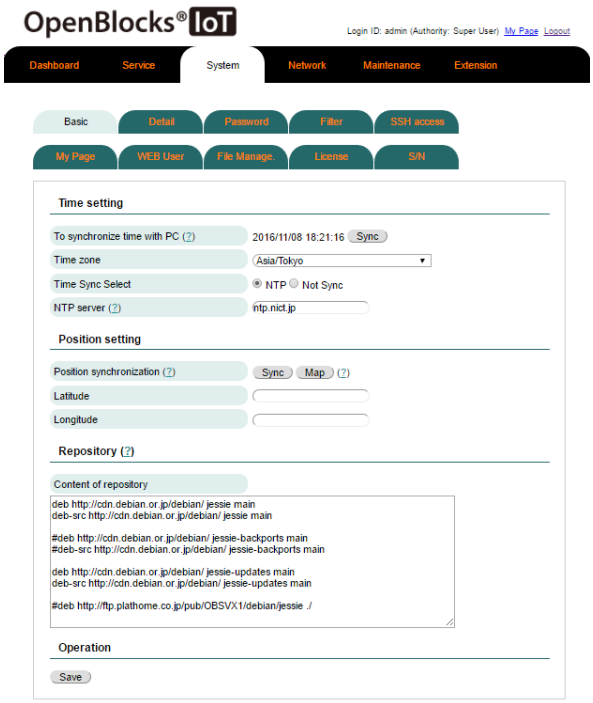
Currently, you can select the country codes of countries where the W52 band is supported from the pull-down menu.

The country code of Japan is [JP].

3-4. Internal Clock Setting

This product is equipped with RTC backup battery. However, time synchronization with the NTP server is recommended.

For operation in the environment where the NTP server cannot be used, you can synchronize the time of PC or smartphone that displays the Web UI of this device on the web browser.



Time setting

To synchronize time with PC:

Clicking the [Sync] button applies the time of the PC that displays the web.

Time zone:

Select the region where you install this device.

Time Sync Select:

Select the time synchronization method. Normally specify NTP. When the G4 comunication module is installed, the “Mobile modem” item is displayed and it is possible to synchronize the time from the modem. (SIM card must be inserted and correct APN setting is required.)

NTP server:

Enter the IP address or FQDN of NTP server.

Position setting

Position synchronization:

Pressing the Sync button will reflect the location information held by the browser. (This function needs to be implemented by HTTPS connection.)

When you press the map information button, the location information is displayed on GoogleMap.

Latitude:

Specify latitude.

Longitude:

Specify longitude.

Repository information

Content of repository:

The repository for update information of software of this device is displayed. The information cannot be edited on this screen.

To edit the information, log in to the CUI with SSH or other protocol and edit the /etc/apt/sources.list file.

(You must manage the edited result at your own risk.)

Settings are saved when you click the [Save] button after editing them. Although it is basically not necessary to reboot the device, reboot is recommended to apply the time zone information and other settings to your applications.

These are basic setting items required to operate this device.

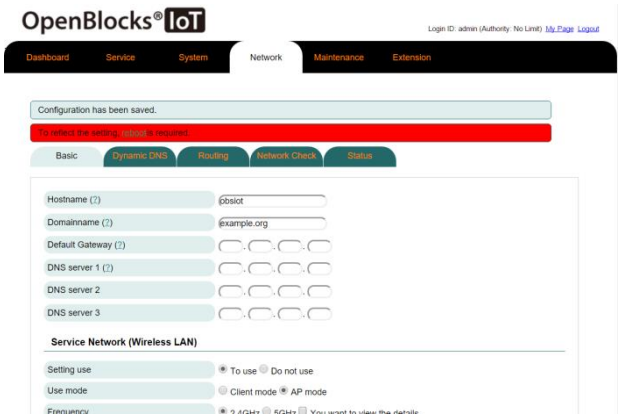
After completing setup, reboot the system as described in the next section.

3-5. Applying Setting Items by Rebooting the System

We have seen the minimum setting items required to operate this device so far.

For other setting items, see their description as needed.

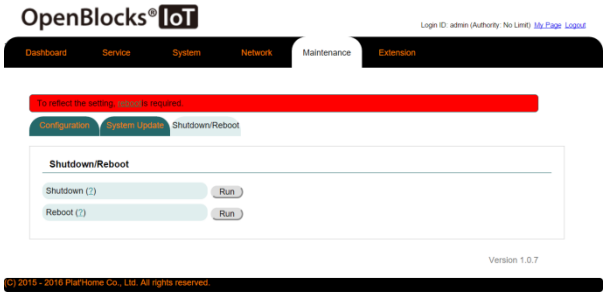
This section describes system reboot to apply settings to the system after specifying basic network settings.



When you click the [Save] button after specifying basic network settings, the message prompting for system reboot appears at the top of the web screen as shown in the left screenshot.

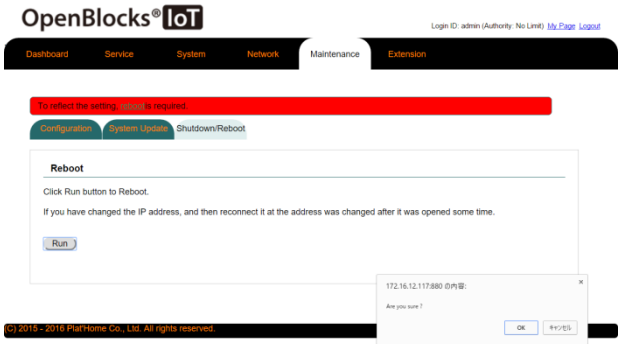
To reboot the system, click the [reboot] link in this message in the red box. When you click this link, the Shutdown/Reboot tab in the Maintenance menu appears.

Click the [Run] button for [Reboot] on this screen.



When the reboot confirmation screen appears, click the [Run] button. The final confirmation window pops up.

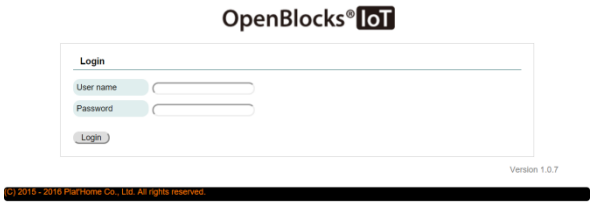
This is the final confirmation. When you click the [OK] button, the system starts rebooting.



Although the reboot time depends on the system status, wait for several seconds as displayed.

When you access the Web UI through wireless network and this device is in the AP mode, connection to this device is established again after reboot. To display the login screen after reboot is complete, you need the reload operation from the web browser.

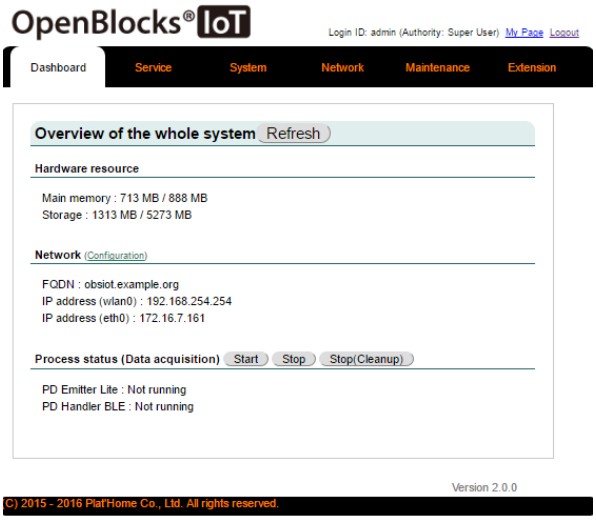
3-6. Administrator Login Screen



This is the screen first displayed unless this device is in the status immediately after shipment.

After you log out, you start the operation with this screen. Log in to the device on this screen.

3-7. Dashboard Screen



This is the screen first displayed when you log in to the Web UI of this device.

This screen displays information about the hardware resources of OpenBlocks IoT VX1, network, process status described later and so on.

To display the latest information, click the [Refresh] button.

Chapter 4 SMS Control

This device supports SMS with some mobile line modem modules.

(SMS cannot be supported if the mobile line contract does not include the SMS function.)

SMS is the short message service available in the mobile phone. With this function, you can send a message that contains up to about 70 characters to the destination phone number. This is different from data communication that this device normally uses.

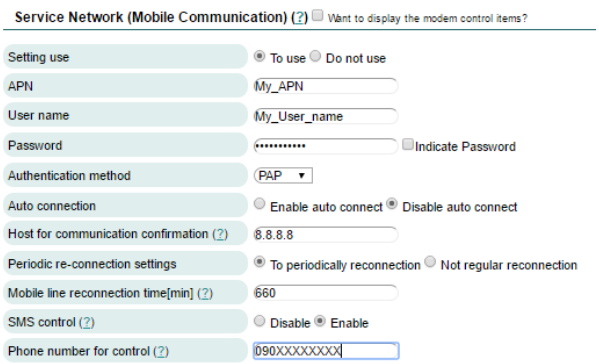
This device can start or stop data communication or execute the shell script when receiving SMS messages that contain certain keywords.

* This function can not be used with the G4 communication module.

4-1. SMS Control Startup Settings

SMS control is the function for mobile line users.

For mobile line settings, see "Service Network (Mobile Communication)" in "3-3-1. Mobile Router Configuration."



Service Network (Mobile Communication)

Auto connection:

You can select either option.

Note that if you connect to the mobile line with SMS control, connection is not established again if the line is disconnected from the network side.

SMS control:

Select [Enable] here.

Phone number for control:

This item is displayed when you select [Enable] for [SMS control].

Enter the phone number of smartphone or other device which SMS control applies to here. SMS messages from phone numbers other than the one specified here are ignored.

Enter the phone number from the long-distance code.

This number may be short such as four digits in case of SMS for the private line.

Be sure to enter this item.

4-2. SMS Control Commands

SMS control incorporates the following commands:

Command	Description of command	Remark
CON	Connects the mobile line.	
COFF	Disconnects the mobile line.	
SSHON	Opens SSH.	If you reboot the OS after opening SSH, SSH is automatically closed. Close SSH after using it because SSH remains open until reboot.
SSHOFF	Closes SSH.	
REBOOT	Reboots the system.	
USCR1 to USCR5	Executes the user script at background.	These commands can be edited with the script editor on the [Extension] tab on the Web UI. For the registration procedure, see "4-4. Registering an SMS User-Defined Script."
USCR1F to USCR5F	Executes the user script at foreground.	
UPGRADE	Executes the online update.	In order to do online updates, must be connected to the Internet.
STUNNEL	Enable SSH reverse tunnel	See section 7-1.

