Plat'Home
TECHNOLOGY to serve you.

OpenBlocks IoT Family
WEB UI Set-up Guide

Version 3.2.0

Plat'Home Co., Ltd.

■ About trademarks

- Linux is a trademark or registered trademark of Linus Torvalds in the United States and/or other countries.
- Firefox is a registered trademark of the Mozilla Foundation in the United States and/or other countries.
- Google Chrome is a registered trademark of Google Inc.
- Microsoft and .NET, Windows, Microsoft Azure, Internet Explorer are registered trademark of the Microsoft Corporation in the United States and/or other countries.
- Company and product names mentioned in this Set-up Guide may be trademarks or registered trademarks of their respective companies.
- Product names and other proper nouns in this Set-up Guide are trademarks or registered trademarks of their respective companies.
- Docker and Docker logo are trademarks or registered trademarks of Docker, Inc. in the United States and/or other countries. Docker, Inc. and other parties may also have trademark rights in other terms used herein.

■ Before using this product

- No reproduction of this material is allowed without written permission of Plat'Home Co., Ltd.
- Content and information contained within this material may be changed or updated without prior notice.
- We consistently aim to keep the content in this material as precise as possible. However, should any errors in descriptions, etc. be noticed, please contact Plat'Home Co., Ltd. The latest version of this material can be downloaded from our website.
- While using this product, please be aware that it is not designed or assumed for use in fields where there is a risk to life.
- Regardless of the aforementioned, in no event will Plat'Home be liable for any special, incidental, indirect or consequential damage arising out of use of this product, including but not limited to damage to profits or loss.

Table of contents

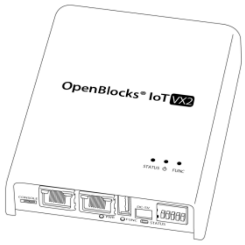
Chapter 1 General

This manual describes how to set up OpenBlocks IoT Family products via a web user interface (hereinafter referred to as "WEB UI"). For setup, a client device (PC, smartphone, tablet PC, etc.) that can use a web browser is required.

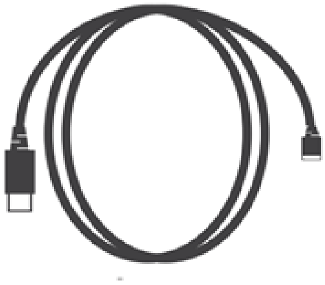
1-1. Items included in package for VX2

The standard configuration of OpenBlocks IoT VX2 is as follows:

1 x VX2 main body



1 x USB Type-A Micro USB cable



1 x Start-up Guide

ver 1.1

OpenBlocks IoT VX2

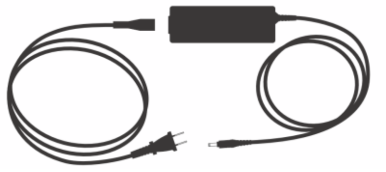
Start-up Guide

- Warranty
- Services included in package
- Agreements
- About software
- Items included in package
- Inquiries
- Safety precautions
- For the safe use of IoT device
- Precautions when using BT/WLAN
- Other precautions

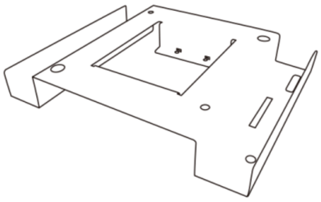
⚠ Carefully read the Start-up Guide (this leaflet, including Warranty), before actually using the product.
https://www.plathome.co.jp/support/

<1>

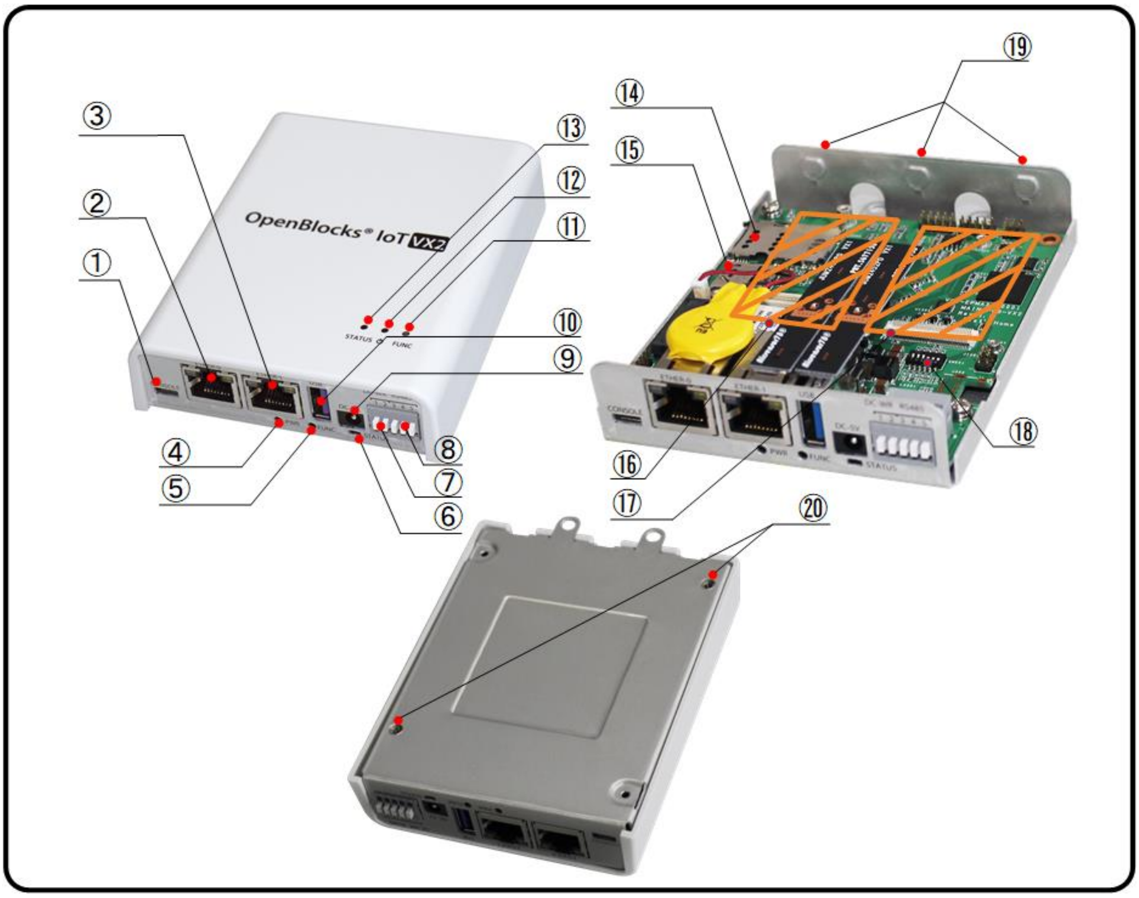
1 x AC adapter



1 x Heat radiation and installation bracket



1-2. Names of parts (VX2 main body)



No.	Name	Remarks
①	USB serial console port	Micro USB Micro-B
②	Ethernet port 0	10BASE-T / 100BASE-TX / 1000BASE-T
③	Ethernet port 1	10BASE-T / 100BASE-TX / 1000BASE-T
④	Power switch	Shuts down OS if in operation. Starts up OS if not in operation.
⑤	FUNC switch	Enables allocated function.
⑥	Status indicator	LEDs illuminate or flash in seven colors.
⑦	RS-485 (half duplex) connector	
⑧	Wide range power supply input	
⑨	USB host mode port	A-Type/USB3.0
⑩	USB host mode port	A-Type/USB3.0
⑪	FUNC switch	Enables allocated function.

No.	Name	Remarks
⑫	Power switch	Shuts down OS if in operation. Starts up OS if not in operation.
⑬	Status indicator	LEDs illuminate or flash in seven colors.
⑭	SIM slot	Slot to insert SIM card. *Supports mini-SIM card format (2FF) (standard SIM)
⑮	MMC slot	As MMC cards cannot secure sufficient reliability for system operations, use them for file exchanges and log storage only.
⑯	Expansion slot 2	Expansion slot for EnOcean, Wi-SUN and other modules.
⑰	Expansion slot 1	Expansion slot of mobile adapter card for mobile networks. A mobile adapter card supporting carrier To be use is mounted. Essentially, this is a factory option.
⑱	DIP switch	As this switch is set before factory shipment, do not alter the settings. SW1-3: For modem identification SW4-5: Not used SW6: OFF=RS485 terminator ON (default)
⑲	Hole to install external antenna	Holes are unopened in image.
⑳	Holes to mount heat radiation and installation bracket	

*To insert a SIM card, turn the VX2 main body upside down and insert into the back of the slot. Similarly, to remove a SIM card, turn the VX2 main body upside down and extract the card.

●Modem type identification

Modem type	SW1	SW2	SW3
3G module	ON	OFF	OFF
Modem uninstalled	ON	ON	ON

1-3. Status indicator

The status indicator of the OpenBlocks IoT Family uses seven LED colors to indicate status. Each status and its indication are as follows:

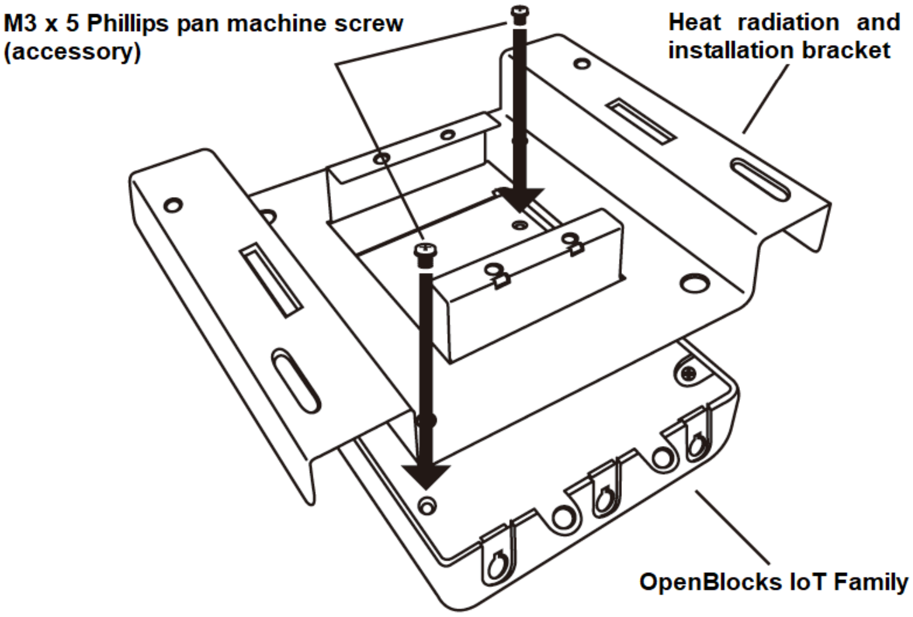
Status	Color	Illumination status	Remarks
Main body and OS in operation	Yellow	Illuminating	After completing startup of the main body and OS, the unit will begin to check for signal reception in the mobile network. *Flashes green if no SIM card is inserted.
When the SIM slot is unused	Green	Flashing	Normal operation without a SIM card or in a waiting status before changing over to waiting for signal reception
Mobile network signal: Strong	White	Flashing	Refer to "Details of signal status"
Mobile network signal: Medium	Light blue	Flashing	Refer to "Details of signal status"
Mobile network signal: Weak	Blue	Flashing	Refer to "Details of signal status" *Communication at this field intensity may cause frequent retrials. Therefore, if a mobile network is used, use the unit with a medium field strength or better.
Mobile network signal: No signal	Purple	Flashing	Refer to "Details of signal status"
When the function is enabled by FUNC button	Yellow	Flashing	Alternately flashes with the status indicator displaying that the mobile network or SIM slot is not used.
Terminating OS	Yellow	Illuminated	
Initial trial to access AirManage failed	Red	Illuminated	This indication is shown when initial access to AirManage remote control server has failed. If no WEB UI is used, the OS will start to terminate in five minutes.
OS terminating after an initial access to AirManage remote control server has failed.	Red	Flashing	

*Details of signal status

Model type	Signal: Strong	Signal: Medium	Signal: Weak	Signal: No signal
3G module	-87 dBm or higher	-88 to -108 dBm	-109 to -112 dBm	-113 dBm or lower

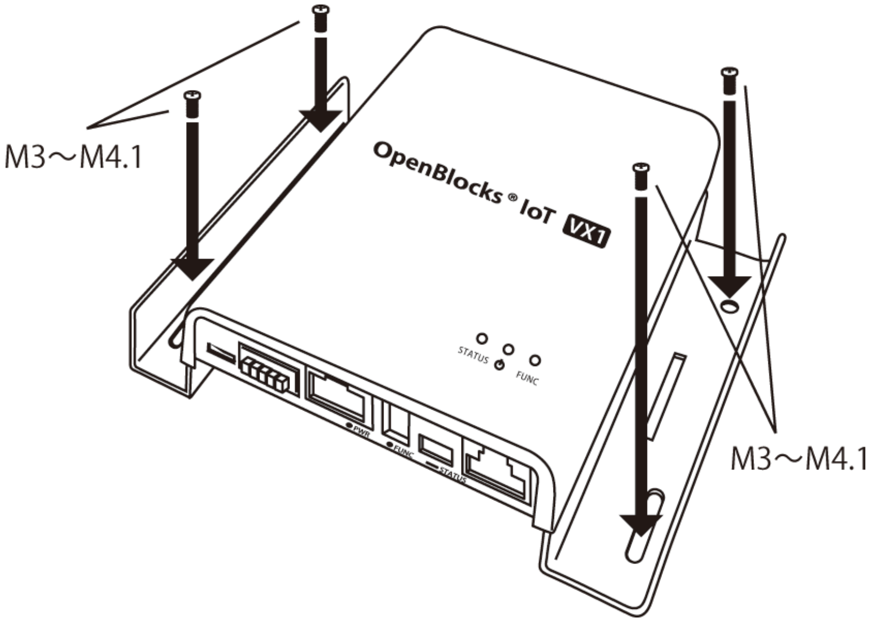
1-4. How to mount heat radiation and installation bracket

●Mounting onto OpenBlocks IoT VX series main body


M3 x 5 Phillips pan machine screw (accessory)
Heat radiation and installation bracket
OpenBlocks IoT Family

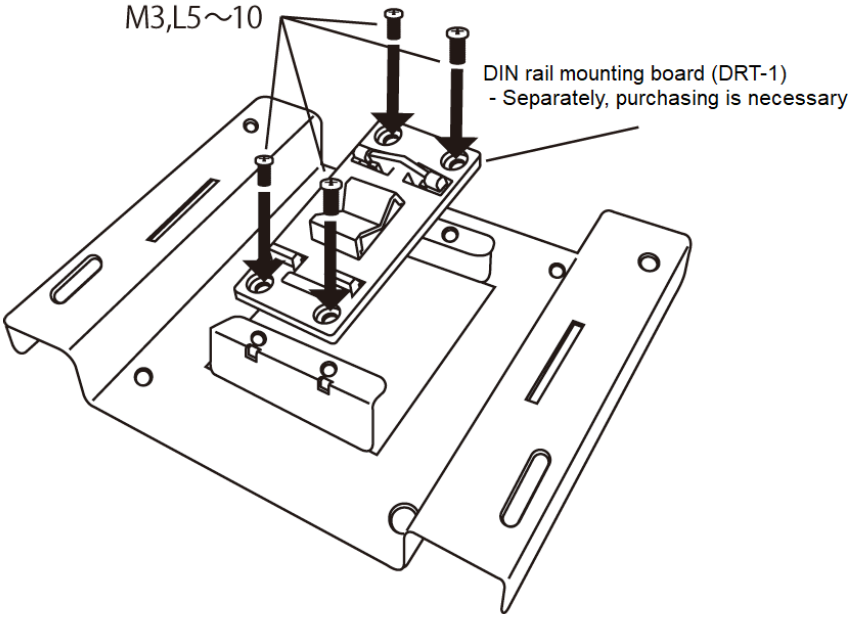
Align the holes at the back of OpenBlocks IoT VX series main body with the two holes diagonally located on the heat radiation and installation bracket and affix them together using an M3 x 5 Phillips pan machine screw (accessory) from the top.

●Mounting onto a wall, etc.



Mount the OpenBlocks IoT VX series main body equipped with the heat radiation and installation bracket to a cabinet or wall by using M3 or M4 machine screws*1 or 3 or 4.1 tapping screws*1.

●Mounting onto DIN rail


M3,L5～10
DIN rail mounting board (DRT-1)
- Separately, purchasing is necessary

Mount the DIN rail mounting board (DRT-1; optional) onto the heat radiation and installation bracket by using M3 L5 or 10 machine screws*1.

*1: To be purchased separately.

Chapter 2: Before starting to use the unit

2-1. About SIM cards

SIM cards that can be mounted onto OpenBlocks IoT Family are in a mini-SIM (2FF) format. If there is a need to use micro-SIM or nano-SIM cards, use an adapter that can fix a SIM card with a fall-preventing film and adhesive tape. Please note that any damage to the SIM slot while a SIM adapter is used will be subject to repair on an at-cost basis.