4-3. Sending Multiple Commands with SMS

You can send multiple commands in an SMS message.
Because "CON","COFF","SSHON","SSHOFF","USCR1F" to "USCR5F" and “UPGRADE” are executed at foreground, you can sequentially execute them by concatenating them with "+" as shown below in the character string sent with SMS.

Example 1)

CON+USCR1F+USCR2F+COFF : Connect to the mobile line, execute script 1, execute script 2, and disconnect from the mobile line.

Example 2)

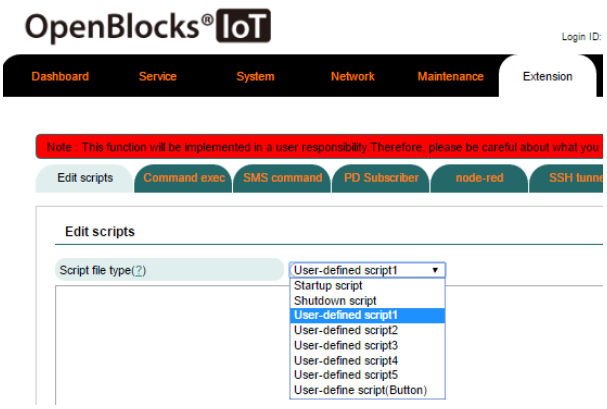
CON+SSHON : Connect to the mobile line and open SSH.
SSHOFF+COFF : Close SSH and disconnect the mobile line.

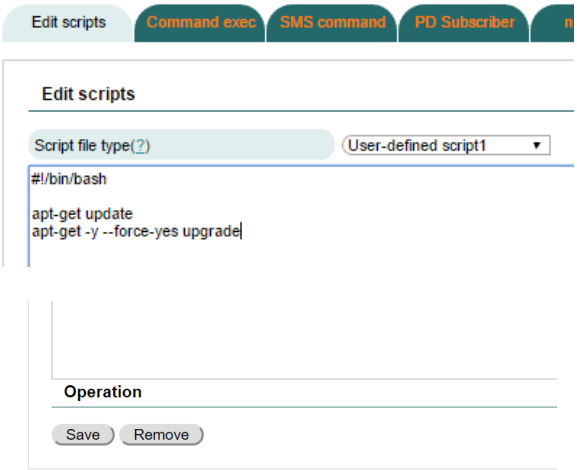
* "USCR1" to "USCR5" and “STUNNEL”are executed at background and, therefore, in parallel.

4-4. Registering an SMS User-Defined Script

You can register and edit a user-defined script with the Web UI. Note that this function is intended for users who can create Linux shell scripts by themselves. Note that we do not support the execution of user-defined script.

You can create and edit scripts in [Edit scripts] on the [Extension] tab.





<u>Edit scripts</u>

Script file type:

Select the script you want to edit from the pull-down menu.

You can create a script automatically executed when the OS of this device starts up in the startup script you can select from this pull-down menu.

The contents of the startup script is executed at background.

Enter a script in this field.

This script example updates each application in the Internet environment.

(This is a recommended script because security updates are frequently issued for each application.)

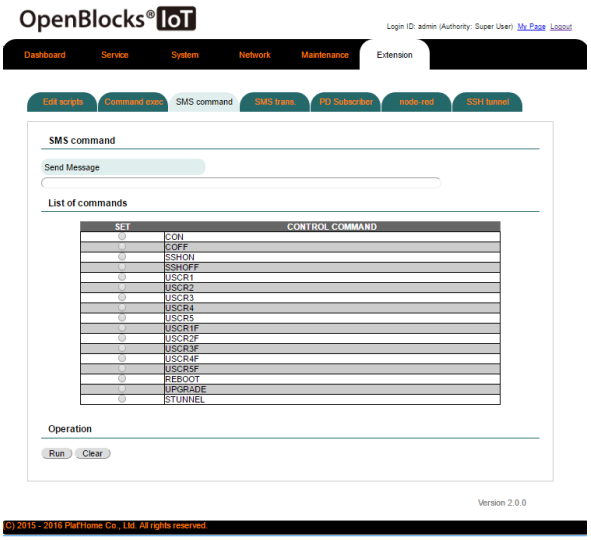
After completing the script, click the [Save] button at the left bottom of the screen.

In addition, you can erase unnecessary scripts with the [Remove] button.

*In the above reference example, the script applies OS patches to this device at a remote location via SMS.

4-5. Direct Execution of SMS Control Commands

Although SMS control commands registered in this device are usually executed by issuing them with the mobile phone, they can be also directly executed from the Web UI.



<u>SMS command</u>

Send Message:

Enter the SMS commands to be sent in a pseudo way here.

<u>List of commands</u>

Select the SET radio button in the SMS command list to add the corresponding command to the message to be sent. A plus sign (+) is automatically inserted for the second and subsequent commands.

*"CON" and "COFF" are displayed only when [To use] is selected for the mobile line.

<u>Operation</u>

[Save] button:

Sends commands included in the message to be sent to this device in a pseudo way.

[Clear] button:

Erases the contents of the message to be sent.

Chapter 5 Items Related to Bluetooth Device

This device supports the Bluetooth interface as the standard IoT device.

Bluetooth is broken down into two categories: that uses old specifications and BLE (Bluetooth Low Energy), which uses new specifications.

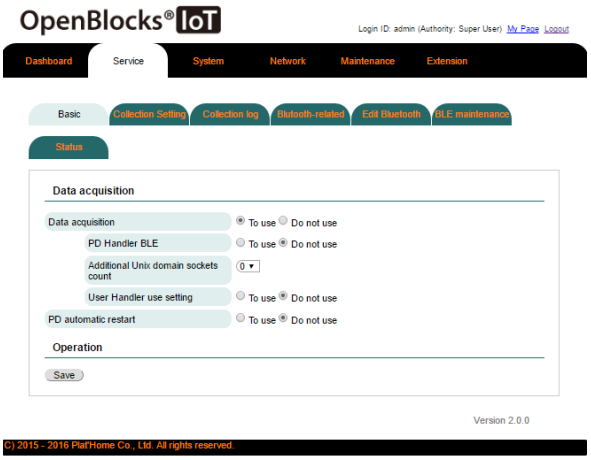
This device supports SPP (serial communication device) for Bluetooth with old specifications and can redirect SSH via the Internet to the SPP device using this device as the serial communication platform.

This device also supports the GAT profile to transmit sensor data through BLE communication and can scan sensor data such as temperature and humidity with standard exchange. However, individual support is required because each sensor has different data formats.

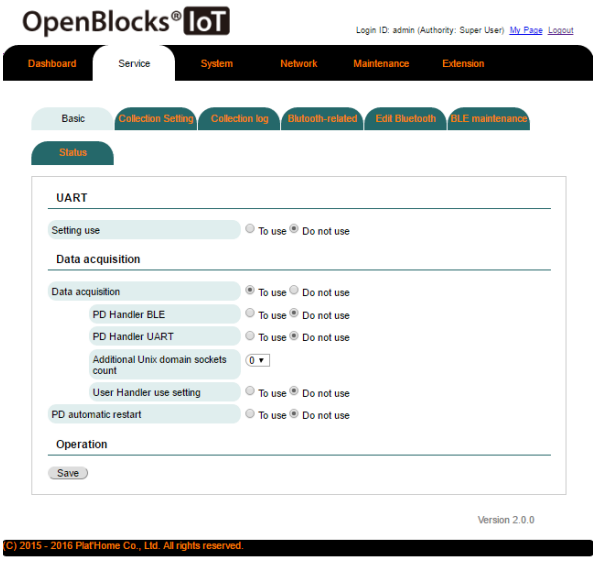
The OpenBlocks IoT VX1 will gradually support additional sensors. (For the latest support information, see our website.)

5-1. Starting the Bluetooth Service

To support a Bluetooth device, activate its service on [Basic] tab.



* If extended additional module is installed.



UART

Setting use:

Select depending on whether UART is used or not. Select [Do not use] in this document.

This item is displayed only when extended additional module is installed.

Data acquisition

Data acquisition:

To use the standard function of this system to automatically acquire sensor and other data from the Bluetooth device, select [To use].

When you select [To use] and save the setting, the [Collection Setting] and [Collection log] tabs are added. (When only supporting the SPP device, select [Do not use].)

Keep [Do not use] selected until you complete registration of sensors and other processes.

PD Handler BLE:

Specify whether to use the application to acquire data from the Bluetooth device provided from us.

Select [To use] in this document.

PD Handler UART:

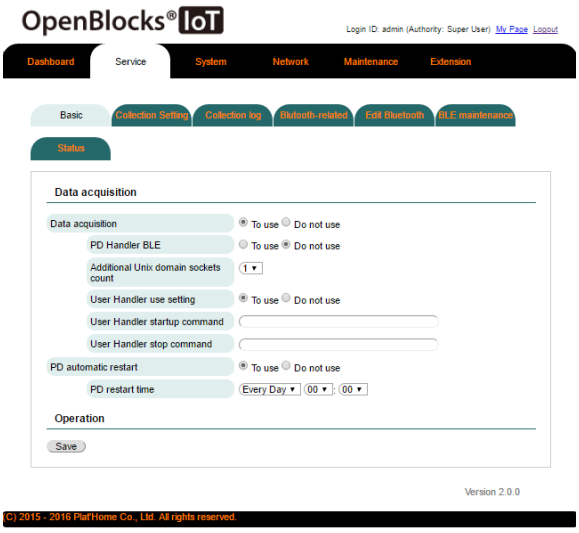
Specify whether to use the application to acquire data from the UART device provided from us. Select [Do not use] in this document.

This item is displayed only when extended additional module is installed.

PD automatic reboot setting:

Select whether to automatically reboot our data acquisition tool.

* If enabled “User Handler” and “PD automatic reboot”.



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.

PD automatic reboot setting:

Select whether to automatically reboot our data acquisition tool.

PD restart time:

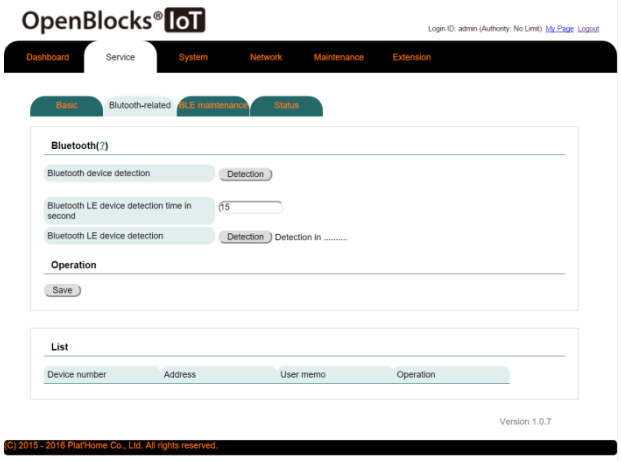
Specify the time to reboot our data acquisition tool.

After completing the above setup, click the [Save] button.

The setting tab for each service appears after you select [To use] for each of them and click the [Save] button.

5-2. Paring with the Bluetooth Device

To support a Bluetooth device, activate its service on [Basic] tab.



Bluetooth

Bluetooth device detection:

When you click the [Detection] button, near-by Bluetooth devices are listed.

When you select the use setting check box for the device to be used in the list, pairing is executed. The device is registered by clicking the [Save] button after pairing is complete.

Bluetooth LE device detection time in second:

Specify the time to detect BLE devices. (You can normally use the default.)

Bluetooth LE device detection:

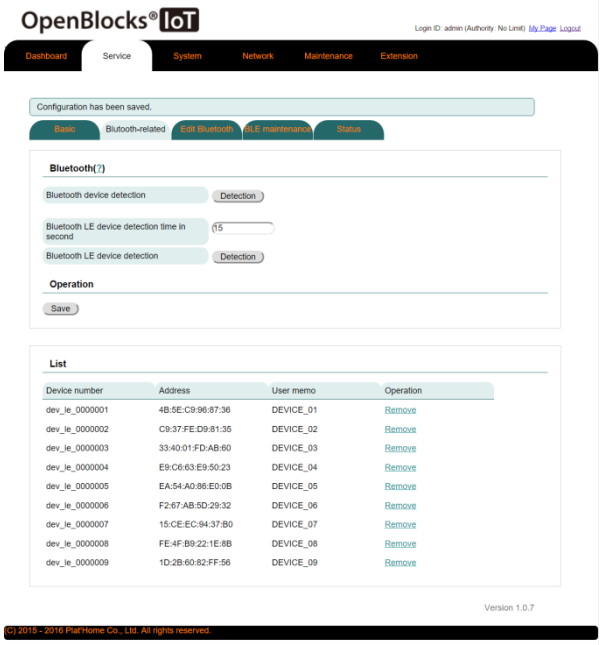
When you click the [Detection] button, near-by BLE devices are listed.

The device is registered by selecting the use setting check box for the device to be used in the list and clicking the [Save] button.

*Paring is not performed with the BLE.

Sensor data is only imported.

It is recommended to enter information so that the device can be identified in the [Memo] field after you register a Bluetooth device here.



List

Device number:

This device assigns numbers to automatically detected devices.

Address:

Address used for Bluetooth access.

User memo:

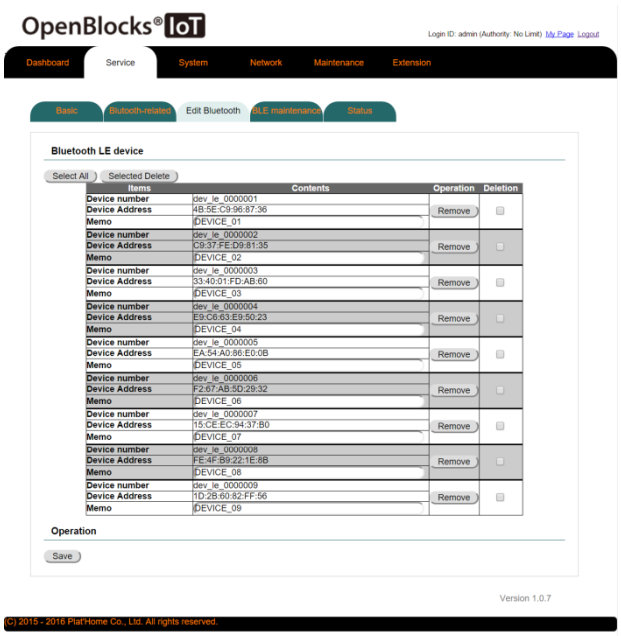
Displays information written in the [Memo] field on the screen displayed during registration.

Operation:

Click [Remove] to unregister the device.

5-3. Editing Registered Devices and Memo

When one or more devices are registered, the [Edit Bluetooth] tab is added.



To edit or delete the [Memo] field for a registered device later, perform the operation from the [Edit Bluetooth] tab.

It is more convenient when deleting or otherwise editing the device if you specify information that facilitates device identification in the [Memo] field.

To apply the edited data, click the [Save] button.

5-4. Data Acquisition Settings

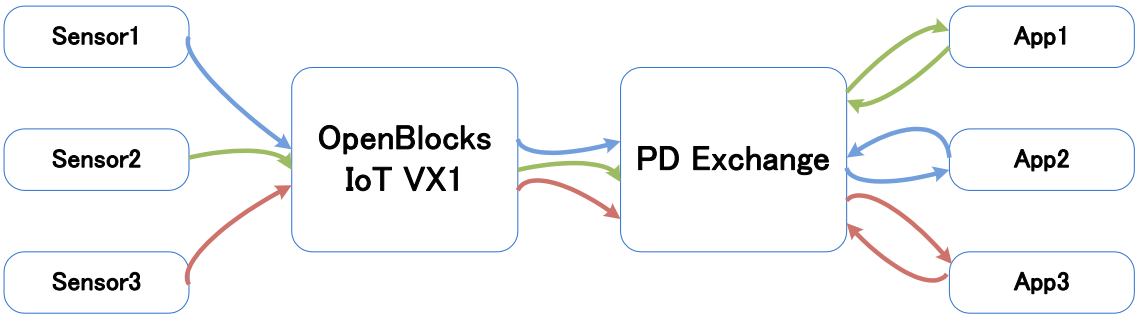
The [Collection Setting] tab can be used to specify settings to acquire information from each Bluetooth device.

Please refer to " OpenBlocks IoT VX1 Data Acquisition Guide" for this section.

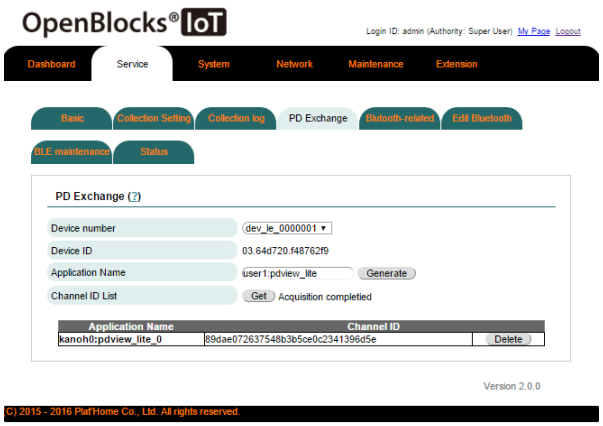
5-5. Linkage between PD Exchange, Applications, and Devices

PD Exchange (separately available) has a function to provide data to multiple applications for each sensor device.

This section describes how to link applications registered in PD Exchange and devices registered in this device, which is necessary for using the PD Exchange server.



Perform the following operations on the [PD Exchange] tab.



Device number:

Select the registered device you want to link from the pull-down menu.

Application name:

Specify an application registered in PD Exchange in advance and click the [Generate] button.

If you specify the name of application not registered in PD Exchange, an error occurs.

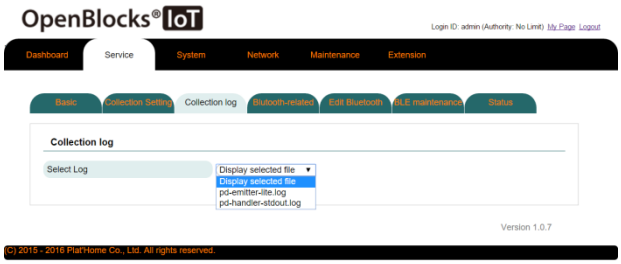
Channel ID list:

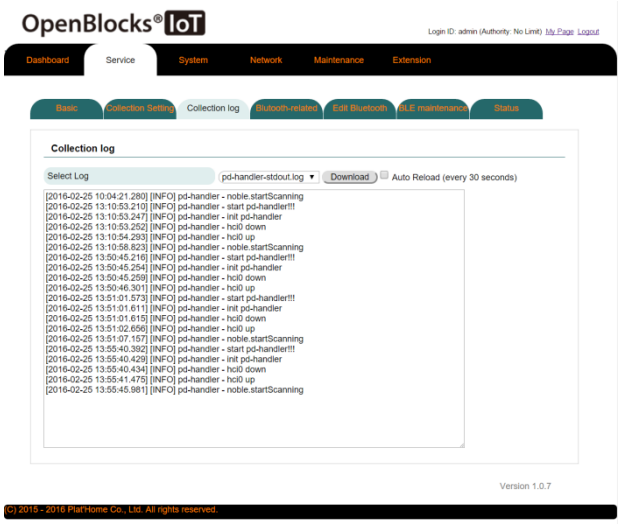
Clicking the [Acquire] button displays the channel ID of linked device and application.

5-6. Checking the Collection Log

When you complete the settings until this section, the device is ready to acquire data and data transmission to the reception log and each destination has already started.

Each operation log and other data can be downloaded from the [Collection log] tab to the web client.





<u>Collection log</u>

Select Log:

Select the logs to be displayed from the pull-down menu.

The log that starts with pd-emitter is the log of data transfer to the destination.

The log that starts with pd-handler-stdout is the collection log from sensors or beacons.

pd-handler-local-beacon.log is a log of surrounding beacons. If the data filter is specified, this is filtered information.

The log that starts with pd-handler-uart is the collection log from extended additional module such as Wi-SUN or EnOcean.

When you select a log, it is partly displayed.

To display the whole log, click the [Download] button to save the log in the local disk. You can then check the saved log with a text editor.

5-7. Checking Sensor Data

The [Data display] tab is a display page to check how sensor data is captured.
Latest 20 sensor data items are displayed for each sensor.

Graph display example

Click the [Redraw] button to create a graph based on latest 20 data items.
0°C or 0% is displayed for items that do not support the temperature or humidity.

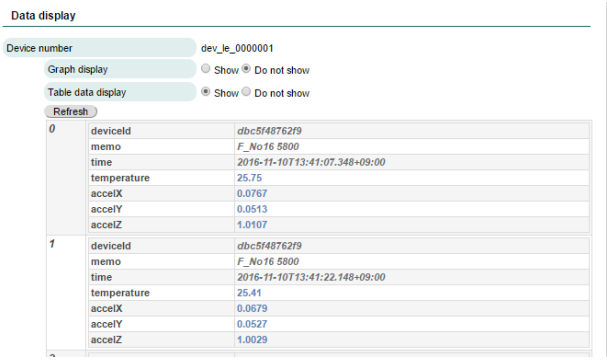
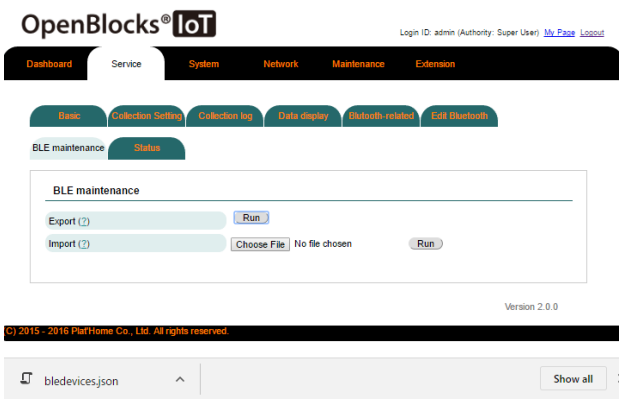


Table display example

You can update the display to the latest data with the [Refresh] button.