2-2 Installation of OpenBlocks IoT Family

Connect OpenBlocks IoT series unit to a power supply by using the AC adapter included in the package.

*Please note that for the OpenBlocks IoT VX series, any operation using a power supply other than the AC adapter or wide-range power supply input will not come under the scope of our support.

When unit is ready, the status indicator will illuminate/flash.
(Indication colors vary, depending on actual status).

2-3. Preparation of web client

To access WEB UI of this product, a web client is necessary.

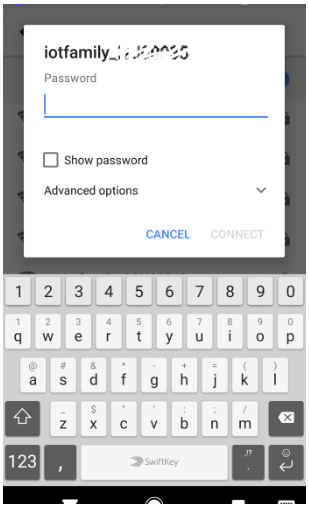
As a web client, PCs that can use Ethernet or connect to WLAN can be used, in addition to tablet computers and smartphones.

Select access point (SSID) of the unit and establish a connection via WLAN settings.

●WLAN connection

The snapshot on the right shows a smartphone screen where the SSID of the unit (iotfamily_"serial number of the unit") from a list of SSIDs on SLAN. Establish a connection by entering default password at the time of shipment, "openblocks".

After making a connection via WLAN, use a web browser to access the address in the table below.

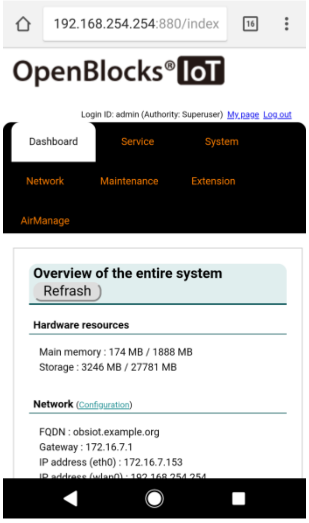

iotfamily_[redacted]

Password

□ Show password

Advanced options

When SSID is selected


192.168.254.254:880/index

OpenBlocks® IoT

Login ID: admin (Authority: Superuser) My page Log out

Overview of the entire system

Hardware resources

Main memory : 174 MB / 1888 MB
Storage : 3246 MB / 27781 MB

Network (Configuration)

FQDN : obsiot.example.org
Gateway : 172.16.7.1
IP address (eth0) : 172.16.7.153
IP address (wlan0) : 192.168.254.254

WEB screen

●Ethernet connection

Set IP address of web client to connect to an IP address that can access the network with an IP address of 192.168.253.0 (other than 254) and use a web browser to access the address in the table below.

*Serial number of the unit is shown at the back of the chassis.

	URL via WLAN	URL for Ethernet connection
HTTP connection	http://192.168.254.254:880	http://192.168.253.254:880
HTTPS connection	https://192.168.254.254:4430	https://192.168.253.254:4430

*As a web browser to use as a web client from PCs, the latest versions of Google Chrome and Firefox are supported. As no operation is available for Internet Explorer, do not use this browser.

Chapter 3: Initial basic settings for WEB UI

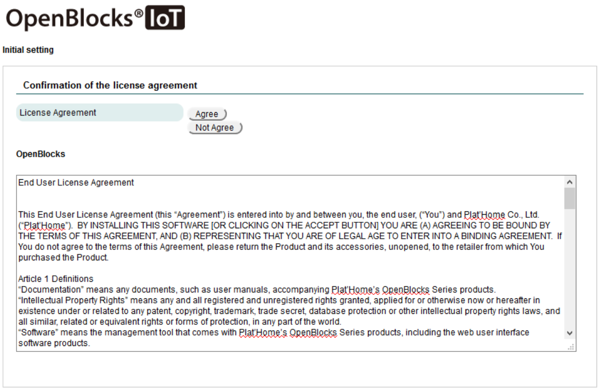
This Chapter describes the initial basic settings using WEB UI.

Chapter 3-1 through 3-3 are the initial basic setting procedures required when turning on the power for the first time. Otherwise, please refer to Chapter 3-4 and the Chapters that follow. In addition, please note that Chapter 3-1 through 3-3 describe a minimum procedure for the initial basic settings of the OpenBlocks IoT Family, giving an account of minimum network settings as a mobile router or as an independent server.

Attention:

The setting of the administrator account in Chapter 3-2 in this chapter is very important in terms of security. Therefore, set a password that is difficult to be compromised.

3-1 License agreement screen



End User License Agreement

This End User License Agreement (this "Agreement") is entered into by and between you, the end user, ("You") and Plat'Home Co., Ltd. ("Plat'Home"). BY INSTALLING THIS SOFTWARE [OR CLICKING ON THE ACCEPT BUTTON] YOU ARE (A) AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, AND (B) REPRESENTING THAT YOU ARE OF LEGAL AGE TO ENTER INTO A BINDING AGREEMENT. If You do not agree to the terms of this Agreement, please return the Product and its accessories, unopened, to the retailer from which You purchased the Product.

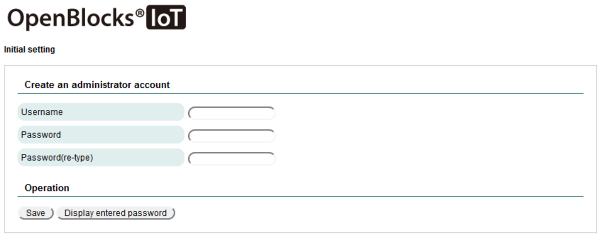
Article 1 Definitions
"Documentation" means any documents, such as user manuals, accompanying Plat'Home's OpenBlocks Series products.
"Intellectual Property Rights" means any and all registered and unregistered rights granted, applied for or otherwise now or hereafter in existence under or related to any patent, copyright, trademark, trade secret, database protection or other intellectual property rights laws, and all similar, related or equivalent rights or forms of protection, in any part of the world.
"Software" means the management tool that comes with Plat'Home's OpenBlocks Series products, including the web user interface software products.

Immediately following shipment without settings by a customer, the license agreement screen for the unit will be displayed.

The customer can use the unit only by agreeing in full with the license agreement.

Read through the agreement by scrolling down the screen. Upon agreement with the content, choose "I agree" and proceed to the next screen. By choosing "I do not agree," you will be redirected to a Google screen.

3-2 Setting up administrator account (WEB UI administrator account)



OpenBlocks® IoT

Initial setting

Create an administrator account

Username

Password

Password(re-type)

Operation

Upon agreement with the license agreement, an initial setting screen to enter WEB UI administrator account and password will be displayed.

To see the password being entered, press the Display entered password. button

Precaution: **Administrator account**

The username for the WEB UI administrator entered from this screen cannot be changed a later point. Use extra caution when entering a username. Also, please note that this account has the authority to change the root user's password.

After entering account information and pressing "Save," it will write and save initial configuration information.

Once configuration is saved, the screens in Chapter 3-1 and 3-2 will not be displayed the next time access is made.

The initial screen for web access will be the log-in screen for the administrator.

*It can change the WEB UI administrator account after the initial basic setting using the **[System]-[WEB user]** tab.

3-3. Network setting screen

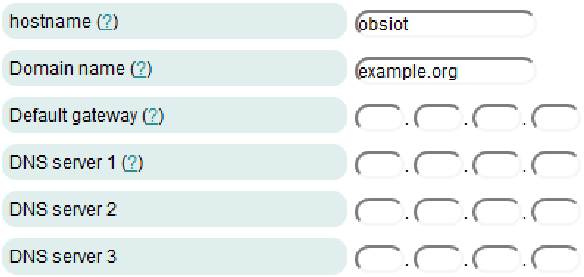
This network setting screen requires the minimum settings to use OpenBlocks IoT Family.

This Chapter describes the basic and common part of the network setting used the **[Network]-[Basic]** tab.

The following description is based on a product mounted with a modem module.

Two types of configurations are available: a configuration to use the unit as a mobile router and a configuration to use the unit as a server, without using a mobile network.

As shown in the illustration below, in the upper part of screen of the **[Network]-[Basic]** tab, there is a box to enter the name of the unit.



hostname (?)	obsiot
Domain name (?)	example.org
Default gateway (?)	. . .
DNS server 1 (?)	. . .
DNS server 2	. . .
DNS server 3	. . .

Host name:

The name of this unit as a server.

Domain name:

Name of the network domain this unit belongs to:

Default gateway:

If an IP is dynamically acquired using DHCP, setting is not required.

DNS server 1/2/3:

If an IP is dynamically acquired using DHCP, setting is not required.

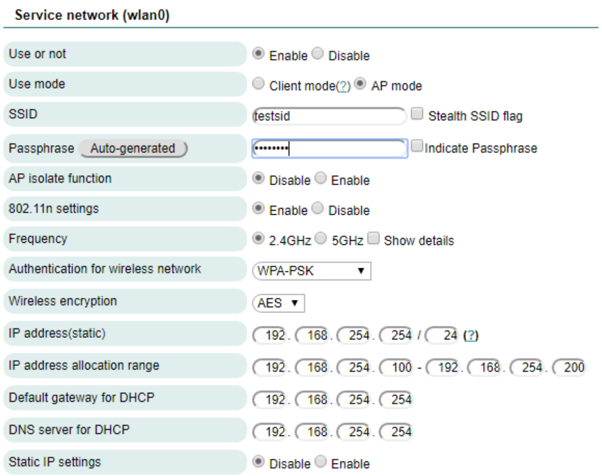
If setting these items, at least one item must be set up. The setting of two or more servers is recommended.

In Chapter 3-3-1 "Mobile router configuration" and Charpter 3-3-2 "Server configuration," the setting methods are different.

The setting screen is the same as the above, and this Chapter describes how to put the setting items in the lower side of the screen.

3-3-1. Mobile router configuration

This Chapter describes the setting method when using this unit as a mobile router using the **Service network** menu in the **[Network]-[Basic]** tab.



Service network (wlan0)

Use or not	● Enable ○ Disable
Use mode	○ Client mode(?) ● AP mode
SSID	testsid □ Stealth SSID flag
Passphrase Auto-generated	•••••••• □ Indicate Passphrase
AP isolate function	● Disable ○ Enable
802.11n settings	● Enable ○ Disable
Frequency	● 2.4GHz ○ 5GHz □ Show details
Authentication for wireless network	WPA-PSK ▼
Wireless encryption	AES ▼
IP address(static)	192 . 168 . 254 . 254 / 24 (?)
IP address allocation range	192 . 168 . 254 . 100 - 192 . 168 . 254 . 200
Default gateway for DHCP	192 . 168 . 254 . 254
DNS server for DHCP	192 . 168 . 254 . 254
Static IP settings	● Disable ○ Enable

Service network (wlanN)

To be use:[*1]

Choose "To be use."

Use mode:

Choose "AP mode."

Frequency:

Choose either "2.4GHz" or "5GHz."

SSID:

Enter an access point name.

To hide SSID from general users, check "Stealth SSID flag."

Authentication for wireless network/Wireless encryption:

Choose a mode from the pull-down menu. It is possible to use a default setting.

Passphrase: (Security key)

Password must have at least eight characters.

AP isolate function:

This function disables communication among clients when the unit is started up as an AP.

802.11n To be use:

Use this item to set up if the unit uses 802.11n when used as an AP.

IP address:

Enter this unit's IP address, in addition to a bit number for net mask for WLAN.

IP address allocation range:

For this setting, the IP address allocation can be set in order to function as a DHCP server.

Default gateway for DHCP use:

DNS server for DHCP

These items set IP addresses of the default gateway and DNS to notify DHCP clients.

Static IP setting:

This item enables/disables static IP settings To be use for a static IP allocation.

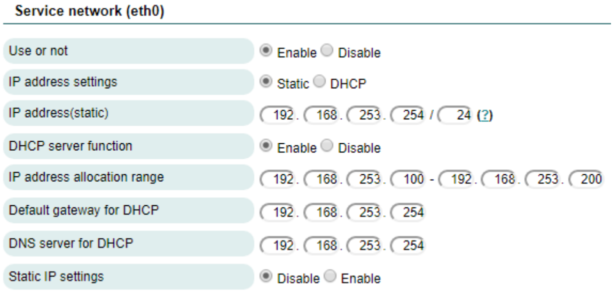
Service network (ethN)

To be use:

Choose "To be use" only if a service network (Ethernet-n) is used.

IP address settings:

This item sets an IP address for Ethernet. If a static IP setting is selected, the following items will be displayed.



Service network (eth0)

Use or not	● Enable ○ Disable
IP address settings	● Static ○ DHCP
IP address(static)	192 . 168 . 253 . 254 / 24 (?)
DHCP server function	● Enable ○ Disable
IP address allocation range	192 . 168 . 253 . 100 - 192 . 168 . 253 . 200
Default gateway for DHCP	192 . 168 . 253 . 254
DNS server for DHCP	192 . 168 . 253 . 254
Static IP settings	● Disable ○ Enable

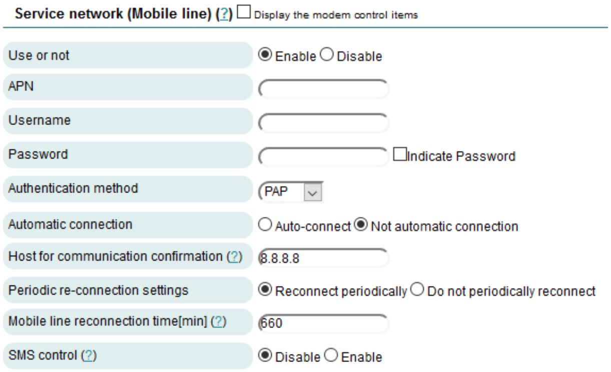
IP address (Static):

When using a static address, set an IP address from this item.

DHCP server function:

As is the case with service network (Wireless LAN), choose "To be use" when using the DHCP function.

Similarly, the setting items are "Default gateway for DHCP," "DNS server for DHCP" and "Static IP settings."



Service network (Mobile line) (?) □ Display the modem control items

Use or not	● Enable ○ Disable
APN	
Username	
Password	□Indicate Password
Authentication method	PAP
Automatic connection	○ Auto-connect ● Not automatic connection
Host for communication confirmation (?)	8.8.8.8
Periodic re-connection settings	● Reconnect periodically ○ Do not periodically reconnect
Mobile line reconnection time[min] (?)	660
SMS control (?)	● Disable ○ Enable

Service network (Mobile line)

It is not necessary to check "Display modem control items."

To be use:

Choose "To be use."

APN:

Enter APN assigned by carrier.

Username:

Enter username assigned by carrier.

Password:

Enter password assigned by carrier.

Authentication method:

Choose authentication method assigned by carrier.

Automatic connection:

Choosing "Auto-connect" will automatically connect the unit to mobile network at startup.

Host for communication confirmation:

Specify host to verify if the mobile network is connected to the Internet, etc.

*If "127.0.0.1" is entered for this item, a connection check will not be carried out.

Periodic re-connection settings:

Choose if reconnections to mobile network will be periodically carried out.

Mobile line reconnection time [min]:

After making a connection to mobile network, the unit will automatically disconnect and connect to the network when the time specified in this item has elapsed.

SMS control:

Choose "Disable."

When the above settings are completed, press "Save."

Pressing the "Save" button will save settings. Network settings will be applied after rebooting, so proceed to Chapter 3-4. "Internal clock settings."

3-3-2. Server configuration

This Chapter describes the setting method when using this unit as a server on network using the **Service network** menu in the **[Network]-[Basic]** tab**.**

Service network (wlanN)

To be use[*1]:

Choose "To be use."

Use mode:

Choose "Client mode."

SSID:

Enter the SSID of access point to connect. When connecting the unit to a stealth SSID, check "Stealth SSID flag."

IP address settings:

Choose either "Static" or "DHCP."

If choosing "DHCP," make a setup so that the DHCP server assigns a static IP to this unit.

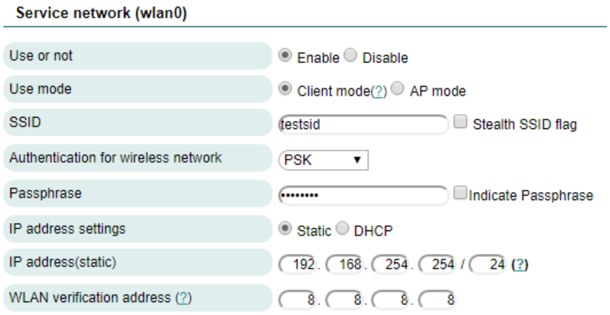
IP address (Static):

Enter an IP address if setting "IP address settings" to "Static."

WLAN verification address:

Enter IP address or FQDN of the server to send a ping to monitor the connection conditions of WLAN.

Set a device that can respond to a ping in the upstream of WLAN.



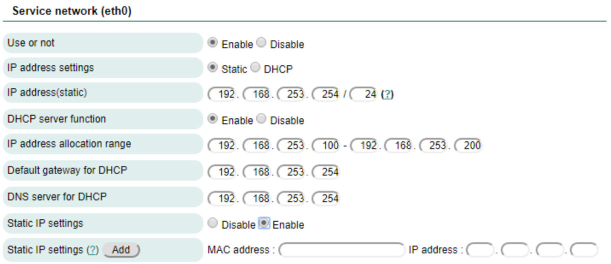
Service network (wlan0)

Use or not	● Enable ○ Disable
Use mode	● Client mode(?) ○ AP mode
SSID	testsid □ Stealth SSID flag
Authentication for wireless network	PSK ▾
Passphrase	•••••••• □Indicate Passphrase
IP address settings	● Static ○ DHCP
IP address(static)	192 . 168 . 254 . 254 / 24 (?)
WLAN verification address (?)	8 . 8 . 8 . 8

Service network (ethN)

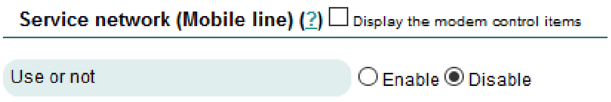
If using this, choose "To be use" for "To be use." If also using a static address, enter an IP address in "IP address (static)."

When using the DHCP function, it is necessary to set up the relevant items.



Service network (eth0)

Use or not	● Enable ○ Disable
IP address settings	● Static ○ DHCP
IP address(static)	192 . 168 . 253 . 254 / 24 (?)
DHCP server function	● Enable ○ Disable
IP address allocation range	192 . 168 . 253 . 100 - 192 . 168 . 253 . 200
Default gateway for DHCP	192 . 168 . 253 . 254
DNS server for DHCP	192 . 168 . 253 . 254
Static IP settings	○ Disable ● Enable
Static IP settings (?) Add	MAC address : IP address : . . .



Service network (Mobile line) (?) □ Display the modem control items

Use or not ○ Enable ● Disable

Service network (Mobile line)

It is not necessary to check "Display modem control items."

To be use:

Choose "Disable."

*"Display modem control items" is for developers only. For further details, refer to the Developer Guide.

When the above settings are completed, press "Save," and proceed to Chapter 3-4. "Internal clock settings."

/ **If rebooting the unit after entering an incorrect SSID:**

If registering an SSID from the upstream access point that does not exist, it will not be possible to access the unit with a general method.

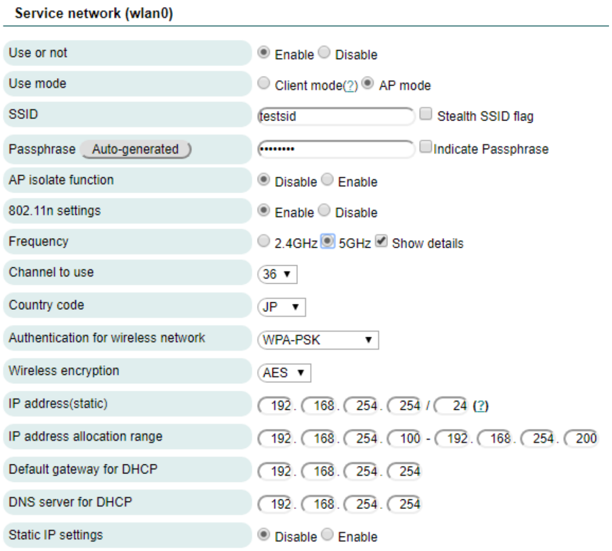
Should this be the case, reboot the unit by resetting the unit to default.

*If browser has a WEB UI session information, the previous conditions will remain on screen. Therefore, first log out and re-access the unit to start at the license agreement screen.

1. Connect a USB console to unit to make a connection with PC.
2. Press the Power switch of unit to shut down.
3. Press the Power switch after shutting unit down.
4. Choose "WEB UI init boot" from the GRUB menu.
5. Unit will reboot at factory default settings.
6. Carry out the settings of unit and reboot.

3-3-3. Advanced settings of WLAN AP mode (CH settings and overseas support)

It is possible to change channels to avoid interference or set a country code to use WLAN AP mode overseas, using the **Service network (Wireless LAN)** menu in the **[Networ]}-[Basic]** tab.



Service network (wlan0)

Use or not	● Enable ○ Disable
Use mode	○ Client mode(?) ● AP mode
SSID	testsid □ Stealth SSID flag
Passphrase Auto-generated	•••••••• □Indicate Passphrase
AP isolate function	● Disable ○ Enable
802.11n settings	● Enable ○ Disable
Frequency	○ 2.4GHz ● 5GHz ☑ Show details
Channel to use	36 ▾
Country code	JP ▾
Authentication for wireless network	WPA-PSK ▾
Wireless encryption	AES ▾
IP address(static)	192 . 168 . 254 . 254 / 24 (?)
IP address allocation range	192 . 168 . 254 . 100 - 192 . 168 . 254 . 200
Default gateway for DHCP	192 . 168 . 254 . 254
DNS server for DHCP	192 . 168 . 254 . 254
Static IP settings	● Disable ○ Enable

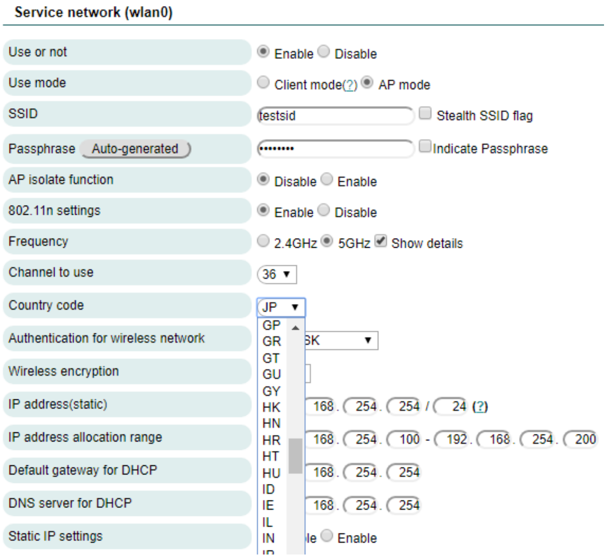
Service network (wlanN)

Use mode:

Choose "AP mode."

When "AP mode" is selected, a check box, "Show details" will be displayed to the right of Frequency.

Check this check box to display Channel to use and Country code.



Service network (wlan0)

Use or not	● Enable ○ Disable
Use mode	○ Client mode(?) ● AP mode
SSID	testsid □ Stealth SSID flag
Passphrase Auto-generated	•••••••• □Indicate Passphrase
AP isolate function	● Disable ○ Enable
802.11n settings	● Enable ○ Disable
Frequency	○ 2.4GHz ● 5GHz ☑ Show details
Channel to use	36 ▾
Country code	JP ▾
Authentication for wireless network	SK ▾
Wireless encryption	
IP address(static)	168 . 254 . 254 / 24 (?)
IP address allocation range	168 . 254 . 100 - 192 . 168 . 254 . 200
Default gateway for DHCP	168 . 254 . 254
DNS server for DHCP	168 . 254 . 254
Static IP settings	le ○ Enable

Channel to use:

Choose a channel from the pull-down menu. To find an open channel, it helps to use a smartphone application such as a WLAN channel analyzer.

The channel to use also depends on the use setting of 802.11n. Check channels that can be used in advance.

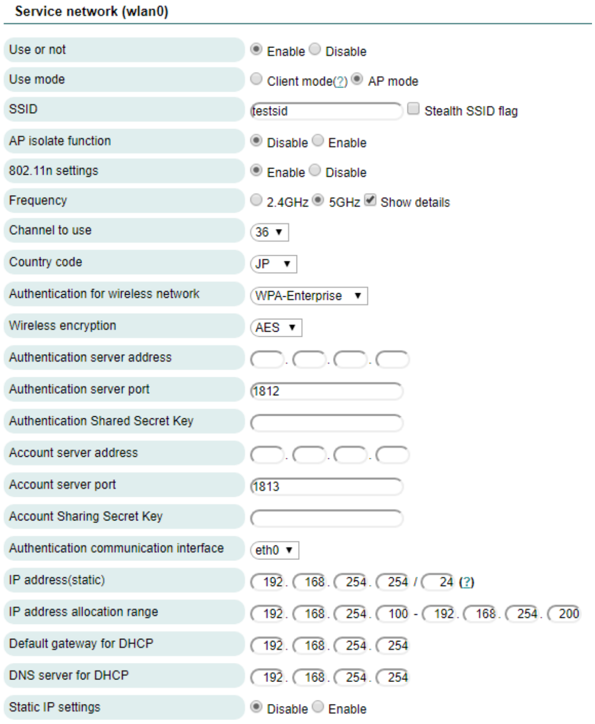
Country code:

Enter the country code responding to the country to install this unit.

For example, enter "JP" for Japan.

3-3-4 Enterprise authentication

When using WPA-Enterprise authentication or WPA 2-Enterprise authentication in AP mode, communication with the RADIUS server is required. Therefore, set up the communication destination RADIUS server and communication interface.



Service network (wlan0)

Use or not	● Enable ○ Disable
Use mode	○ Client mode(?) ● AP mode
SSID	testsid ☐ Stealth SSID flag
AP isolate function	● Disable ○ Enable
802.11n settings	● Enable ○ Disable
Frequency	○ 2.4GHz ● 5GHz ☑ Show details
Channel to use	36 ▼
Country code	JP ▼
Authentication for wireless network	WPA-Enterprise ▼
Wireless encryption	AES ▼
Authentication server address	. . .
Authentication server port	1812
Authentication Shared Secret Key	
Account server address	. . .
Account server port	1813
Account Sharing Secret Key	
Authentication communication interface	eth0 ▼
IP address(static)	192 . 168 . 254 . 254 / 24 (?)
IP address allocation range	192 . 168 . 254 . 100 - 192 . 168 . 254 . 200
Default gateway for DHCP	192 . 168 . 254 . 254
DNS server for DHCP	192 . 168 . 254 . 254
Static IP settings	● Disable ○ Enable

Service network (wlanN)

Autentication server address:

Specify the IP address of the authentication server.

Autentication server port:

Specify the port number of the authentication server.

* Usually it is not necessary to change from the default 1812.

Autentication shared secret key:

Specify the shared secret key to communicate with the authentication server.

Account server address:

Specify the IP address of the accounting server.

Account server port:

Specify the port number of the accounting server.

* Usually it is not necessary to change from the default 1813.

Account shared secret key:

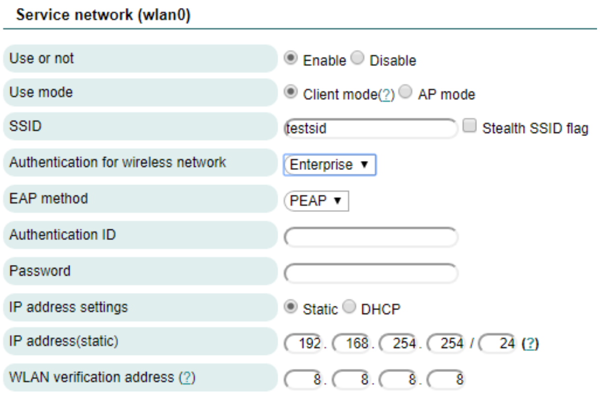
Specify the shared secret key to communicate with the accounting server.

Autentication communication interface:

Specify the interface to communicate with the authentication server and the accounting server.

When using WPA-Enterprise authentication or WPA 2-Enterprise authentication in the client mode, It necessary to set parameters of EAP method. The EAP method supports PEA and TLS.

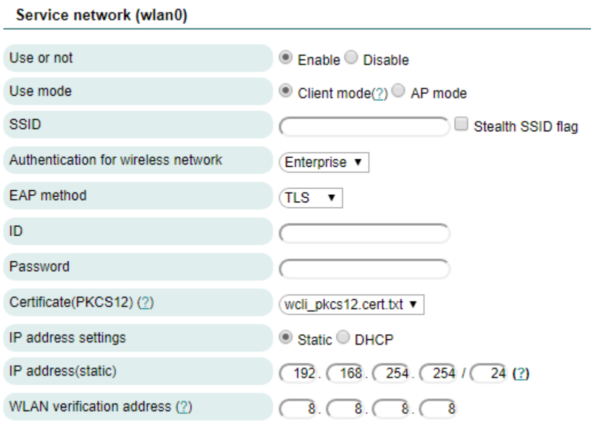
PEAP method



Service network (wlan0)

Use or not	● Enable ○ Disable
Use mode	● Client mode(?) ○ AP mode
SSID	testsid □ Stealth SSID flag
Authentication for wireless network	Enterprise ▾
EAP method	PEAP ▾
Authentication ID	
Password	
IP address settings	● Static ○ DHCP
IP address(static)	192 . 168 . 254 . 254 / 24 (?)
WLAN verification address (?)	8 . 8 . 8 . 8

TLS method



Service network (wlan0)

Use or not	● Enable ○ Disable
Use mode	● Client mode(?) ○ AP mode
SSID	□ Stealth SSID flag
Authentication for wireless network	Enterprise ▾
EAP method	TLS ▾
ID	
Password	
Certificate(PKCS12) (?)	wcli_pkcs12.cert.txt ▾
IP address settings	● Static ○ DHCP
IP address(static)	192 . 168 . 254 . 254 / 24 (?)
WLAN verification address (?)	8 . 8 . 8 . 8

Service network (wlanN)

EAP method:

Select either PEAP or TLS.

Authentication ID (for PEAP):

Specify the authentication ID to connecting.

Password (for PEAP):

Specify the password to conectiong.

ID (for TLS):

Specify the ID to connecting.

Password (for TLS):

Specify the password of the PKCS12 certificate.

Certificate(PKCS12) (for TLS) :

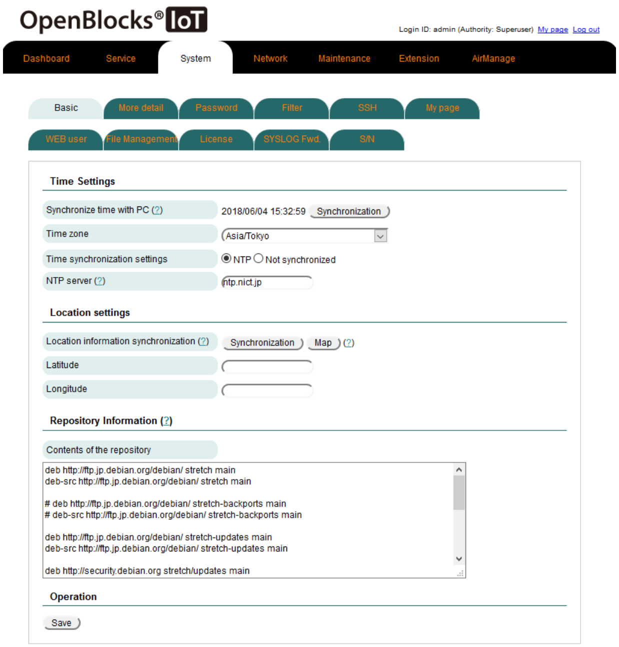
Select the PKCS12 certificate to be used for authentication.

*Upload the certificate file using the **Certificat of WLAN** menu in the **[Network]-[WLAN Cert]** tab.

3-4. Internal clock settings

This product has a backup battery for RTC, but it is recommended to synchronize the unit with an NTP server, using **Time setting** menu in the **[System]-[Basic]** tab.

However, if the unit is used in an environment where an NTP server is not available, it is possible to synchronize the time of the unit with that of a PC or smartphone on which this unit's WEB UI is displayed.



Time Settings

Synchronize time with PC (?)	2018/06/04 15:32:59 Synchronization
Time zone	Asia/Tokyo
Time synchronization settings	● NTP ○ Not synchronized
NTP server (?)	ntp.nict.jp

Location settings

Location information synchronization (?)	Synchronization Map (?)
Latitude	
Longitude	

Repository Information (?)

Contents of the repository

```
deb http://ftp.jp.debian.org/debian/ stretch main
deb-src http://ftp.jp.debian.org/debian/ stretch main

# deb http://ftp.jp.debian.org/debian/ stretch-backports main
# deb-src http://ftp.jp.debian.org/debian/ stretch-backports main

deb http://ftp.jp.debian.org/debian/ stretch-updates main
deb-src http://ftp.jp.debian.org/debian/ stretch-updates main

deb http://security.debian.org stretch/updates main
```

Operation

Time settings

Synchronize time with PC:

Press "Synchronization" to reflect the time of the PC displaying the WEB.

Time zone:

Choose the region where the unit is installed from the pull-down menu.

Time synchronization settings:

Use this item to set up a time synchronization method. Normally, choose "NTP."

NTP server (when NTP is chosen):

Enter IP address or FQDN of NTP server.

Location settings

Location information synchronization:

Press "Synchronization" to reflect location information maintained in browser. (This function should be implemented with HTTPS connection).

Press "Map" to display location information on GoogleMap.

Latitude:

Enter latitude information.

Longitude:

Enter longitude information.

Repository information

Contents of repository:

This box with a scroll bar shows a repository of software update information of this unit. This box cannot be edited directly.

To edit the content, log in with CUI using an SSH, etc. and edit "/etc/apt/sources.list" file.

(All editing and subsequent results are the sole responsibility of customer).