5-8. Exporting or Importing BLE Device Setting Information

The setting information of BLE device, which does not require pairing, can also be used in other OpenBlocks IoT Families. So, that setting information can be exported or imported as the JSON file.



Export:

Export the setting information of BLE device registered in this device in a JSON file.

Click the [Run] button to start the download process.

The downloaded file is saved in the storage on the web client.

Import:

Click the [Select file] button to select the JSON file saved on the web client. Click the [Run] button to start the import process.


```
{
    "D4:D4:64:B2:8F:6A": {
        "send_flag": "true",
        "information": "",
        "signal_strength": "0",
        "interval": "50",
        "destination": [
            "LOCAL",
            "NODE-RED"
        ],
        "PD_EXCHANGE": {
            "suffix": "64b28f6a"
        },
        "AWS_IOT": {
            "client_id": "d4d464b28f6a",
            "thing_shadows": "false",
            "topic": "d4d464b28f6a",
            "cert_path": "¥/var¥/webui¥/upload_dir¥/d4d464b28f6a¥/cert.pem",
            "privatekey_path": "¥/var¥/webui¥/upload_dir¥/d4d464b28f6a¥/privatekey.pem"
        },
        "WATSON_DEVICE": {
            "device_type": "sensor",
            "device_id": "d4d464b28f6a"
        },
        "WATSON_GATEWAY": {
            "device_type": "sensor",
            "device_id": "d4d464b28f6a"
        },
        "MS_EVENT_HUBS": {
            "hubs_name": "",
            "sas_policy": "",
            "sas_key": ""
        },
        "MS_IOT_HUB": {
            "device_id": "",
            "device_key": ""
        },
        "TOAMI_FOR_DOCOMO": {
            "gwname": "",
            "appkey": ""
        },
        "MQTT": {
            "client_id": "d4d464b28f6a"
        }
    }
}
```


This is a display example of JSON file.

*Output differs depending on the version of Web UI.

When you import a JSON file, the contents of the csv file are displayed.

If there are no problems, click the [Save] button.

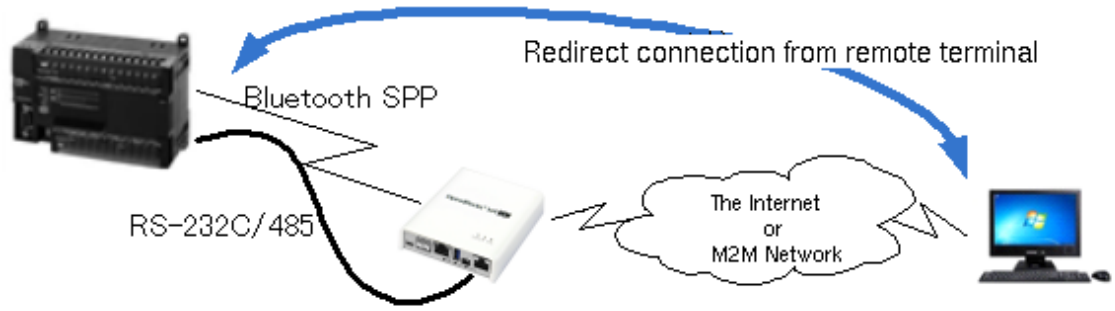
This registers the JSON file.

Chapter 6 Serial Communication Redirection Function

The serial communication redirection function is a function to redirect communication data from the RS-232C/RS-485 interface or Bluetooth SPP device connected to this device to a serial communication device at a remote location.

Many M2M legacy devices use the RS-232C, RS-485 or other interface to connect with external devices required for maintenance and control. For many of these devices, the maintenance representative visits the installation site and connects a PC or other device for log acquisition and software update.

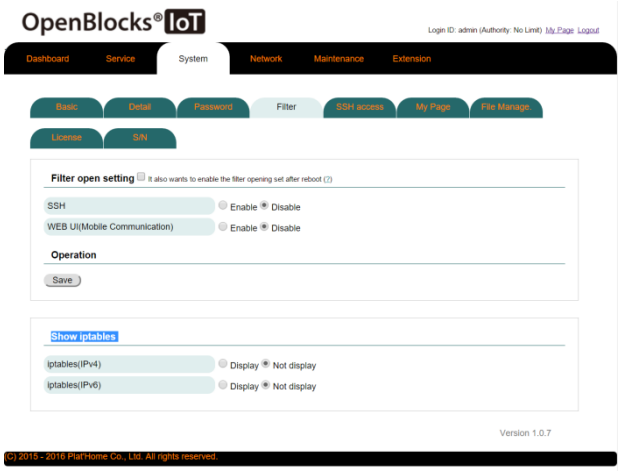
With this device, you can directly connect to such devices via Internet without visiting the site. The customer can perform network remote operations because the mobile line can be used at that time.



6-1. Serial Communication Redirection Function in the SPP Device

If the paired Bluetooth device is of SPP (serial port profile) type, serial communication to this device via SSH can be redirected to a Bluetooth device.

Make the SSH port usable before using this function.



Select the [System] tab on the Web UI and click the [Filter] tab to display the SSH open/close setting.

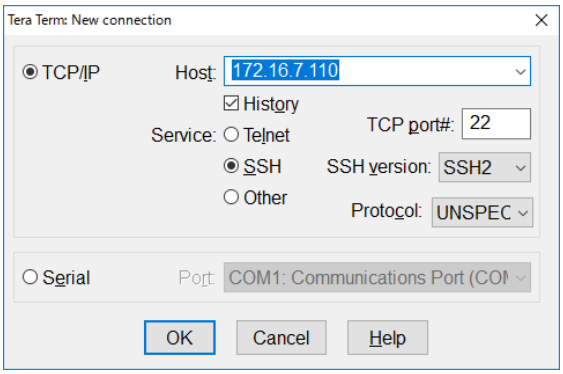
Select [Enable] and click the [Save] button. This makes SSH usable.

You can also open SSH with SMS control.

> **Lines on which SSH can be used**
>
> This section assumes that SSH can pass through the firewall and the terminal using SSH can access this device with global IP or other protocol.
>
> Generally, SSH can be used in the local network or private network for M2M. However, NAPT connection is often used for the mobile line that uses the public Internet line and global IP is not allocated it. So, in many cases, this device cannot be reached with SSH.
>
> However, there are services to optionally allocate global IP to the mobile line. You may use such an optional service or our PacketiX VPN for SSH connection.

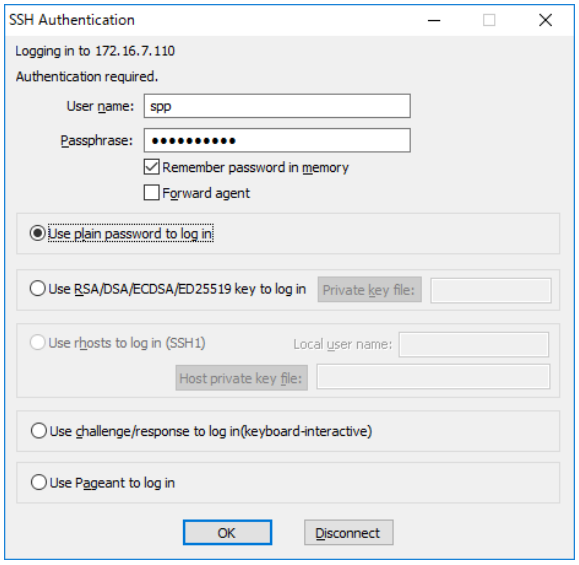
When preparations are made, start connection by using communication software that supports SSH such as TeraTerm.

This section assumes the local network for description purposes.



Enter the IP address of this device in the LAN because you are within the local network.

Select SSH and click the [OK] button to open the authentication screen.



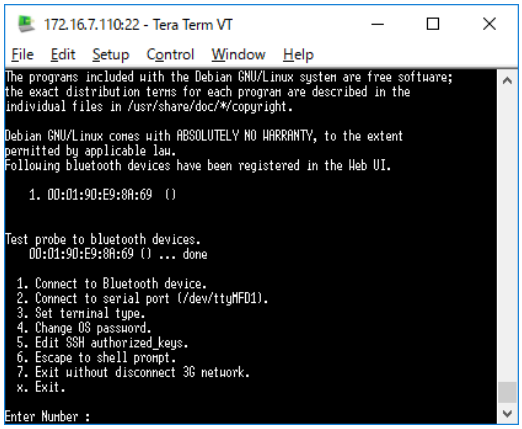
Enter spp as the user name on the authentication screen.
The default password is the same as the default root password set to this device.

* This password cannot be changed from the Web UI, It can be changed from the CLI that shown following .

Select the plain password as the authentication method.

After specifying the authentication, click the [OK] button to start connection.

When you can successfully log in as the user, spp, the serial communication redirection menu screen appears.

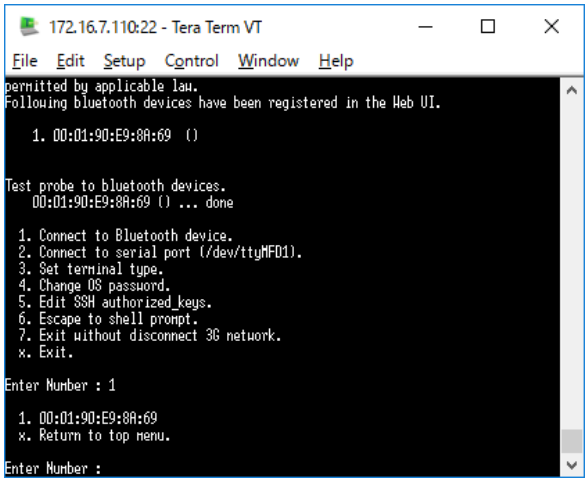


Carefully confirm that the Bluetooth device paired in "5-2. Paring with the Bluetooth Device" is properly probed.

Detected devices are displayed below "Test probe to Bluetooth devices." For example, if the device is turned off, "fail" is shown.
Connection is possible if "done" is displayed here.