After editing, press "Save" to save settings. Though no rebooting is essentially necessary, rebooting is recommended to reflect time zone information, etc. of applications being used.

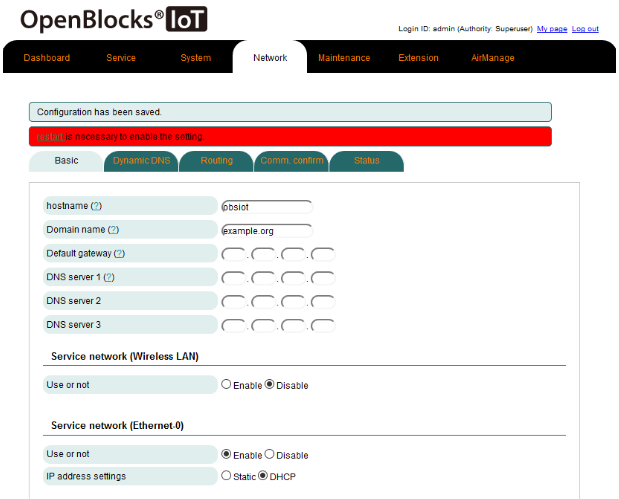
This is it for the basic settings necessary to operate the OpenBlocks IoT Family.

After settings are completed, carry out a system reboot in the following section.

3-5. Reflecting changes in settings by rebooting the system

Minimum settings necessary to operate the Open Blocks IoT Family have been discussed above. For other setting times, refer to relevant descriptions as necessary.

This section describes how to reboot the system so that after basic network settings, the system will reflect such changes.



Configuration has been saved.

restart is necessary to enable the setting.

hostname (?)	obsiot
Domain name (?)	example.org
Default gateway (?)	. . .
DNS server 1 (?)	. . .
DNS server 2	. . .
DNS server 3	. . .

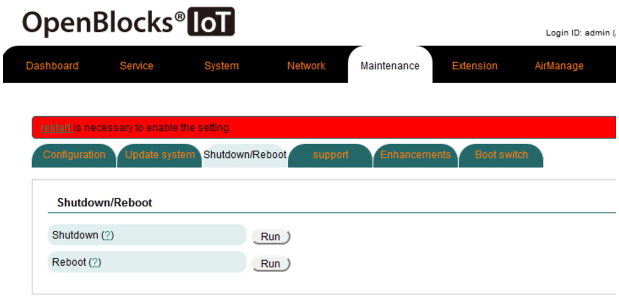
Service network (Wireless LAN)

Use or not	○ Enable ● Disable

Service network (Ethernet-0)

Use or not	● Enable ○ Disable
IP address settings	○ Static ● DHCP

After completing basic settings and pressing "Save," a message prompting a reboot of the system will be displayed at the top of the web screen as shown in the illustration on the left. To reboot the system, click the "Reboot" link as shown in the red box. Clicking this link will display the **Shutdown/Maintenance** menu in the **[Maintenance]-[Shutdown/Reboot]** tab.



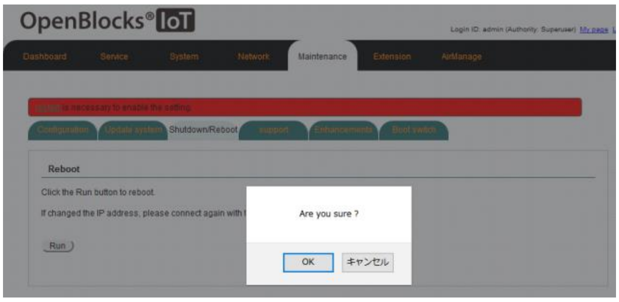
restart is necessary to enable the setting.

Shutdown/Reboot

Shutdown (?)

Reboot (?)

Click "Run" next to Reboot.



restart is necessary to enable the setting.

Reboot

Click the Run button to reboot.

If changed the IP address, please connect again with t

Are you sure ?

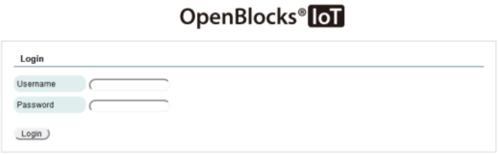
A reboot confirmation screen will be displayed. Press "Run" to show the final confirmation window.

This is the final confirmation. Press "OK" to reboot the system.

Wait for reboot to be completed. This process depends on system conditions, but please wait for seconds to be displayed.

If accessing WEB UI via a wireless network and if the OpenBlocks IoT Family is in AP mode, a reconnection to the unit will take place after rebooting. To show the log-in screen after rebooting, it is necessary to reload via a web browser.

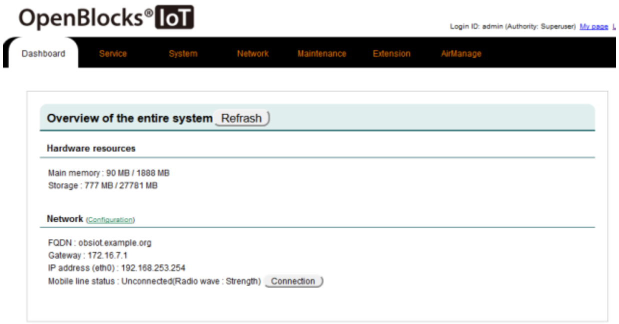
3-6. Administrator log-in screen



This is the first screen that will be displayed, if the unit is not on factory default conditions.

After logging out, this screen will be displayed next time. Please log in from here.

3-7. Dashboard screen



Overview of the entire system

Hardware resources

Main memory : 90 MB / 1888 MB
Storage : 777 MB / 27781 MB

Network

FQDN : obsiot.example.org
Gateway : 172.16.7.1
IP address (eth0) : 192.168.253.254
Mobile line status : Unconnected(Radio wave : Strength)

This is the first screen that will be displayed when logging in to WEB UI of this unit.

This screen shows information such as hardware resources and network information of the OpenBlocks IoT Family.

To update screen to show the latest information, press "Refrash."

Chapter 4: SMS control

The OpenBlocks IoT Family supports a Short Message Service (hereinafter referred to as “SMS”) for some mobile network modem modules.

(Note: If a mobile network agreement does not include SMS functions, it will not be supported).

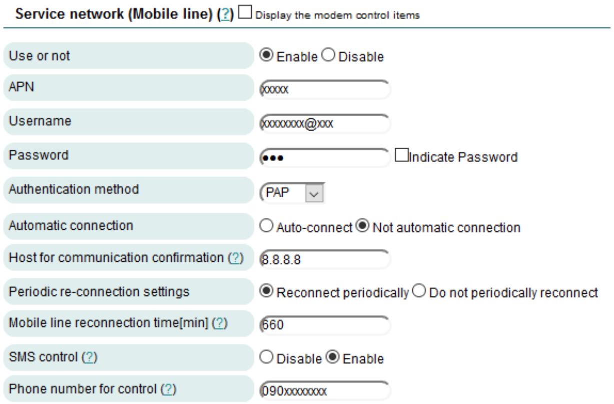
SMS in that it can be used by a cellular phone to send a messages of up to about 70 characters to a receiver's phone number. This differs from data communication that normally involves this unit .

Through receiving SMS messages with specific keywords, this unit can start or stop data communication or run shell scripts.

4-1. Startup settings for SMS control

SMS control is a function for users using mobile networks.

For mobile network settings, using the **Service network (Mobile line)** menu in the **[Network]-[Basic]** tab, refer to "Service network (Mobile network)" in Chapter 3-3-1. "Mobile router configuration."



Service network (Mobile line) (?) □ Display the modem control items

Use or not	● Enable ○ Disable
APN	xxxxx
Username	xxxxxxxx@xxx
Password	••• □Indicate Password
Authentication method	PAP
Automatic connection	○ Auto-connect ● Not automatic connection
Host for communication confirmation (?)	8.8.8.8
Periodic re-connection settings	● Reconnect periodically ○ Do not periodically reconnect
Mobile line reconnection time[min] (?)	660
SMS control (?)	○ Disable ● Enable
Phone number for control (?)	090xxxxxxxx

Service network (Mobile network)

Automatic connection:

Either setting will suffice.

If the unit is connected to a mobile network with SMS control and is disconnected by the network, a reconnection will not take place.

SMS control:

Choose "Enable."

Phone number for control

This item will be displayed when SMS control is set to "Enable."

Enter the phone number of smartphone, etc. for SMS control. Any messages other than those from this phone number will be ignored.

Enter the phone number starting with area code.

This number may be as short as four digits for SMS on private networks.

This entry is obligatory.

4-2. SMS control commands

SMS control has the following commands:

Command	Command description	Remarks
CON	Connects to mobile network.	
COFF	Disconnects from mobile network.	
SSHON	Opens SSH session.	If the OS is rebooted after opening an SSH session, this session will be automatically closed. Until rebooting, as the SSH session will remain open, close the session after use.
SSHOFF	Closes SSH session.	
REBOOT	Reboots the system.	
USCR1~USCR5	Runs a user script in the background.	A user script can be edited by the Edit scripts tab in the Extension tab of WEB UI. For registration method, refer to Chapter 4-4. "Registering user defined SMS script."
USCR1F~USCR5F	Runs user scripts in the background.	
UPGRADE	Carries out online update processing.	Fails if unit not connected to the Internet.
STUNNEL	Creates an SSH tunnel.	

4-3. Sending multiple commands using SMS

It is possible to send multiple commands in bulk with a single SMS message.

“CON," "COFF," "SSHON," "SSHOFF," "USCR1F" through "USCR5F," and "UPGRADE" are run in the foreground. For example, by connecting them with "+" in a text to be sent via SMS as exemplified below, the commands will run sequentially.

Example 1)

CON+USCR1F+USCR2F+COFF : Connect to mobile network, run script 1, run script 2 and disconnect from mobile network

Example 2)

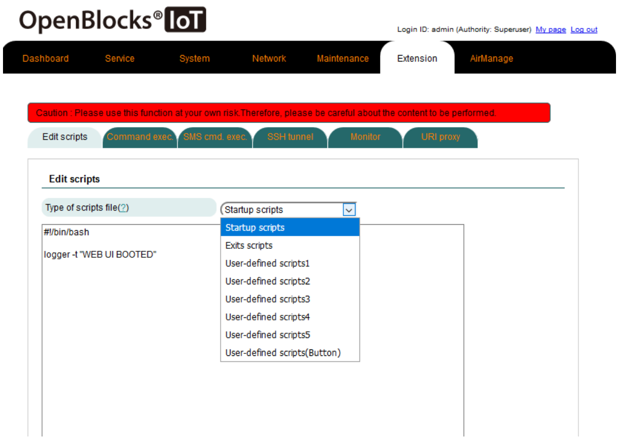
CON+SSHON : Connect to mobile network and open SSH.

SSHOFF+COFF : Close SSH and disconnect from mobile network.

*"USCR1" through "USCR5" plus "STUNNEL" are run in the background and thus processed in parallel.

4-4. Registering user defined SMS script

User-defined scripts can be registered and edited using the **[Extension]-[Script editing]** tab. Please note that this function is for users creating Linux shell scripts. Performance content of scripts do not come under the scope of our support.



Caution : Please use this function at your own risk.Therefore, please be careful about the content to be performed.

```
#!/bin/bash

logger -t "WEB UI BOOTED"
```

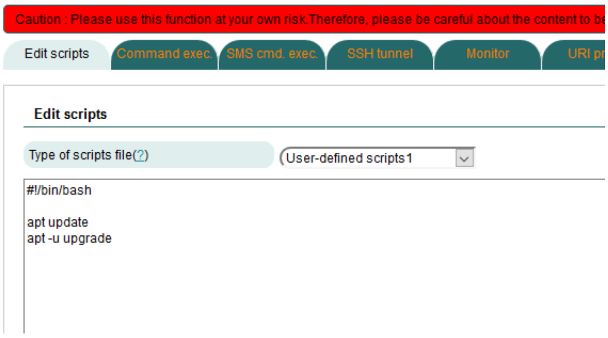
Edit scripts

Types of script file:

Choose a script to be edited from the pull-down menu.

Choose "Startup scripts," describing scripts to be automatically run at the time of starting up the OS on this unit.

Please note that scripts described in startup scripts will be run in the background.



Caution : Please use this function at your own risk.Therefore, please be careful about the content to be

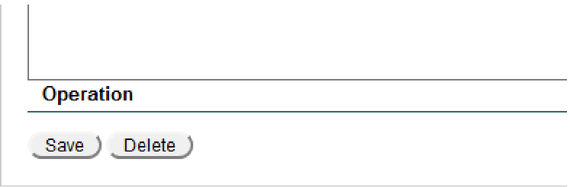
```
#!/bin/bash

apt update
apt -u upgrade
```

Describe scripts in this box.

In this script example, it is possible to update individual applications in an Internet environment.

(This script is recommended, as security updates of individual applications are frequently carried out).



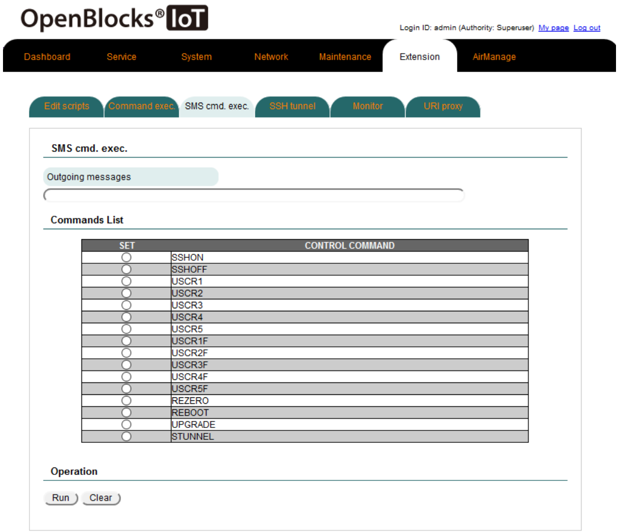
When script has been completed, press the "Save" button on the bottom left of the screen.

It is possible to delete unnecessary scripts using the "Delete" button.

*In the above example, an OS patch will be applied to this unit in a remote location via SMS.

4-5. Directly running SMS control commands

SMS control commands are issued and run normally by mobile phones but directly using the **[Extension]-[Command exec.]** tab as well.



SMS cmd. exec.

Outgoing messages

Commands List

SET	CONTROL COMMAND
○	SSHON
○	SSHOFF
○	USCR1
○	USCR2
○	USCR3
○	USCR4
○	USCR5
○	USCR1F
○	USCR2F
○	USCR3F
○	USCR4F
○	USCR5F
○	REZERO
○	REBOOT
○	UPGRADE
○	STUNNEL

Operation

SMS cmd. exec.

Outgoing messages:

Enter SMS commands to be pseudo-sent here.

Command list

When choosing a command from the "SET" column in the list, the command chosen will be added to the message to be sent. The system automatically adds "+" before the second command and beyond.

*Note: "CON" and "COFF" will only be displayed if the mobile network is set to "To be use."

Operation

Run:

Pseudo-sends the commands entered in the message to be sent.

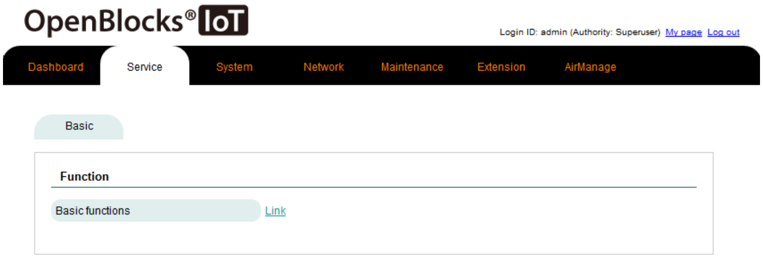
Clear:

Deletes the content of message to be sent.

Chapter 5: Service functions

The standard service functions in the OpenBlocks IoT Family support only the functions of BT interface control and the registration of various devices.

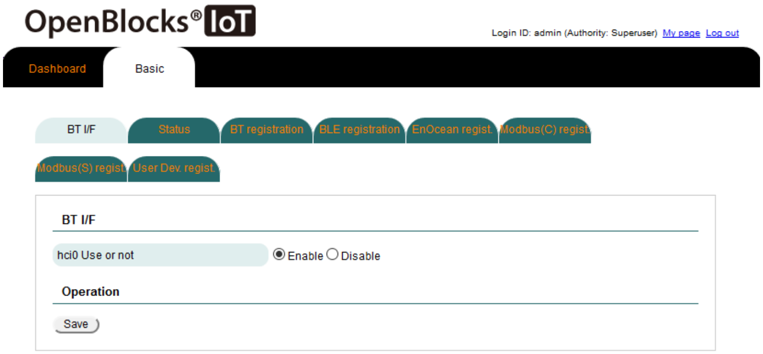
Usually, choosing the **[Service]** tab will display the screen below:



Function

Basic functions Link

Pressing **[Basic]** tab, initiates a change to the following screen:



BT I/F

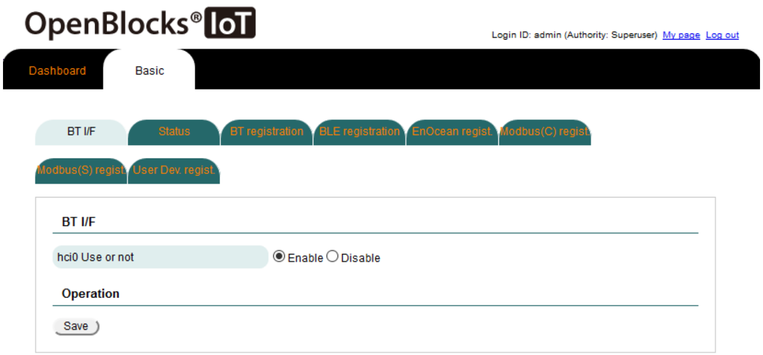
hci0 Use or not ● Enable ○ Disable

Operation

Save

5-1 BT I/F control

One of the interface that the OpenBlocks IoT Family supports by default as an IoT device is BT. Use the **[Basic]-[BT I/F]** tab to set up the BT interface control.



BT I/F

hci0 Use or not ● Enable ○ Disable

Operation

BT I/F

hci0 to be use:

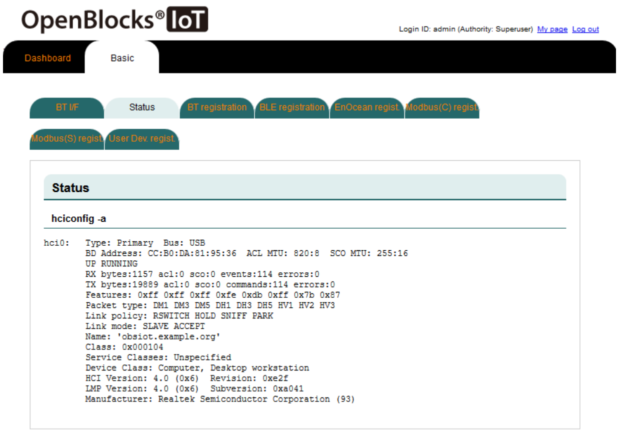
Can be set up if using the BT interface or not.

Choosing "To be use" brings the BT Interface up.

Choosing "Disable" brings the BT Interface down.

5-2 Status

The status of BT as one of the interfaces that the OpenBlocks IoT Family supports by default as an IoT device can be checked using the **[Basic]-[Status]** tab.



Status

hciconfig -a

```
hci0:   Type: Primary  Bus: USB
        BD Address: CC:B0:DA:81:95:36  ACL MTU: 820:8  SCO MTU: 255:16
        UP RUNNING
        RX bytes:1157 acl:0 sco:0 events:114 errors:0
        TX bytes:19889 acl:0 sco:0 commands:114 errors:0
        Features: 0xff 0xff 0xff 0xfe 0xdb 0xff 0x7b 0x87
        Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
        Link policy: RSWITCH HOLD SNIFF PARK
        Link mode: SLAVE ACCEPT
        Name: 'obsiot.example.org'
        Class: 0x000104
        Service Classes: Unspecified
        Device Class: Computer, Desktop workstation
        HCI Version: 4.0 (0x6)  Revision: 0xe2f
        LMP Version: 4.0 (0x6)  Subversion: 0xa041
        Manufacturer: Realtek Semiconductor Corporation (93)
```

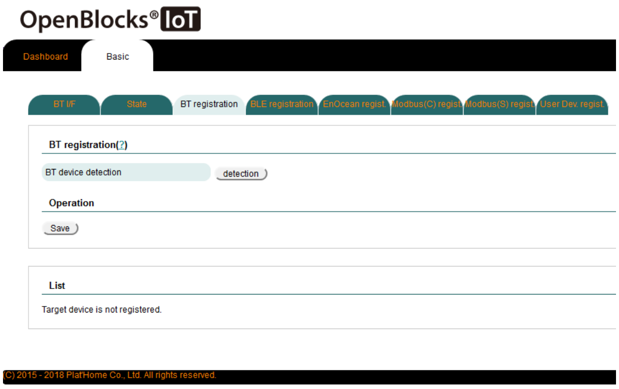
State

hciconfig -a:

Can check the status of the BT Interface.

5-3 Registering BT

If the BT Interface is up, BT devices can be registered using the **[Basic]-[BT registration]** tab.



BT registration(?)

BT device detection   detection

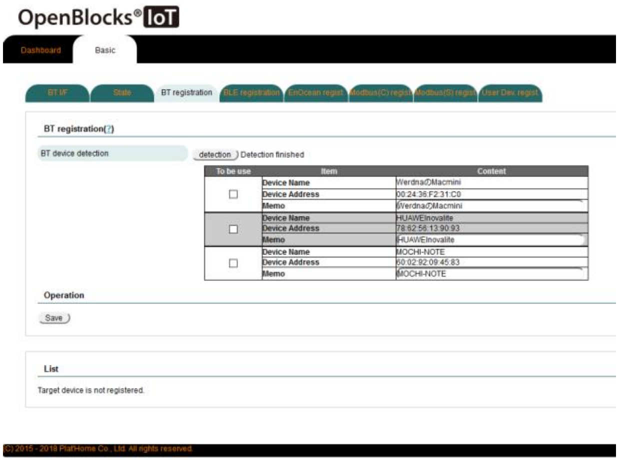
Operation

Save

List

Target device is not registered.

*After detection



BT registration(?)

BT device detection   detection   Detection finished

To be use	Item	Content
□	Device Name	WerdnaのMacmini
	Device Address	00:24:36:F2:31:C0
	Memo	WerdnaのMacmini
□	Device Name	HUAWEInovalite
	Device Address	78:62:56:13:90:93
	Memo	HUAWEInovalite
□	Device Name	MOCHI-NOTE
	Device Address	60:02:92:09:45:83
	Memo	MOCHI-NOTE

Operation

Save

List

Target device is not registered.

BT registration

BT device detection:

Press the "detection" button to show BT devices around the unit in list form.

Check boxes corresponding to BT devices to be paired in the "To be use" column to run pairing. After completing pairing, press the "Save" button to register devices.

Device name:

Device names will be displayed on the basis of discovery data acquired at the time of BT device detection.

Device address:

Device addresses will be displayed on the basis of discovery data acquired at the time of BT device detection.

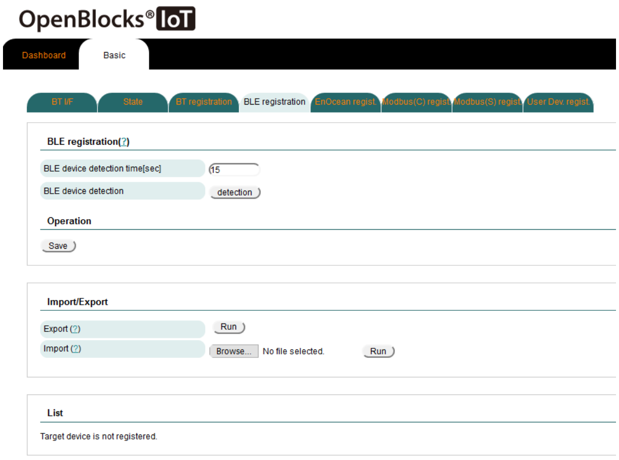
Memo:

Device names will be set up by default on the basis of discovery data acquired at the time of BT device detection. As this field can be edited, edit if any revisions are necessary.

Please note that if BT devices are registered, the field under List will display a list of registered devices. It is possible to delete devices or update the Memo information.

5-4 Registering BLE

If the BT Interface is up, BLE devices can be registered using the **[Basic]-[BLE registration]** tab.



BLE registration(?)

BLE device detection time[sec]: 15

BLE device detection

Operation

Import/Export

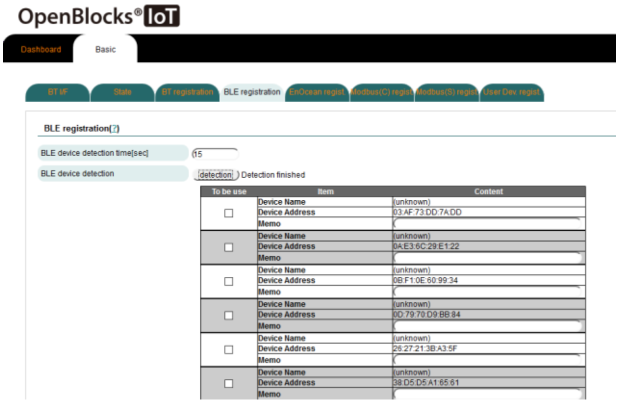
Export (?)

Import (?) No file selected.

List

Target device is not registered.

*After detection



BLE registration(?)

BLE device detection time[sec]: 15

BLE device detection: Detection finished

To be use	Item	Content
□	Device Name	(unknown)
	Device Address	03:AF:73:DD:7A:DD
	Memo	
□	Device Name	(unknown)
	Device Address	0A:E3:6C:29:E1:22
	Memo	
□	Device Name	(unknown)
	Device Address	0B:F1:0E:60:99:34
	Memo	
□	Device Name	(unknown)
	Device Address	0D:79:70:D9:BB:84
	Memo	
□	Device Name	(unknown)
	Device Address	26:27:21:3B:A3:5F
	Memo	
□	Device Name	(unknown)
	Device Address	38:D5:D5:A1:65:61
	Memo	

BLE registration

BLE device detection time (sec):

Sets up BLE device detection time in seconds.

BLE device detection

Press the "detection" button to show BLE devices around the unit in list form.

Check boxes corresponding to BLE devices to be paired in the "To be use" column. After completing pairing, press the "Save" button to register devices.

Device name:

Device names will be displayed on the basis of advertised data acquired at the time of detecting BLE devices.

Device address:

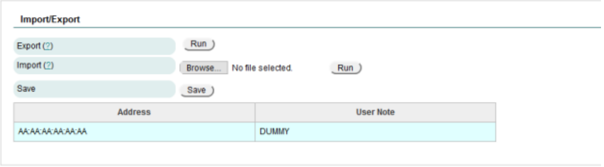
Device addresses will be displayed on the basis of advertised data acquired at the time of BT device detection.

Memo:

Device names will be set up by default on the basis of discovery data acquired at the time of BLE device detection. As this field can be edited, edit if any revisions are necessary.

Please note that if BLE devices are registered, the field under List will display a list of registered devices. It is possible to delete devices or update the Memo information.

*After importing JSON file



Address	User Note
AA:AA:AA:AA:AA:AA	DUMMY

Import/Export

Export:

Exports BLE device information maintained in this unit as a JSON file.

Import:

Choose a JSON file and import BLE device information to be registered/updated in the unit.

Save:

Saves the content of imported JSON file on BLE devices in the unit.

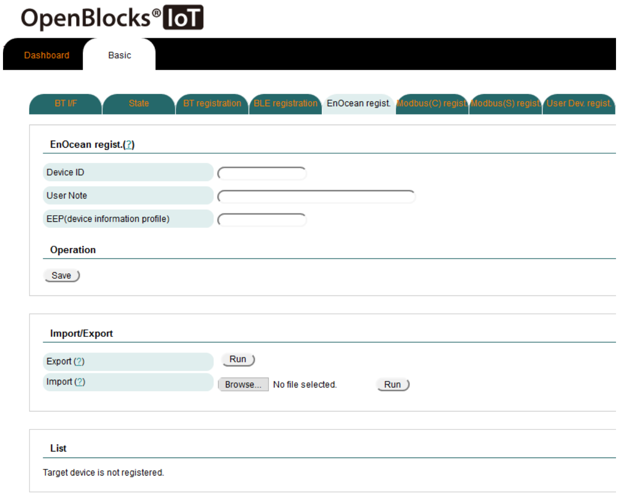
Content of the JSON file may differ, depending on the versions of WEB UI.
Please therefore create a JSON file, while referring to an exported JSON file.

5-5 EnOcean registration

*This function is recommended only in the territory of Japan.

If the EnOcean extension module is mounted on this unit, it is possible to acquire EnOcean device information. (This function is only available when the IoT control function is installed using the **[Maintenance]-[Enhancements]** tab)

It is possible to then register EnOcean devices to be registered using the **[Basic]-[EnOcean regist.]** tab.



No file selected.

Target device is not registered.

EnOcean regist.

Device ID:

Sets the device IDs of EnOcean devices to be registered.

User note:

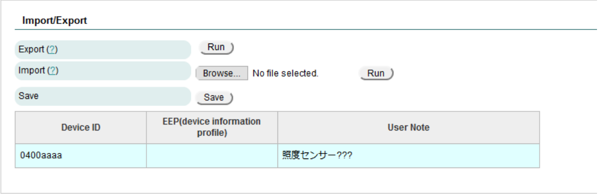
It is possible to add notes to EnOcean devices to be registered. These notes may be used for data communication with the cloud.

EEP (device information profile):

It is possible to set up an EEP (EnOcean Equipment Profile) for each device to be registered. If the correct information is set up in this EEP, it is possible to control temperature, humidity and other information in the EnOcean device data.

Please note that if EnOcean devices are registered, the field under List will display a list of registered devices. It is possible to delete devices or update the Memo information.

*After importing JSON file



Device ID	EEP(device information profile)	User Note
0400aaaa		照度センサー???

Import/Export

Export:

Exports EnOcean device information maintained in this unit as a JSON file.

Import:

Choose a JSON file and import EnOcean device information to be registered/updated in the unit.

Save:

Saves the content of imported JSON file on EnOcean devices in the unit.

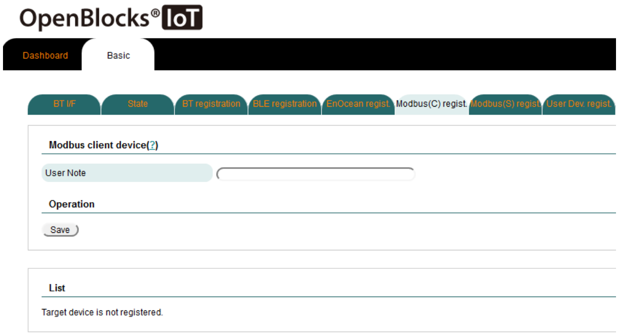
Content of the JSON file may differ, depending on the versions of WEB UI.
Please therefore create a JSON file, while referring to an exported JSON file.

5-6. Modbus (C) registration

It is possible to register a device that speaks the Modbus protocol. Based on registered device information, transmission, reception, etc. using the IoT data control function is possible. (To install IoT data control function, using the **[Maintenance]-[Enhancements]** tab.)

It is possible to register devices using the **[Basic]-[Modbus (C) regist.]** tab.

*The Modbus client device can acquire data from the main chassis (OpenBlocks IoT Family).



Target device is not registered.

Modbus client device

User note:

It is possible to add a note to the Modbus client device to be registered. This note may be used for data communication with the cloud.

*With this device registration, it is possible to only register a note. This item will not set up any device file setups, etc.

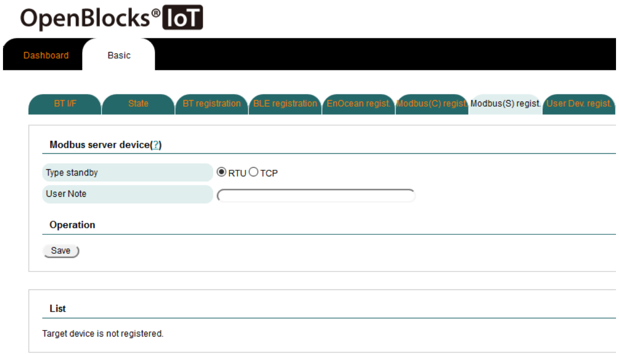
Please note that if a Modbus client device is registered, the field under List will display a list of registered devices. It is possible to delete devices or update the Memo information.

5-7. Modbus (S) registration

It is possible to register a device that speaks the Modbus protocol. Based on registered device information, transmission, reception, etc. using the IoT data control function is possible. (To install IoT data control function, using the **[Maintenance]-[Enhancements]** tab.)

It is possible to register devices using the **[Basic]-[Modbus (S) regist.]** tab.

*The Modbus server device can send data to the main chassis (OpenBlocks IoT Family).



Modbus server device(?)

Type standby: ● RTU ○ TCP

User Note:

Operation

List

Target device is not registered.

Modbus server device

Type standby:

Sets up the standby type for Modbus server devices to be registered.

Can choose either of the following two types:

・TCP: Standby with Ethernet and other network.

・RTU: Standby with a serial device file.

User note:

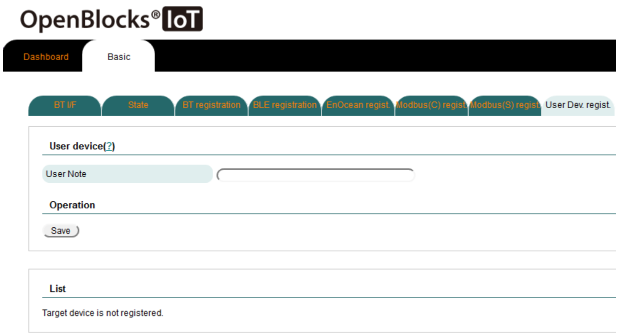
It is possible to add a note to the Modbus server device to be registered. This note may be used for data communication with the cloud.