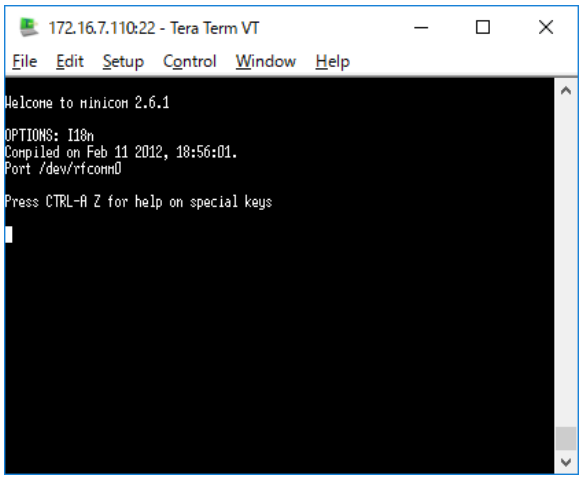
When there are multiple active paired Bluetooth devices, they are listed on several lines.

Select 1 on the menu here.



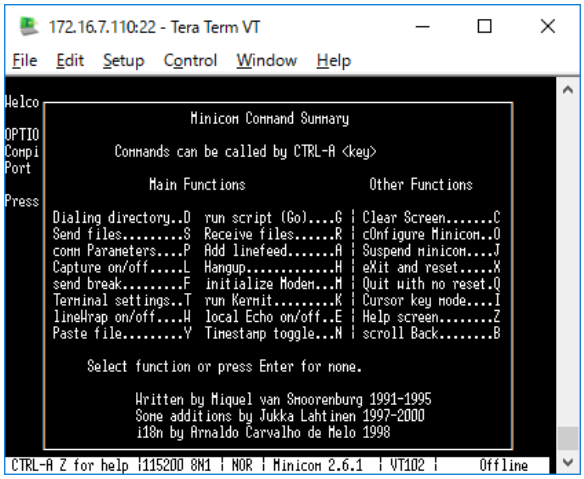
When the next screen lists connectable devices, select the connecting destination number.

When you select the connecting destination, the next screen appears and minicom starts redirection.



Press CTRL-A and enter Z to display the help for minicom.

To exit minicom, follow the help.

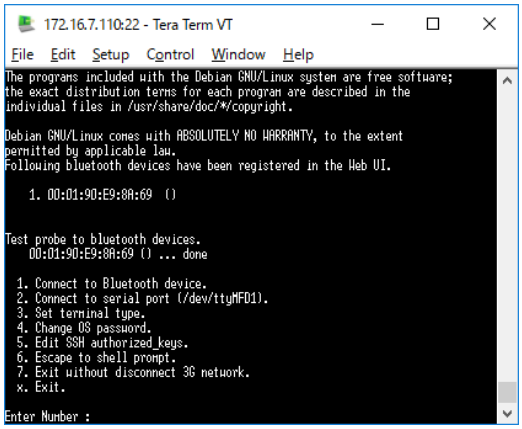


To exit minicom, go back to the top menu following the menu and then exit it.
You can also exit minicom by disconnecting the mobile line at the same time.

You can perform direct serial communication with the SPP device with the above procedure. For example, you can combine a TeraTerm script and a shell script in Linux or other system to automatically acquire data.

6-2. RS-232C Serial Communication Redirection Function

The serial communication redirection function in this device supports not only redirection to Bluetooth but also redirection to the wired interface RS-232C port in this device.



The operation procedure is almost the same as in that in Section 6.1. When you select "2. Connect to serial port (/dev/ttyMFD1)" on the at the serial communication redirection menu first displayed after SSH is started, redirection to the RS-232C port starts.

The serial communication speed is 115200 bps by default. Change the setting as needed.

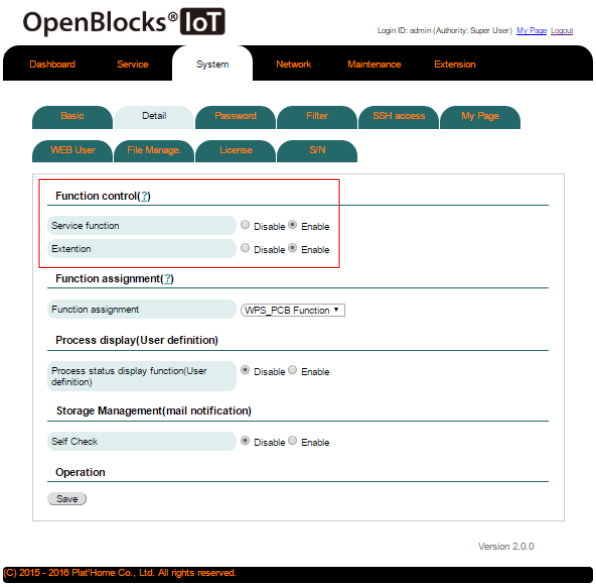
Chapter 7 Reference by Setting Item

Attension)

Sections 7.4 and 7.7 implemented in this chapter are important for security. Therefore, please set a password that makes it difficult to crack.

7-1. Displaying and Hiding the Service Control and Extension Functions

Although this Web UI is customized for IoT, you can disable web display related to the IoT server only leaving the basic server settings when you use this device for another purpose.



<u>Function control</u>

Service function:

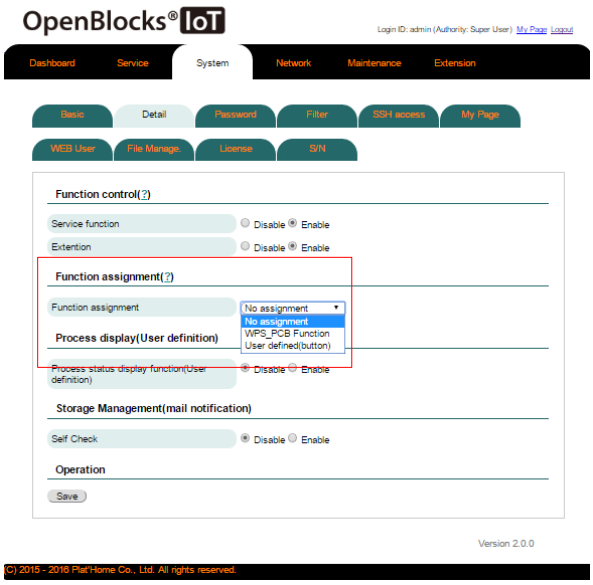
Hides the Service tab.

Extension:

Hides the Extension tab.

7-2. Function assignment to the FUNC switch

You can assign any function to the FUNC switch.



Function assignment

The following functions can be assigned.

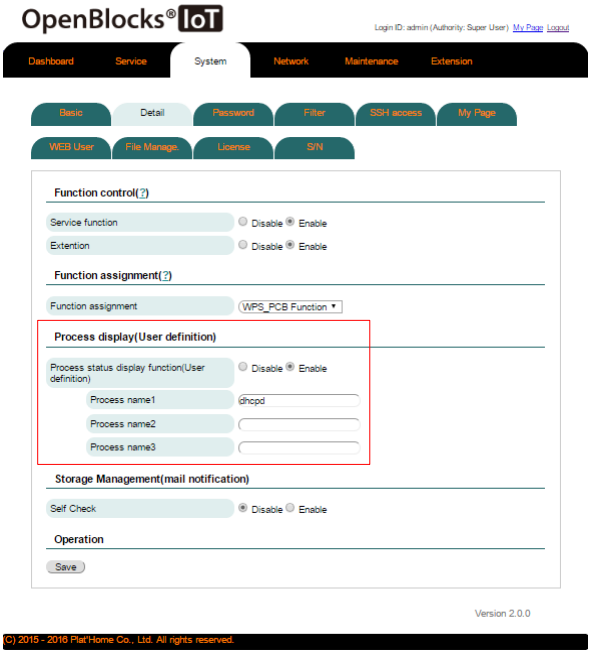
- no assignment
- WPS_PCB Function
- User defined (button)

When Wi-Fi is set to AP mode and WPS function is enabled, the WPS_PCB function is enabled.

In addition, the User defined (button) function is effective when script of target is created by script edit of extended function in the [Extension] ⇒ [Edit scripts]tab.

7-3. Process Status Display Function

You can monitor processes the user added and basic processes.



Process status display

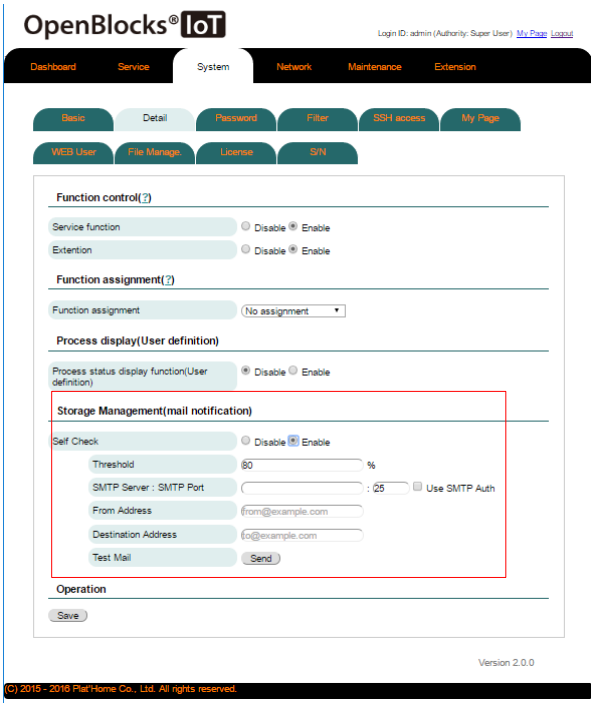
Process status display function (User definition):

For example, you can register dhcpd and other processes you want to monitor to display whether they are active on the dashboard.

You can register up to three processes.

7-4. Storage Alert Function

The storage alert function checks the storage capacity periodically (every hour) and notifies the user by email if the threshold value is exceeded. You can monitor if the storage capacity is running out due to logs or other causes.



<u>Storage Management (mail notification)</u>

Self Check:

To use this function, select [Enable].

Threshold: (Default: 80%)

Threshold to issue an alert.

SMTP Server : SMTP Port:

Enter the address and port of the email server. To use the server that supports SMTP Auth, select the check box.

SMTP Auth:

This item is displayed when you select the [Use SMTP Auth] check box. Specify the user name and password for SMTP Auth.

From Address:

Enter the source address from which email is sent.

Destination Address:

Enter the destination address to which email is sent.