*With this device registration, it is possible to only register a standby type and a note. This item will not set up any device file setups, etc.

Please note that if a Modbus client device is registered, the field under List will display a list of registered devices. It is possible to delete devices or update the Memo information.

5-8 User device registration

It is possible to virtually register device types other than those described above. Based on registered device information, transmission, reception, etc. using the IoT data control function is possible. (To install IoT data control function, using the **[Maintenance]-[Enhancements]** tab.)
It is possible to register devices using the **[Basic]-[User Dev. regist.]** tab.



Target device is not registered.

User device

User note:

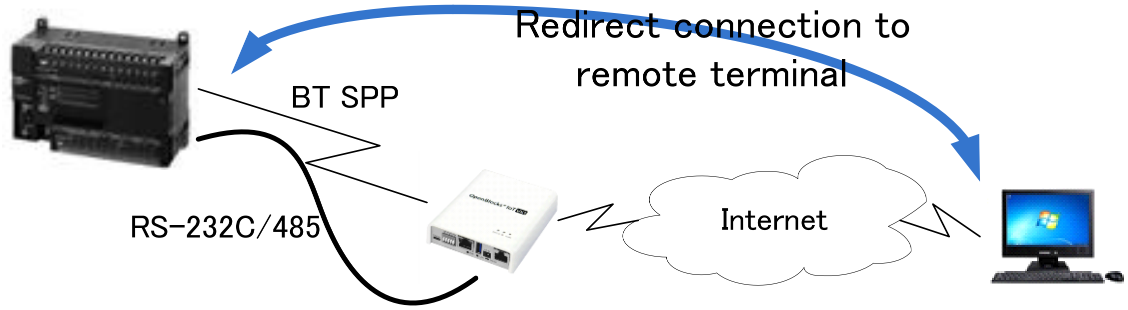
It is possible to add a note to the user device to be registered. This note may be used for data communication with the cloud.

Please note that if a user device is registered, the field under List will display a list of registered devices. It is possible to delete devices or update the Memo information.

Chapter 6: Serial redirection function

Serial redirection function involves redirecting communication data on a RS-232C/RS-485 interface or a BT SPP device connected to this unit to a serial terminal at a remote location. Many M2M legacy devices use RS-232C or RS-485 as connection interfaces with external devices, which are necessary for maintenance and control. For many such devices, maintenance staff members visit installation locations, connect to a PC, etc. in order to collect logs and update software.

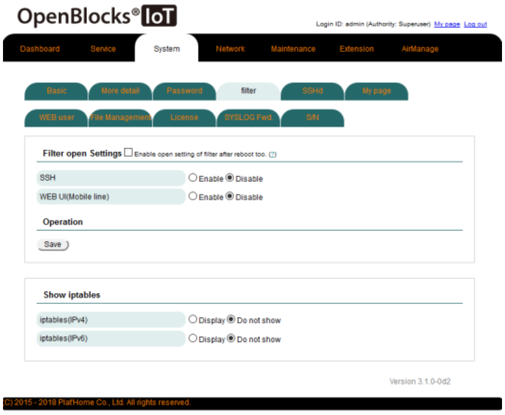
With this unit, it is possible to directly establish connections with such devices via the Internet without the need to visit actual sites. For this service, a mobile network can be used, thereby realizing user network remote control.



6-1 Serial redirection function for SPP devices

When a paired BT device is an SPP (Serial Port Profile) type, serial communication to this unit via SSH can be redirected to the BT device.

To use this function, it is necessary to enable the SSH port to be used in advance.



Filter open Settings ☐ Enable open setting of filter after reboot too. (?)

SSH	○ Enable ● Disable
WEB UI(Mobile line)	○ Enable ● Disable

Operation

Show iptables

iptables(IPv4)	○ Display ● Do not show
iptables(IPv6)	○ Display ● Do not show

Version 3.1.0-0d2

(C) 2015 - 2018 PlatHome Co., Ltd. All rights reserved.

Choose the **[System]-[Filter]** tab to display **Filter open settings** menu for enabling/disabling the SSH.

Choose "Enable" and press the "Save" button. SSH can now be used.

It is also possible to enable SSH via SMS control.

Networks that can use SSH

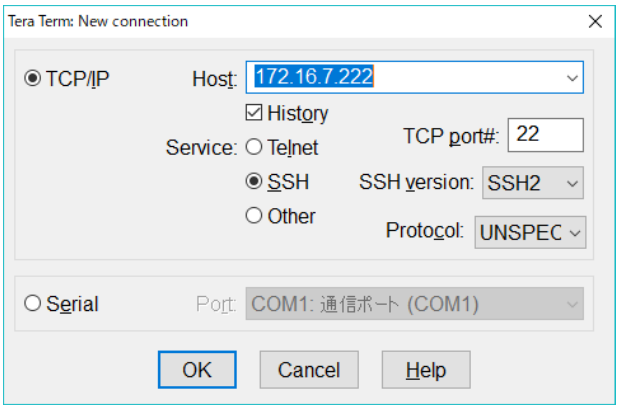
This section assumes that SSH can pass the firewall and that access to this unit is possible from a terminal using SSH via a global IP, etc.

In general, SSH can be used in a local network or an M2M private network. However, with a mobile network using a public Internet network, in many cases, a global IP is not allocated. Instead, an NAPT connection is established. In this case, SSH cannot reach this unit.

However, even with a mobile network, some services allocate a global IP as an option, meaning that it is possible to use such an optional service or the PacketiX VPN we offer to establish SSH connections.

When preparations are complete, start to establish a connection with a communication application that can use SSH such as TeraTerm.

The following description assumes that the procedure will be carried out within a local network.



Tera Term: New connection

● TCP/IP Host: 172.16.7.222

☑ History

Service: ○ Telnet TCP port#: 22

● SSH SSH version: SSH2

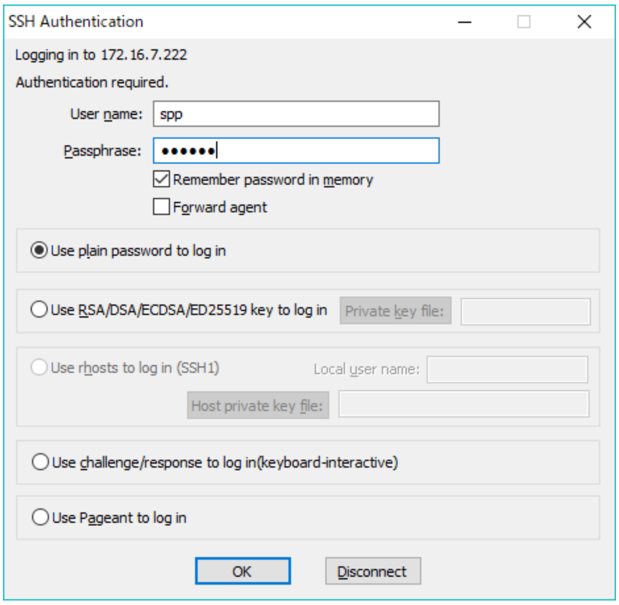
○ Other Protocol: UNSPEC

○ Serial Port: COM1: 通信ポート (COM1)

/

In a local network, enter this unit's IP address into the LAN.

Choose "SSH" and press the "OK" button to enter the authentication screen.



Logging in to 172.16.7.222

Authentication required.

User name: spp

Passphrase: ••••••

☑ Remember password in memory

□ Forward agent

● Use plain password to log in

○ Use RSA/DSA/ECDSA/ED25519 key to log in   Private key file:

○ Use rhosts to log in (SSH1)   Local user name: Host private key file:

○ Use challenge/response to log in(keyboard-interactive)

○ Use Pageant to log in

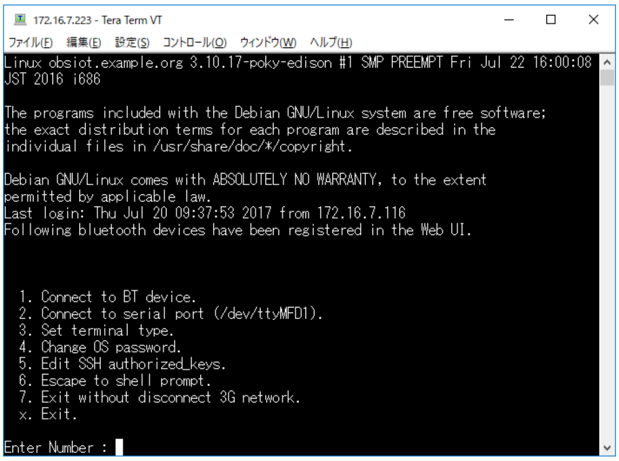
At the authentication screen, enter "spp" in User name.

Password is the same as the default root password set up for this unit.

*This password cannot be changed from WEB UI.

For the authentication method, choose "Use plain password to log in."

After completing authentication setup, click "OK" to start connection.


172.16.7.223 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)

```
Linux obsiot.example.org 3.10.17-poky-edison #1 SMP PREEMPT Fri Jul 22 16:00:08
JST 2016 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 20 09:37:53 2017 from 172.16.7.116
Following bluetooth devices have been registered in the Web UI.



  1. Connect to BT device.
  2. Connect to serial port (/dev/ttyMFD1).
  3. Set terminal type.
  4. Change OS password.
  5. Edit SSH authorized_keys.
  6. Escape to shell prompt.
  7. Exit without disconnect 3G network.
  x. Exit.

Enter Number :
```

When successfully logging in as an "spp" user, a serial redirection menu screen will be displayed.

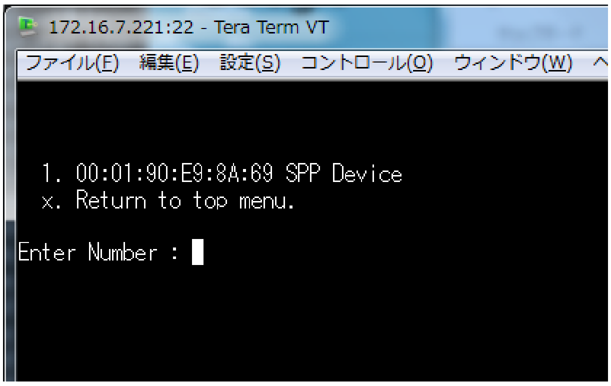
At this screen, it is necessary to carefully check if the paired BT device has been properly probed.

The line below “Test probe to BT devices." shows a detected device. If, for example, the device is turned off, the system will display "fail."

If "done" is displayed, a connection can be established.

If there are multiple active paired BT devices, they will be listed in multiple lines.

Choose "1" from the menu.

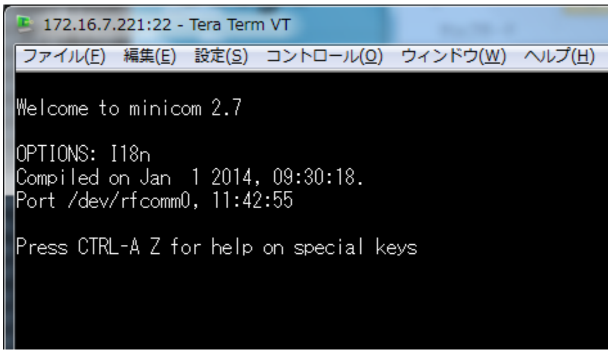

172.16.7.221:22 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘ

```
  1. 00:01:90:E9:8A:69 SPP Device
  x. Return to top menu.

Enter Number :
```

The next screen will show a list of devices that can be connected. Choose the device to be connected by choosing its number.

After choosing the device to be connected, the next screen will be displayed to start redirecting serial communication by minicom.


172.16.7.221:22 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)

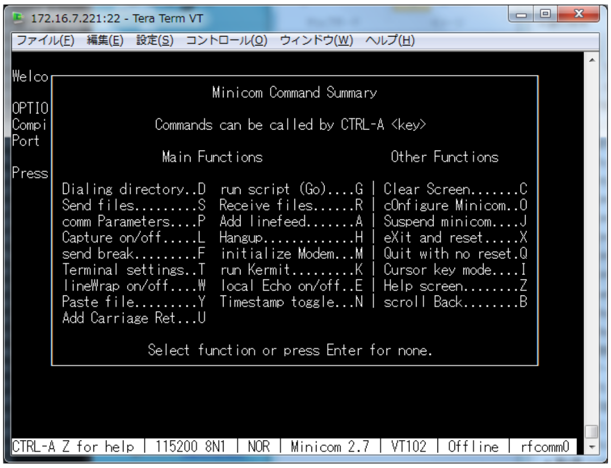
```
Welcome to minicom 2.7

OPTIONS: I18n
Compiled on Jan  1 2014, 09:30:18.
Port /dev/rfcomm0, 11:42:55

Press CTRL-A Z for help on special keys
```

Press CTRL-A and enter "Z" to show Help on minicom.

To terminate minicom, follow the instructions in Help.


172.16.7.221:22 - Tera Term VT
ファイル(F) 編集(E) 設定(S) コントロール(O) ウィンドウ(W) ヘルプ(H)

```
Welco
                   Minicom Command Summary
OPTIO
Compi          Commands can be called by CTRL-A <key>
Port
                 Main Functions                  Other Functions
Press
      Dialing directory..D  run script (Go)....G | Clear Screen.......C
      Send files.........S  Receive files......R | cOnfigure Minicom..O
      comm Parameters....P  Add linefeed.......A | Suspend minicom....J
      Capture on/off.....L  Hangup.............H | eXit and reset.....X
      send break.........F  initialize Modem...M | Quit with no reset.Q
      Terminal settings..T  run Kermit.........K | Cursor key mode....I
      lineWrap on/off....W  local Echo on/off..E | Help screen........Z
      Paste file.........Y  Timestamp toggle...N | scroll Back........B
      Add Carriage Ret...U

              Select function or press Enter for none.

CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7 | VT102 | Offline | rfcomm0
```

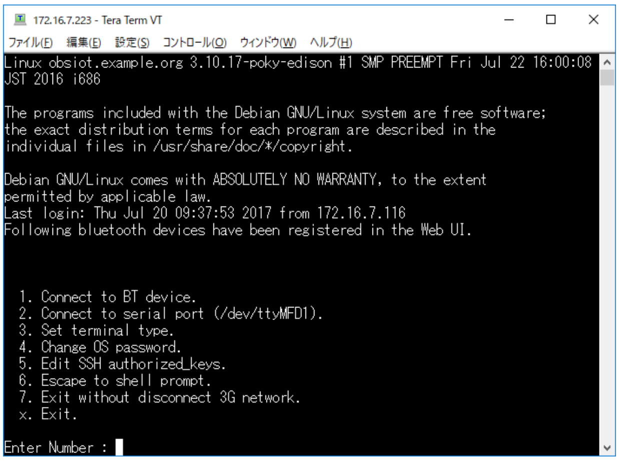
To terminate the connection, follow the menu, return to the top menu and exit.

It is possible to simultaneously disconnect the mobile network when exiting.

With the above procedure, it is possible to establish a direct serial communication with an SPP device. By, for example, combining TeraTerm scripts and Linux shell scripts, it is possible to automatically collect data.

6-2 Serial redirection function for RS-232C

The serial redirection function of this unit allows for redirect communication with the RS-232C port, wired interface of this unit, in addition to BT devices.



```
Linux obsiot.example.org 3.10.17-poky-edison #1 SMP PREEMPT Fri Jul 22 16:00:08
JST 2016 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 20 09:37:53 2017 from 172.16.7.116
Following bluetooth devices have been registered in the Web UI.



  1. Connect to BT device.
  2. Connect to serial port (/dev/ttyMFD1).
  3. Set terminal type.
  4. Change OS password.
  5. Edit SSH authorized_keys.
  6. Escape to shell prompt.
  7. Exit without disconnect 3G network.
  x. Exit.

Enter Number :
```

Operation procedure is almost the same as Item 6.1.

After starting an SSH, choose "2. Connect to serial port (/dev/S4)" from the first redirection menu of the serial communication.

Redirection to RS-232C port will start.

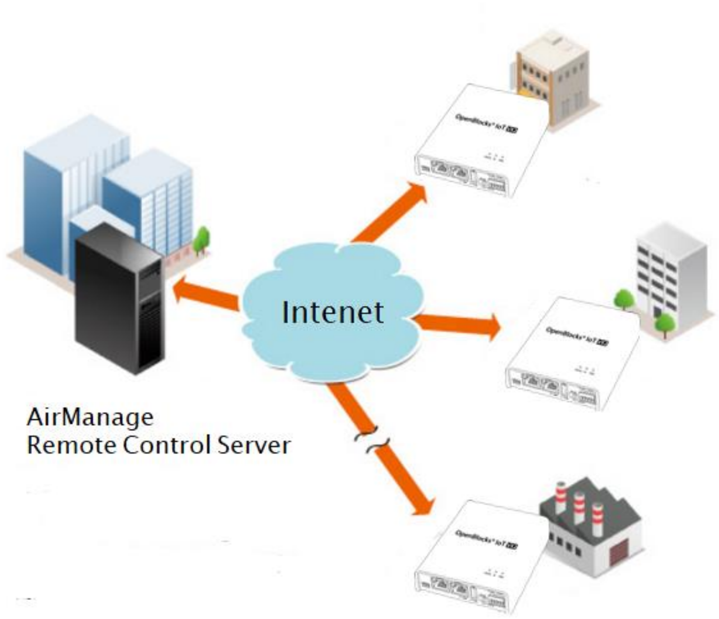
The serial communication speed is set to 115,200 bps by default. Change this setting if deemed necessary.

Chapter 7: AirManage functions

AirManage is a function that allows for the management of the OpenBlocks IoT Family, while deployed in a remote location.

AirManage regulates the configuration of each IoT Gateway by communicating between AirManage remote control servers on the Internet and individual OpenBlocks IoT Family.

For further details of the functions of AirManage and how to subscribe to the service, please contact Sales.



7-1 Initial access settings for AirManage

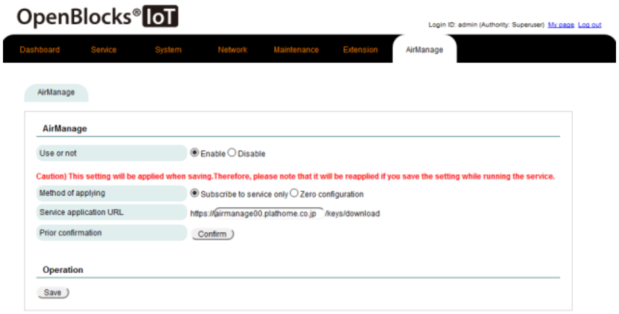
In order to use the AirManage service, it is necessary to register each OpenBlocks IoT Family on AirManage remote control servers in advance.

Following said registration, the AirManage service will become available when each OpenBlocks IoT Family makes initial access to the server.

To install setting for initial access, using the **[AirManage]** tab.

*The network used for the initial access described in this section will succeed the settings of "Basic" settings in the **[Network]-[Basic]** tab. Therefore, make advance preparations for Internet access.

*If the AirManage kitting option is applied at the time of shipment, this process will not be necessary.



Use or not: ● Enable ○ Disable

Caution) This setting will be applied when saving.Therefore, please note that it will be reapplied if you save the setting while running the service.

Method of applying: ● Subscribe to service only ○ Zero configuration

Service application URL: https://airmanage00.plathome.co.jp /keys/download

Prior confirmation: Confirm

AirManage

AirManage to be use:

To subscribe to the AirManage service, choose "To be use."

To cancel the service, choose "Disable."

Methods of applying:

Choose either of the following options.

●Subscribe to service only

Only accesses the AirManage remote control server. No configuration will be applied, but it is possible to subscribe to the service to make various functions available.

●Zero configuration

Downloads configuration from the AirManage remote control server and applies it to system.

Service application URL:

Input the FQDN information at the time of service subscription in the form.

Prior confirmation

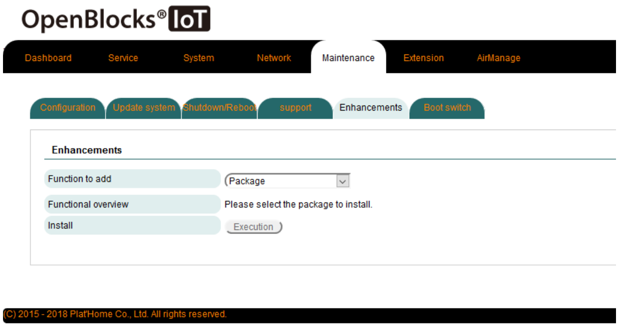
Press the Confirm button to check if machine is registered to the AirManage server by using the node side network and set up the URL information.

After completing the setup, press the Save button. By rebooting the system, it will be possible to make initial access.

Chapter 8: Extension

Immediately after shipment, this unit is installed only with software to set up network settings, etc. If there is a need to apply extentions for use as an IoT Gateway, it is possible to add supported packages using the **[Maintenance]-[Enhancements]** tab.

8-1 Installing an extension package

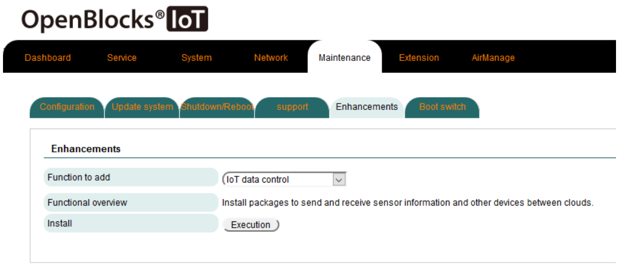


Enhancements

Function to add	Package
Functional overview	Please select the package to install.
Install	Execution

(C) 2015 - 2018 PlatHome Co., Ltd. All rights reserved.

Choose the **[Maintenance]-[Enhancements]** tab to choose packages for extensions.



Enhancements

Function to add	IoT data control
Functional overview	Install packages to send and receive sensor information and other devices between clouds.
Install	Execution

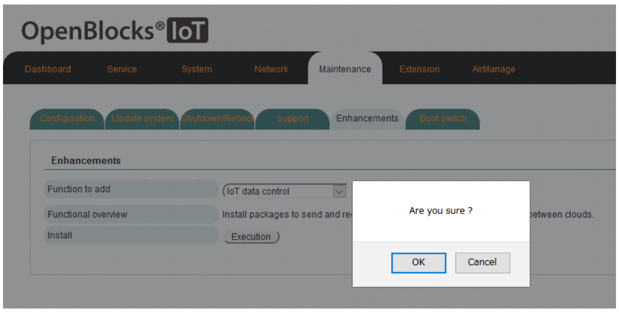
Choose a package to install and press the "Execution" button for installation.

*To install software using this function, the unit must support an Internet environment.

*If the network connected to the Internet is slow, installation of package may take some time.

When the Execution button is pressed, a confirmation window will be displayed. When the proper package is displayed, press the OK button to confirm selection.

During installation, it is not possible to choose buttons.



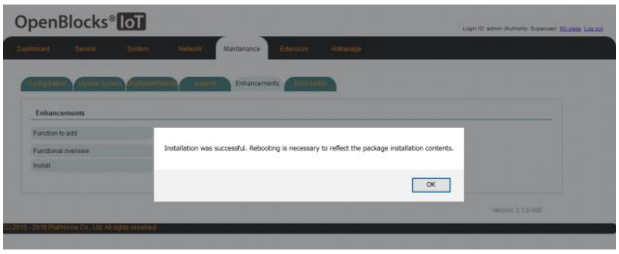
Enhancements

Function to add: IoT data control

Functional overview: Install packages to send and re… between clouds.

Are you sure ?

*After pressing the Execution button, a button to check the installation status will appear. Press this button to check on the progress of installation.



Installation was successful. Rebooting is necessary to reflect the package installation contents.

Regardless of whether an installation has been successful or not, a window will be displayed when the process is completed.

If installation has been a success, press the OK button to accept the message. After installing an extension with this function, and as the system needs to be rebooted, restart the unit.

*If an installation failed, recheck Internet environment, etc., and execute installation again.

*Installing some packages may require the addition to sources.list and public keys of packages repository.

At the time of writing this document, packages available for installation from this function are as follows:

Package	Contents
Samba	WEB UI for Samba and a set of applications for file sharing.
IoT data control	WEB UI for IoT data control and a set of applications.
Node-RED	WEB UI for Node-RED and a set of Node-RED.
Security	A set of functions that carry out access rejection, etc. against illegal access to WEB UI and SSH.
Camera	WEB UI for image capture by camera and image display / motion detection software
Docker	Installs Docker DAEMON.
Moby	Installs Docker DAEMON, which builded by Microsoft from Moby.
Docker (including WEB UI)	Installs a set of functions to control Docker containers, etc. from WEB UI. Docker DAEMON also installed.
Azure IoT Edge	Installs a set of Azure IoT Edge and WEB UI for setup. Docker DAEMON installation is required in advance.

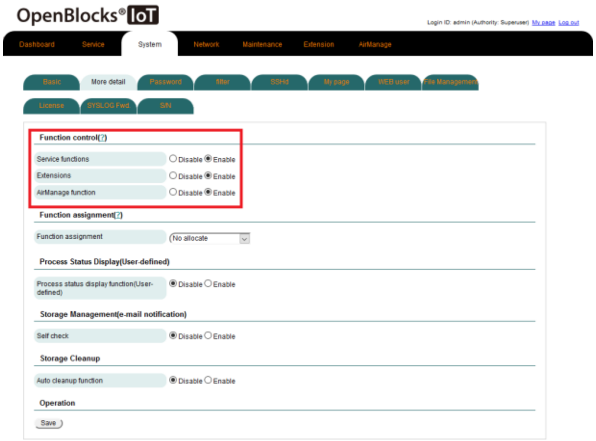
Chapter 9: Reference by setup items

Attention:

Password settings in Chapter 9-4 and 9-7 in this chapter are very important in terms of security. Therefore, set passwords that are difficult to be compromised.

9-1 Show/Hide service control functions and extensions

The WEB UI is customized for IoT-related operations. If the unit is used for a different purpose, IoT-related Web indications except for basic server settings can be disabled, using the **Function control** menu in the **[System]-[More detail]** tab.



Function control(?)

Service functions ○ Disable ● Enable

Extensions ○ Disable ● Enable

AirManage function ○ Disable ● Enable

Function assignment(?)

Function assignment: No allocate

Process Status Display(User-defined)

Process status display function(User-defined) ● Disable ○ Enable

Storage Management(e-mail notification)

Self check ● Disable ○ Enable

Storage Cleanup

Auto cleanup function ● Disable ○ Enable

Operation

Function control

Service functions:

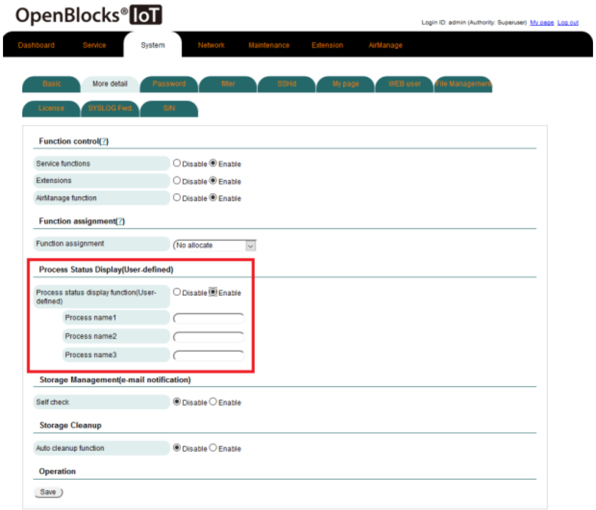
Hides [Service] tab.

Extensions:

Hides [Extensions] tab.

9-2 Process status indication function

Possible to monitor processes added by the user in addition to basic processes, using the **Process status display** menu in the **[System]-[More detail]** tab.



Function control(?)

Service functions ○ Disable ● Enable

Extensions ○ Disable ● Enable

AirManage function ○ Disable ● Enable

Function assignment(?)

Function assignment No allocate

Process Status Display(User-defined)

Process status display function(User-defined) ○ Disable ● Enable

Process name1

Process name2

Process name3

Storage Management(e-mail notification)

Self check ● Disable ○ Enable

Storage Cleanup

Auto cleanup function ● Disable ○ Enable

Operation

Process status display

Process status display function (by user definition):

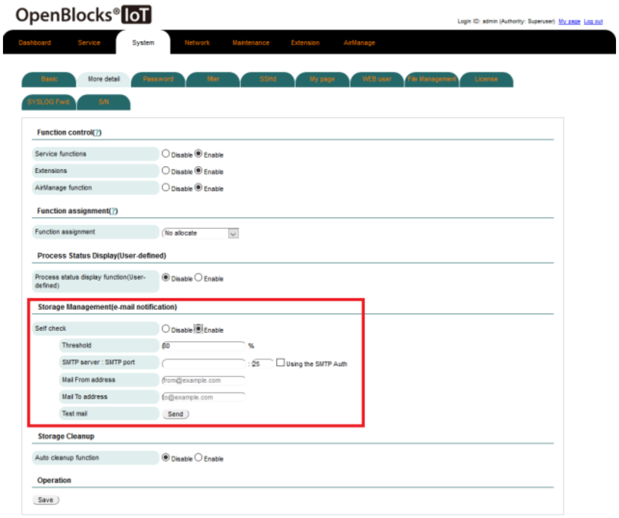
By registering a process to be monitored, for example, dhcpd, and to determine as to whether or not the process has started will be shown on the Dashboard.

Up to three processes can be registered.

9-3 Storage alert function

Storage capacity is checked on a regular basis (once per hour), using the **Storage Management (e-mail notifications)** menu in the **[System]-[More detail]** tab.

If a threshold exceeds a limit, an e-mail notification will be issued. It is possible to monitor the consumption of storage capacity with logs, etc.



Function control(?)

Service functions ○ Disable ● Enable

Extensions ○ Disable ● Enable

AirManage function ○ Disable ● Enable

Function assignment(?)

Function assignment No allocate

Process Status Display(User-defined)

Process status display function(User-defined) ● Disable ○ Enable

Storage Management(e-mail notification)

Self check ○ Disable ● Enable

Threshold 80 %

SMTP server : SMTP port : 25 □ Using the SMTP Auth

Mail From address from@example.com

Mail To address to@example.com

Test mail Send

Storage Cleanup

Auto cleanup function ● Disable ○ Enable

Operation

Save

Storage Management (e-mail notifications)

Self check:

To use this function, choose "Enable."

Threshold: 80% (by default)

Threshold that will issue an alert.

SMTP server: SMTP port

Enter mail server address and port. Check "Using the SMTP Auth" when using a server supporting SMTP Auth.

SMTP Auth:

This item will be displayed when "Using the SMTP Auth" is checked. Set up a username and password for SMTP Auth.

Mail From address:

Enter sender (From) address for e-mail transmission.

Mail To address:

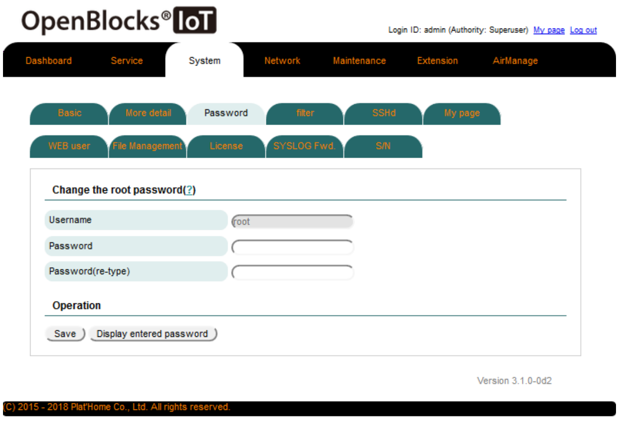
Enter recipient (To) address for e-mail transmission.

Test mail:

Sends a test mail message with content setup. Possible to check the content of e-mail text in addition to setup.

9-4 Setting root password

Possible to change the password for the root account that can be used for logging onto the OpenBlocks IoT Family via SSH or a serial console, using the **[System]-[Password]** tab.



Change the root password(?)

Username	root
Password	
Password(re-type)	

Operation

Version 3.1.0-0d2

(C) 2015 - 2018 Plat'Home Co., Ltd. All rights reserved.

Enter a new password in Password and Password (retype) boxes and press the Save button.

When using this system, change the default password for security reasons.

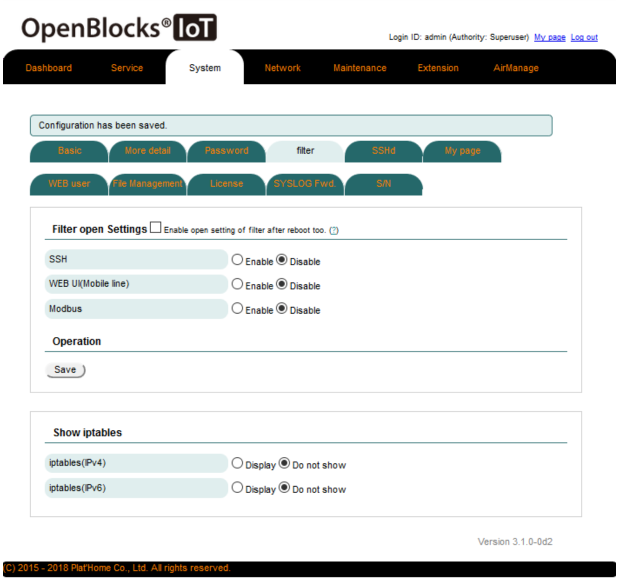
Default root password

Default password for the root account of this unit is 0BSI0T.

(The two "0"s are numerical characters).

9-5 Filter permissions

Individual filters of the OpenBlocks IoT Family can be temporarily or permanently made effective after rebooting, using the **[System]-[Filter]** tab.



Configuration has been saved.

Filter open Settings □ Enable open setting of filter after reboot too. (?)

SSH ○ Enable ● Disable

WEB UI(Mobile line) ○ Enable ● Disable

Modbus ○ Enable ● Disable

Operation

Show iptables

iptables(IPv4) ○ Display ● Do not show

iptables(IPv6) ○ Display ● Do not show

Version 3.1.0-0d2

(C) 2015 - 2018 Plat'Home Co., Ltd. All rights reserved.