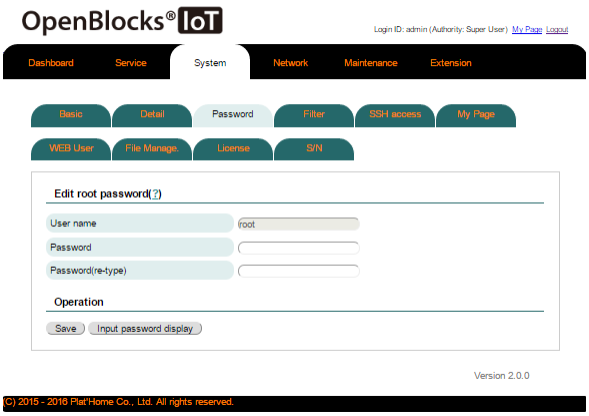
Test Email:

Sends test email with the settings you specified.

You can confirm that the body of email and the settings are correct.

7-5. Setting the Root Password

You can change the password of the root account you can use to log in to this device with SSH or serial console.



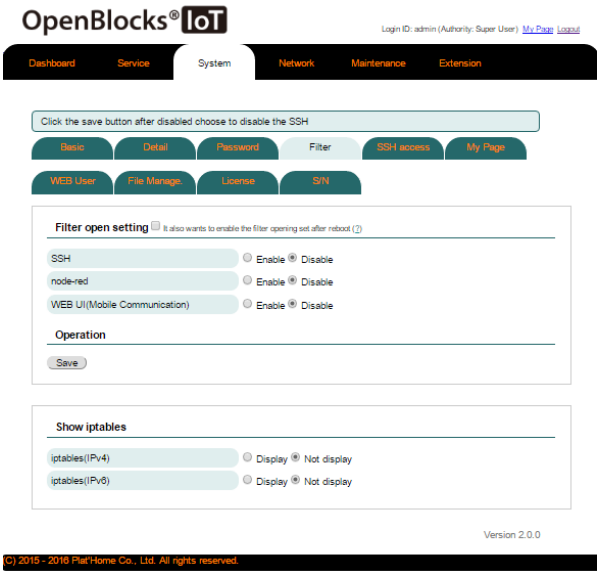
Enter the new password twice in the password field and the confirmation field and click the [Save] button.

Before using this system, be sure to change the default password to ensure security.

> **Default root password**
>
> The default password of the root account in this device is 0BSI0T.
>
> (The two 0s are numbers.)

7-6. Filter Permission

You can enable each filter in this device temporarily or permanently after reboot or other specific operation.



Filter open setting

To keep each filter open after reboot or other specific operation, select the check box and click the [Save] button.

SSH:

To log in to this device using SSH, select the [Enable] radio button and click the [Save] button.

node-red:

To using the Node-RED in the [Extension] ⇒ [node-red]tab, select the [Enable] radio button and click the [Save] button.

Web UI (Mobile Communication):[1]

To access the Web UI via the mobile line, select the [Enable] radio button and click the [Save] button.

Show iptables

iptables (IPv4):

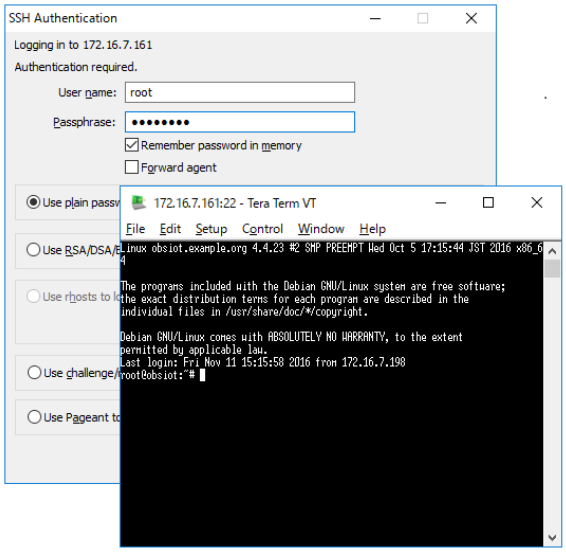
When you select the [Display] radio button, the IPv4 information in iptables is displayed.

iptables (IPv6):

When you select the [Display] radio button, the IPv6 information in iptables is displayed.

Be sure to disable each filter if it does no longer have to be open!!

[1] The Web UI can be only accessed via Wi-Fi or Ethernet. Access via the mobile line is usually not supported for security reasons.

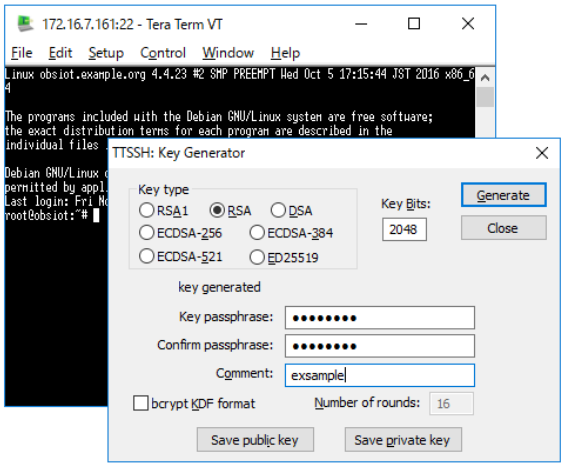


As shown in the left screenshots, SSH is logged in to by specifying the IP address in terminal software such as TeraTerm.

It is recommended to register the public key as described in "7-7. SSH Key Exchange" to more securely operate SSH.

7-7. SSH Key Exchange

This is the setting screen to more securely use SSH.

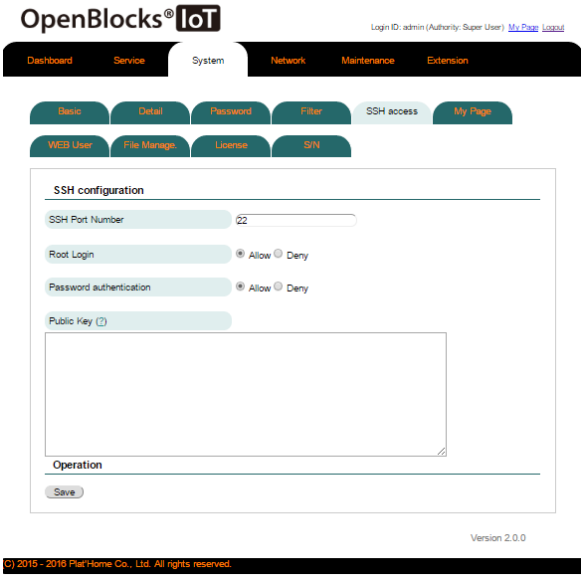


First, generate the public key and private key with TeraTerm or other software as shown on the left screen.

When you use TeraTerm, these two keys are saved in the specified directory. Display the public key with text editor or other software and save it in the copy buffer.

* In TeraTerm, the Key Generator is on the [Setup] menu.

Settings are located at [System] ⇒ [SSH access] tab.



SSH configuration

SSH Port Number:

Specify the port number used for SSH.

Root Login:

To permit SSH login to this device with the root account, select [Allow].

Password authentication:

To access SSH without using a key, select [Allow] in [Password authentication].

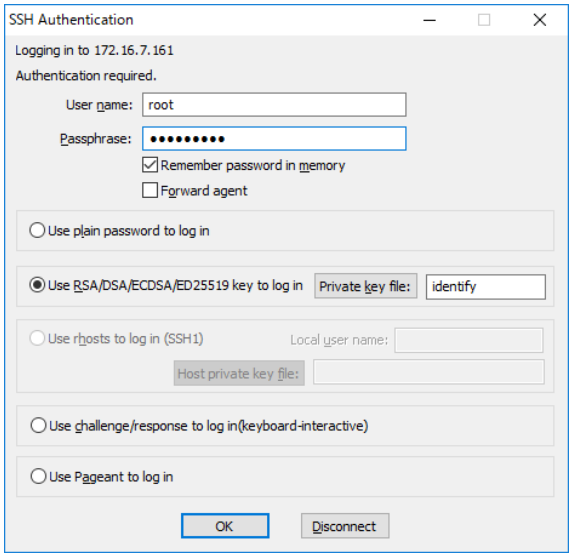
To use authentication with a key, select [Deny].

Public Key:

Paste the public key you created in above-mentioned TeraTerm or other software.

Leave this field empty if you do not use the key.

After completing the setup, click the [Save] button.



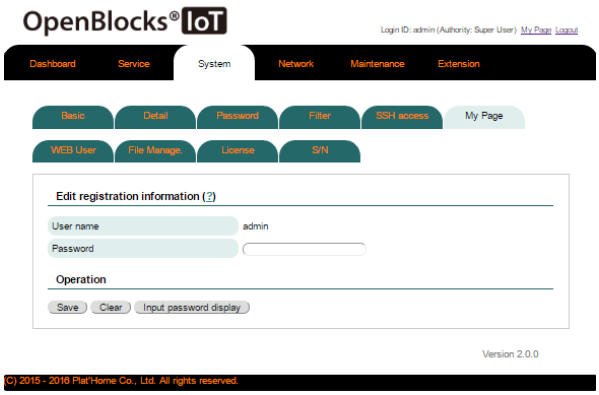
After completing the above setup, log in with SSH using the key.

The left screen is a connection example using TeraTerm.

7-8. Changing the Web Administrator Password

You can change the Web UI administrator password. Note that you cannot change the user name.

Settings are located at [System] ⇒ [My Page] tab.



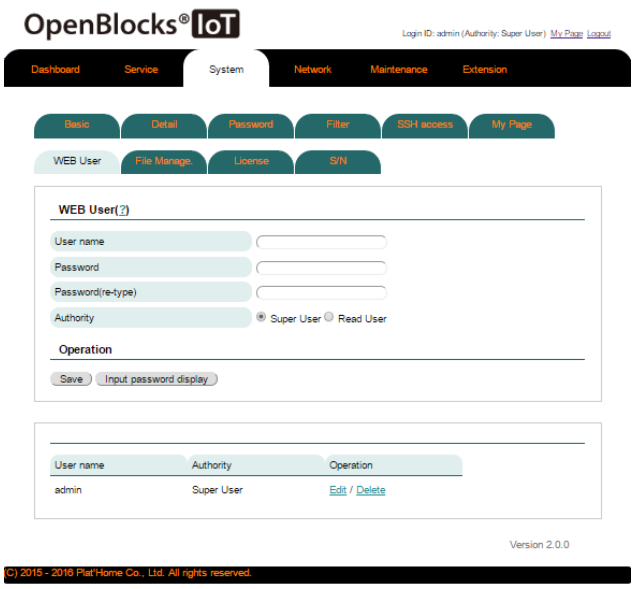
When you click the [Save] button after editing, the change is applied.

After changing the password, log in to this device again.

7-9. WEB User

You can add login user of WEB UI or change password of another login user (superuser only).

Settings are located at [System] ⇒ [WEB User] tab.

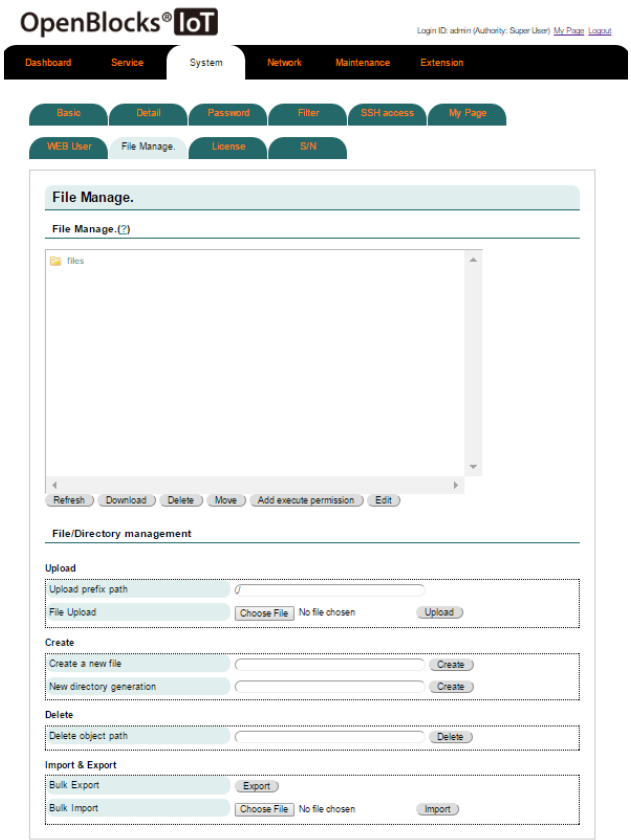


After setting the user name, password etc, the change will be effective when you press the save button.

7-10. File Management

You can upload a file in a specific directory in the OpenBlocks IoT Family or otherwise manage the file by using the Web UI.

Settings are located at [System] ⇒ [File Manage.] tab.



To download, delete, move, permit execution or edit, select the file and press the button for execution.

To upload a file, select the file you want to upload from [Select file] and click the [Upload] button.

The file is uploaded to the following location:

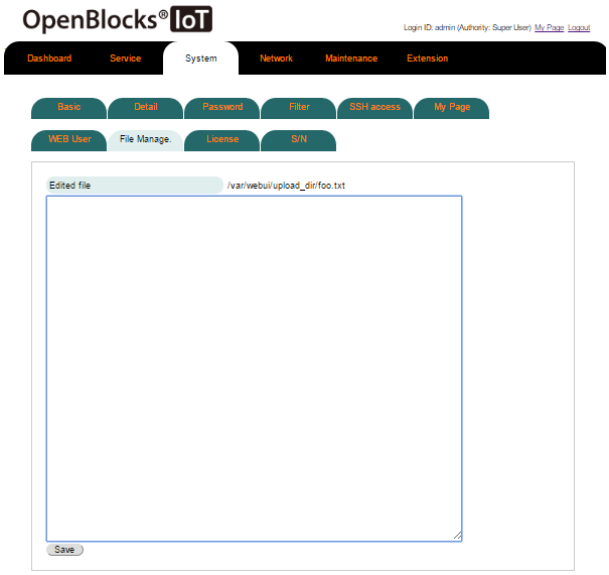
Dir : /var/webui/upload_dir/

Files larger than 256 MB cannot be uploaded. To upload such a file, enable SSH and upload the file with SFTP.

To generate a new file, enter the file path and create a file. You can create files under /var/webui/upload_dir/. (Files cannot be created in an upper-level directory.)

When you perform batch export, a file that contains all files under /var/webui/upload_dir/ compressed in the tar+gz format is exported.

When you perform batch import, data in the tar+gz format is deployed under /var/webui/upload_dir/.



When you click the [Edit] button after selecting a file, the screen appears as shown at the left.

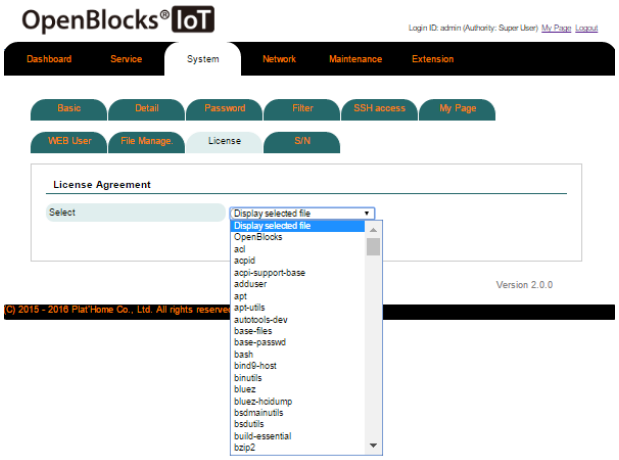
To save edited data, click the [Edit] button.

Note that only text files can be edited.

7-11. Displaying the Software License

You can display the software and other licenses used on the Web UI.

This information is displayed at [System] ⇒ [License] tab.



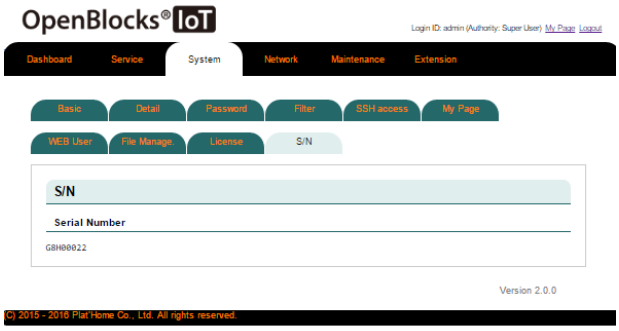
You can select and display software and other licenses used in this device for each software product from the pull-down menu.

Source codes using open source licenses are published on our website.

7-12. Checking the Main Unit Serial Number

You can check the serial number of the OpenBlocks IoT Family main unit with the Web UI.

You can check the serial number on [System] ⇒ [S/N] tab.

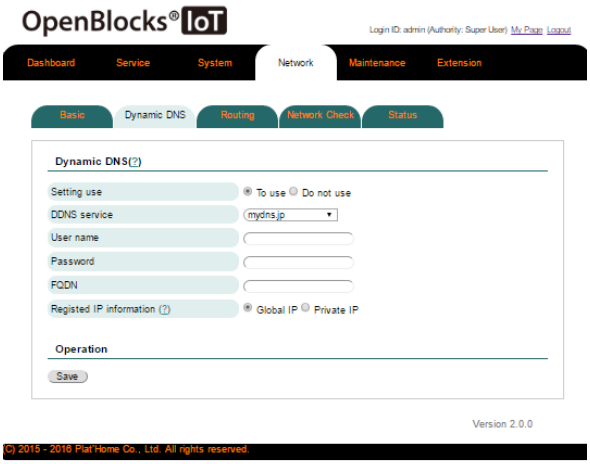


*The serial number displayed on the left screenshot is a sample.

7-13. Dynamic DNS

You can periodically register the current IP address in the dynamic DNS server with the Web UI.

The settings are located at [Network] ⇒ [Dynamic DNS] tab.



<u>Dynamic DNS</u>

Setting use:

To use dynamic DNS, select [To use].

DDNS service:

Select the DDNS service.

(The list contains free DDNSs. Plat'DNS cannot be used because the service is not yet deployed.)

User name:

Enter the user account of DDNS.

Password:

Enter the password of DDNS.

FQDN:

Enter the FQDN registered on the DDNS.

This item is not displayed when you select Plat'DNS.

Registered IP information:

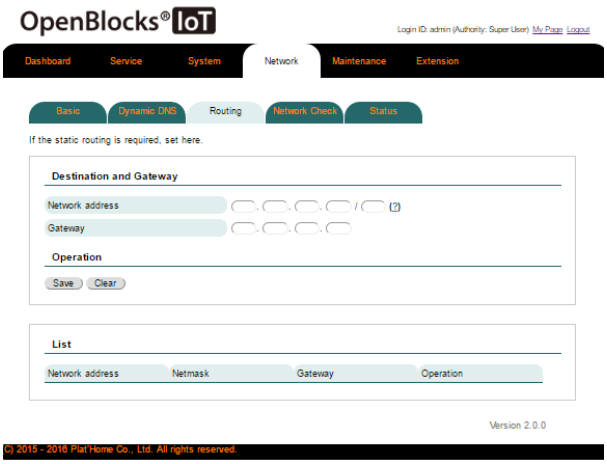
Specify the attribute of the IP address notified on the DDNS.

After completing the setup, click the [Save] button. You must reboot the device to apply the setting.

7-14. Adding Static Routing

You can set up static routing as needed when the router operates in the AP mode, for instance.

The settings are located at [Network] ⇒ [Routing] tab.



Specify the network address and netmask, specify the IP address of the device that serves as the gateway, and click the [Save] button.

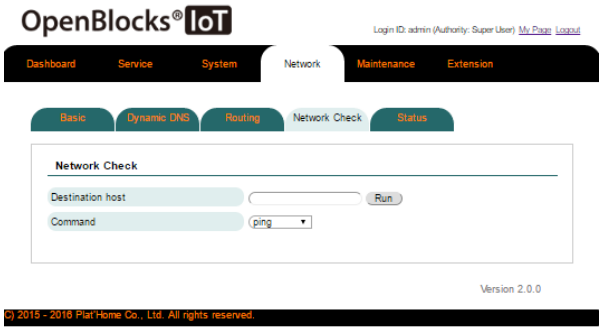
You can register multiple static routing units.

Reboot the device to apply the settings.

7-15. Communication Check

You can test the network to see if it is usable by using the ping command or other means.

You can execute the test at [Network] ⇒ [Network Check] tab.



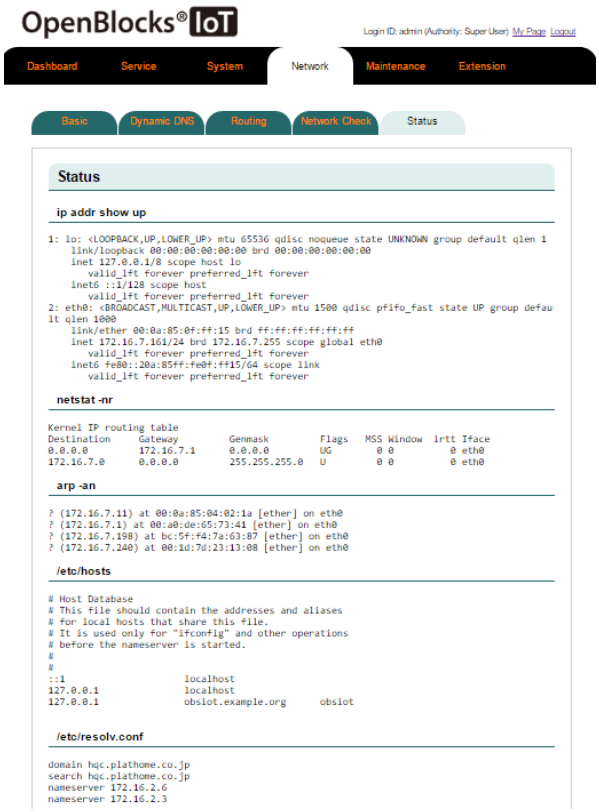
You can select ping, traceroute or nslookup from the pull-down menu as the command to be used.

When you select a command and click the [Run] button, the execution result is immediately displayed at bottom.

7-16. Network Status Check

You can check a variety of network statuses.

You can check the statuses at [Network] ⇒ [Status] tab.



It is recommended to check statuses on this screen after completing setting up this device and rebooting it.

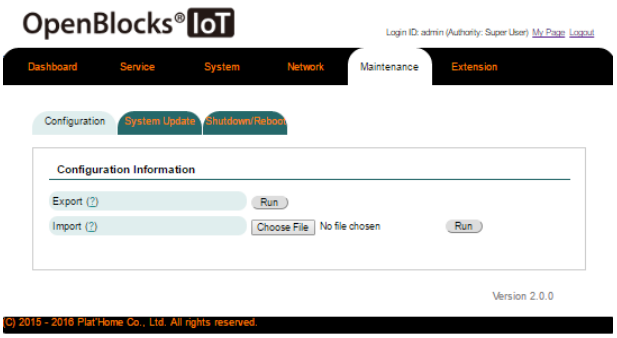
Check the following items:

- IP address
- Routing information
- arp information
- Host information
- DNS server information
- Modem information
- SIM information

7-17. Backing up and Restoring Configuration

You can back up the configuration you specified with the Web UI to the web client. You can also restore the configuration by using the backed up file.

You can perform these operations at [Maintenance] ⇒ [Configuration] tab.



When you click the [Run] button for [Export], the backed up configuration file is downloaded to the web client.

To restore the configuration, select the backup file with [Select file] in [Import] and click the [Run] button. The configuration is restored based on the configuration file.

* It is recommended to back up configuration every time you make changes after completing system setup of this device.

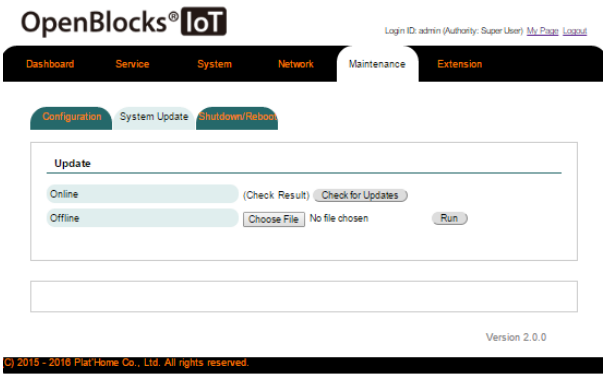
* The following replacement rules are applied when importing the configuration file.

Source string	Replacement contents	Remarks
@@SERIAL@@	Main unit serial number	

7-18. Updating System Software

You can check if the firmware, OS, or application in this device is upgraded and update them.

You can perform these operations at [Maintenance] ⇒ [System Update] tab.



You can perform online update when this device is in the Internet connection environment.

When you click [Check for Updates] in [Online], update information is checked based on repository information and details of each update appear at the bottom of this screen, if any. To apply updates, execute the update operation.

We provide offline packages for important updates.

Download offline packages to the web client (PC is recommended because of the file size), select the update package on the PC with the [Select file] button in [Offline] and click the [Run] button.

Because security updates are frequently issued, it is recommended to apply updates as often as possible.

7-19. Register EnOcean device

If the EnOcean module is installed and enabled the data acquisition with EnOcean in the [Service] ⇒ [Collection Setting] tab, the [Service] ⇒ [EnOcean Regist] tab will be displayed.

<u>EnOcean Regist</u>

Device ID :

Specify the device ID of the EnOcean device to be collected.

User memo :

You can specify the any information to be added to the collected data.

EEP(EnOcean Equipment Profiles) :

Specify the EEP(EnOcean Equipment Profiles) of the target device.

<u>EnOcean Device Bulk Setting</u>

Export :

Pressing the execute button will download the registered EnOcean device list in json file.

Import :

By selecting and importing a json file that conforms to the format, you can register EnOcean device devices in batch.

When input of EnOcean Registration Division is completed, press "Register / Update" button.

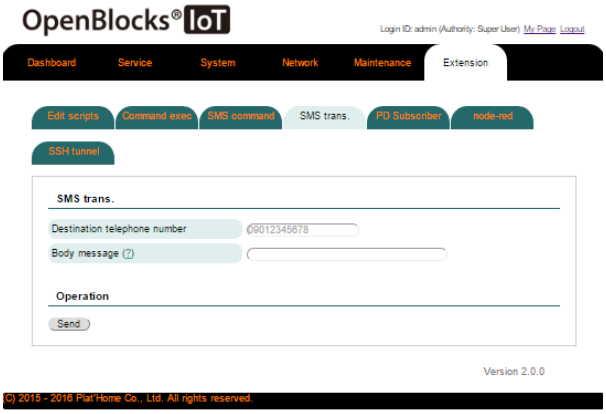
* To change the information of the registered device, select the edit button of the target device in the list.
* If you change to another device ID, it will be treated as new registration.

7-20. SMS Transmit

This product supports SMS with some mobile line modem modules.

(If SMS function is not included in the mobile line contract, it can not be supported, and SIM must be inserted in this device.)

With this function, it is possible to send SMS from WEB UI.



SMS trans

Destination telephone number :

Specify the SMS destination phone number.

Body message :

Enter the body of the SMS to be sent.

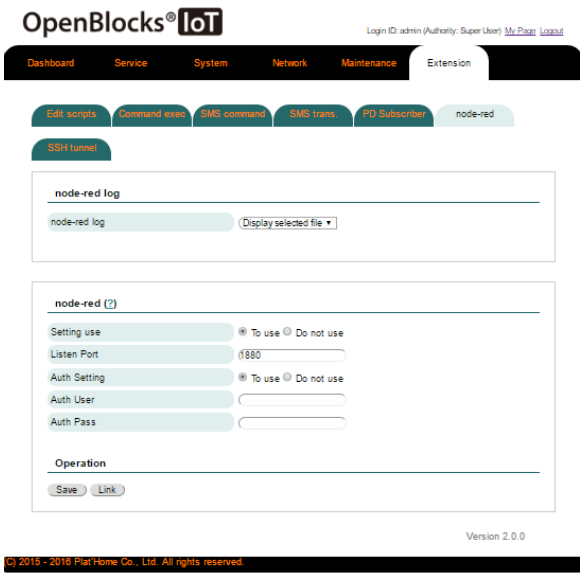
Up to 70 characters can be entered in the body.

SMS is sent by entering the telephone number and text and pressing the "send" button.

7-21. Using Node-RED

This product has Node - RED installed.

To use this function, you need to enable filter for Node-RED in section 7-5. Filter permission".



<u>node-red log</u>

node-red log :

Select the logs to be displayed from the pull-down menu.

<u>node-red</u>

Setting use :

To use Node-RED, select [To use].

Listen Port :

Specify the port number for Node-RED.

Auth Setting:

When using BASIC authentication for Node - RED connection, select [To use].

Auth User:

Specify the user name for authentication.

Auth Pass:

Specify the password for authentication.

When setting is completed, press "Save" button.

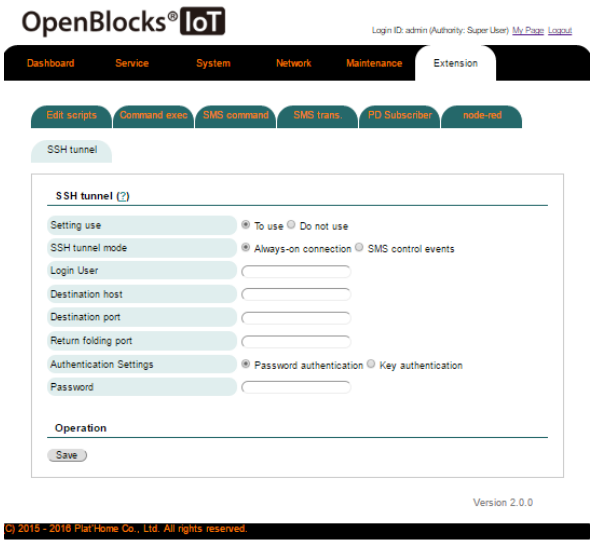
Press the link button creates a new TAB in the Web browser to connect to Node-RED GUI.

7-22. SSH Revers tunnel

SSH connection to the any SSH server and build a revers tunnel.

This makes it possible to SSH access from the SSH server to the Openblocks IoT VX 1 side via the revers tunnel.

To use this function, you need to enable SSH filter in section 7-5. Filter permission".



<u>SSH tunnel</u>

Setting use:

Set whether to use this function. Please select "To use" when using.

SSH tunnel mode:

Select the mode to build SSH tunnel.

When select to "Always-on-connection", it will always try to build SSH tunnel while running.

When select to "SMS control events", SSH tunnel is built by SMS or SMS control direct execution.

* For SMS, an SSH tunnel is built up to 30 minutes.

Login User:

Specify the user name to log in with the SSH server.

Destination host:

Specify the IP address or FQDN of the SSH server to be connected.

Destination port:

Specify the port number of the SSH server to be connected. Usually it will be number 22.

Return folding port:

Specify the port number for accessing the device of the connection source in the SSH server.

Authentication Settings:

Select the authentication method for connecting to the SSH server.

Password:

Specify the password when the authentication method is password authentication.

Passphrase:

Specify the passphrase when the authentication method is key authentication.

Private key file:

Specify the private key file when the authentication method is key authentication.

* Please upload private key file for key authentication from [System] ⇒ [File Manage] tab. After completing the setting, please push the save button. By rebooting, this function becomes effective.

7-23. Support Information

You can check support center information related to services at [Maintenance] ⇒ [Support] tab.

*This is a sample image.

Contact information and other details are subject to changes. Check the latest information with the Web UI.

OpenBlocks IoT VX1 WEB UI Setup Guide
(Version 1, November 14, 2016)

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