Filter open settings

To keep individual filters open after rebooting, check "Enable open setting of filter after reboot too" and press the Save button.

SSH:

To log onto this unit using an SSH, choose "Enable" radio switch and press the Save button.

WEB UI (Mobile line):[1]

To access WEB UI via a mobile network, choose "Enable" radio switch and press the Save button.

Show iptables

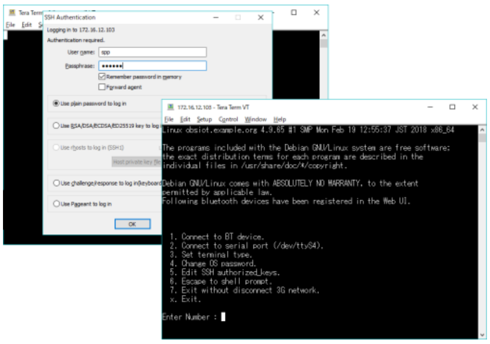
iptables (IPv4):

Choosing "Display" radio button will show the contents of iptables IPv4.

iptables (IPv6):

Choosing "Display" radio button will show the content of iptables IPv6.

ⓘ **Do not forget to choose "Disable" when the opening of individual filters has become unnecessary!**



Tera Term
File Edit
SSH Authentication

Logging in to 172.16.12.103

Authentication required.

User name: spp

Passphrase: ••••••

☑ Remember password in memory

□ Forward agent

● Use plain password to log in

○ Use RSA/DSA/ECDSA/ED25519 key to log in

○ Use rhosts to log in (SSH1)

○ Use challenge/response to log in(keyboard

○ Use Pageant to log in

OK
172.16.12.103 - Tera Term VT
File Edit Setup Control Window Help

```
Linux obsiot.example.org 4.9.65 #1 SMP Mon Feb 19 12:55:37 JST 2018 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Following bluetooth devices have been registered in the Web UI.



 1. Connect to BT device.
 2. Connect to serial port (/dev/ttyS4).
 3. Set terminal type.
 4. Change OS password.
 5. Edit SSH authorized_keys.
 6. Escape to shell prompt.
 7. Exit without disconnect 3G network.
 x. Exit.

Enter Number : █
```

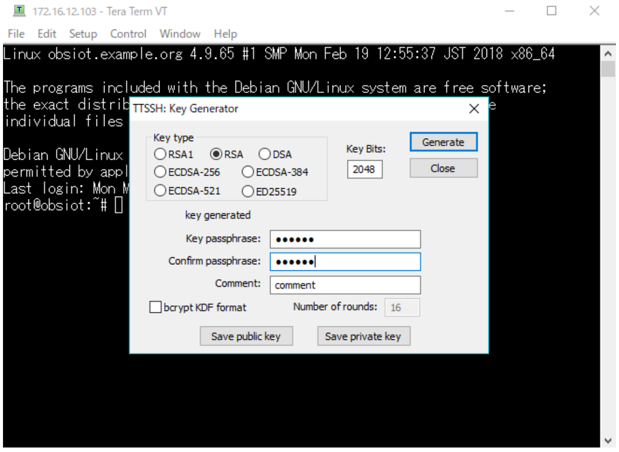
As the illustrations to the left show, it is possible to log in an SSH by using TeraTerm or another terminal application and designating an IP address.

To securely operate an SSH, registering an open key as explained in "9-6 Exchanging SSH keys" is recommended.

1 For access to WEB UI, access via WLAN or Ethernet only is supported. Access via mobile network is not supported in consideration of security.

9-6 Exchanging SSH keys

This screen enables an SSH to be used in a more secure manner.



172.16.12.103 - Tera Term VT
File Edit Setup Control Window Help

```
Linux obsiot.example.org 4.9.65 #1 SMP Mon Feb 19 12:55:37 JST 2018 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distrib
individual files

Debian GNU/Linux
permitted by appl
Last login: Mon M
root@obsiot:~# 
```

TTSSH: Key Generator

Key type: ○ RSA1 ● RSA ○ DSA ○ ECDSA-256 ○ ECDSA-384 ○ ECDSA-521 ○ ED25519

Key Bits: 2048

key generated

Key passphrase: ••••••

Confirm passphrase: ••••••

Comment: comment

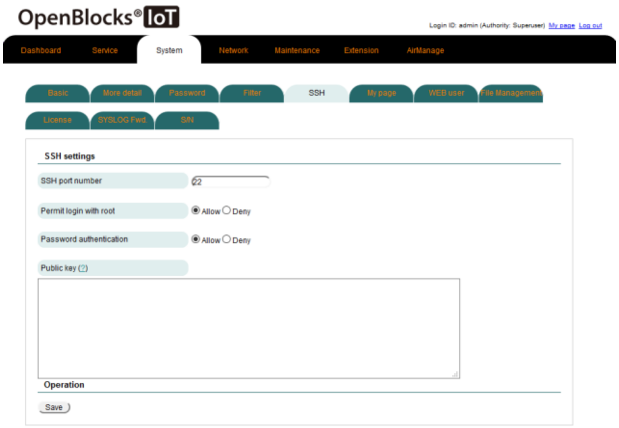
□ bcrypt KDF format

Number of rounds: 16

Firstly, generate public and secret keys using TeraTerm, etc. as shown in the screen-shot to the left.

In the case of TeraTerm, these two keys will be stored in a designated directory. Display the public key with a text editor, etc. and save in the copy buffer.

It is possible to make this setting use the **[System]-[SSH]** tab.



SSH settings

SSH port number: 22

Permit login with root: ● Allow ○ Deny

Password authentication: ● Allow ○ Deny

Public key (?)

Operation

SSH settings

SSH port number:

Sets the port number to be used for an SSH.

Permit login with root:

Choose "Allow" to permit SSH login to this unit with the root account.

Password authentication:

To access an SSH without using a key, choose "Allow" for password authentication.

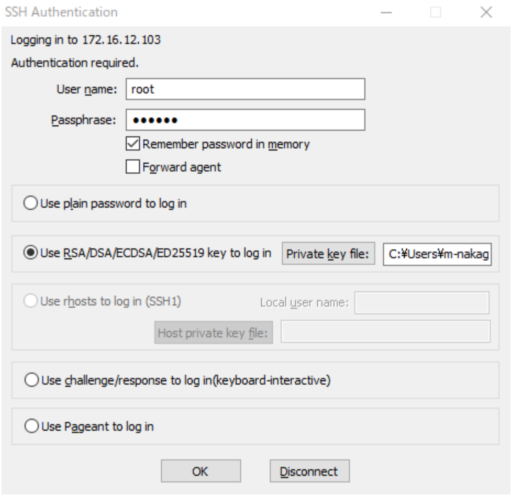
To access an SSH using a key, choose "Deny."

Public key:

Paste public key generated with TeraTerm, etc. as described above.

If not using a key, keep this box blank.

After completing settings, press the Save button.



Logging in to 172.16.12.103

Authentication required.

User name: root

Passphrase: ••••••

☑ Remember password in memory

□ Forward agent

○ Use plain password to log in

● Use RSA/DSA/ECDSA/ED25519 key to log in — Private key file: C:¥Users¥m-nakag

○ Use rhosts to log in (SSH1) — Local user name:

○ Use challenge/response to log in(keyboard-interactive)

○ Use Pageant to log in

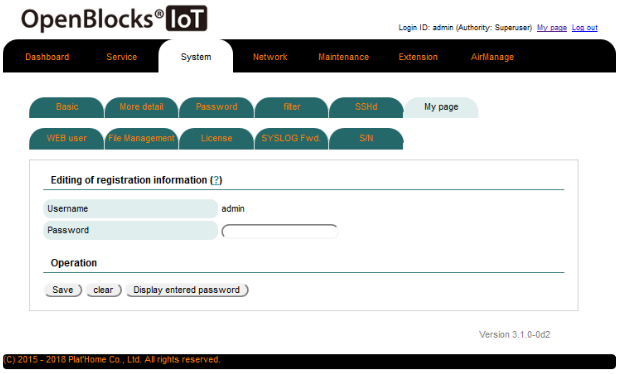
After the above settings, login with an SSH key.

The screen to the left shows an example of a connection with TeraTerm.

9-7 Changing web administrator password

It is possible to change the administrator password for WEB UI. The username cannot be changed.

It is possible to make this setting use the **[System]-[My page]** tab.



Login ID: admin (Authority: Superuser)

Editing of registration information (?)

Username	admin
Password	

Operation

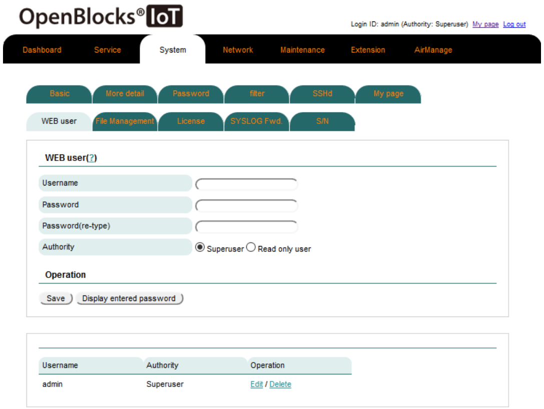
Change will become effective after pressing the Save button following edit.

After making change, login to WEB UI once more.

9-8 Web user

It is possible to add login users to WEB UI and change the password of another login user (super users only).

It is possible to make this setting use the **[System]-[WEB user]** tab.



WEB user(?)

Username

Password

Password(re-type)

Authority ● Superuser ○ Read only user

Operation

Username	Authority	Operation
admin	Superuser	Edit / Delete

Changes will be effective after setting up username, password, etc. and pressing the Save button.

9-9 File management

It is possible to use WEB UI to, for example, upload a file to a specific directory in the OpenBlocks IoT Family.

It is possible to make this setting use the **[System]-[File Management]** tab.

To download, delete, move, grant an execution permission or edit a file, choose a file and press the relevant button.

To upload a file, choose the file to be uploaded by using the "Browse..." button. After choosing a file, press the Upload button.

The file will be uploaded to:

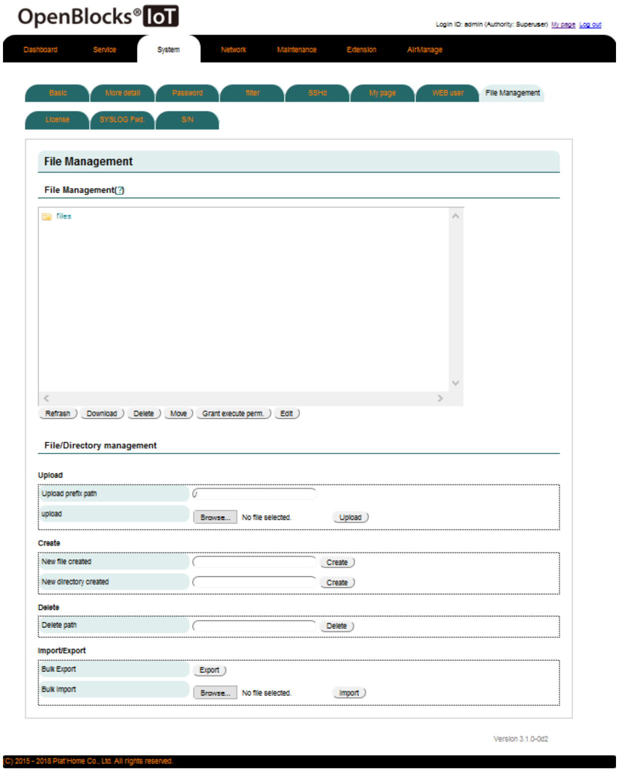
Dir: /var/webui/upload_dir/

Cannot upload a file whose size exceeds 256MB. To upload such a file, make SSH effective and upload the file with SFTP.

To generate a new file or directory, enter the file or directory path. It is possible to create a file in /var/webui/upload_dir/. (Cannot create a file in a higher order directory).

Use Bulk Export to bulk export files in /var/webui/upload_dir/ as a file compressed with a tar+gz format.

Use Bulk Import to extract data in a tar+gz format in /var/webui/upload_dir/.



File Management

File Management(?)

File/Directory management

Upload

Upload prefix path	/
upload	No file selected.

Create

New file created	
New directory created	

Delete

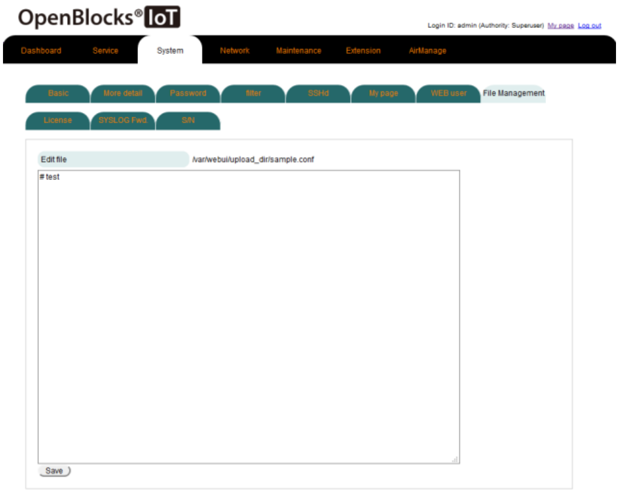
Delete path	

Import/Export

Bulk Export	
Bulk Import	No file selected.

Version 3.1.0-0d2

(C) 2015 - 2018 Plat'Home Co., Ltd. All rights reserved.



Edit file /var/webui/upload_dir/sample.conf

```
# test
```

Pressing the Edit button after choosing a file will display a screen as shown to the left.

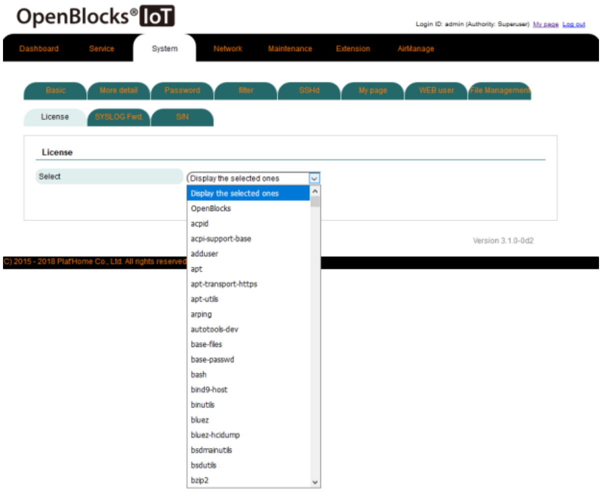
To save edit, press the Save button.

Please note that editing supports text files only.

9-10 Displaying a software license

Can display a software license and user permission used in WEB UI.

To show the information, using the **[System]-[License]** tab.



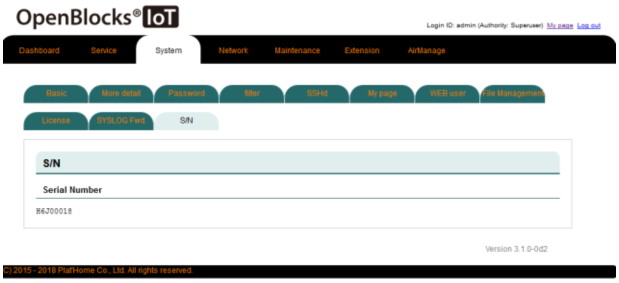
Can choose and display software license and user permission for individual applications from a pull-down menu.

Source codes for open source licenses are disclosed on our website.

9-11. Checking unit's serial number

Can check the serial number of OpenBlocks IoT Family unit.

Can check this information using the **[System]-[S/N]** tab.



Login ID: admin (Authority: Superuser)

S/N

Serial Number

H6J00018

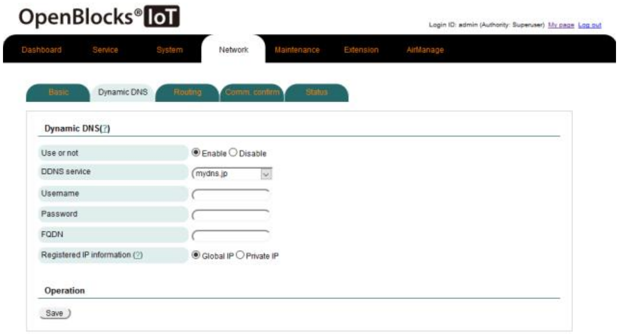
Version 3.1.0-0d2

C) 2015 - 2018 PlatHome Co., Ltd. All rights reserved.

*The serial number shown in the screen-shot to the left is an example.

9-12 Dynamic DNS

Can periodically register current IP address to dynamic DNS server via WEB UI.
Can make this setup using the **[Network]-[Dynamic DNS]** tab.



Dynamic DNS(?)

Use or not	● Enable ○ Disable
DDNS service	mydns.jp
Username	
Password	
FQDN	
Registered IP information (?)	● Global IP ○ Private IP

Operation

Save

Dynamic DNS

To be use:

To use Dynamic DNS, choose "To be use."

DDNS service:

Choose a DDNS service.

Username:

Enter DDNS user account.

Password:

Enter DDNS password.

FQDN:

Enter FQDN registered in DDNS.

Registered IP information

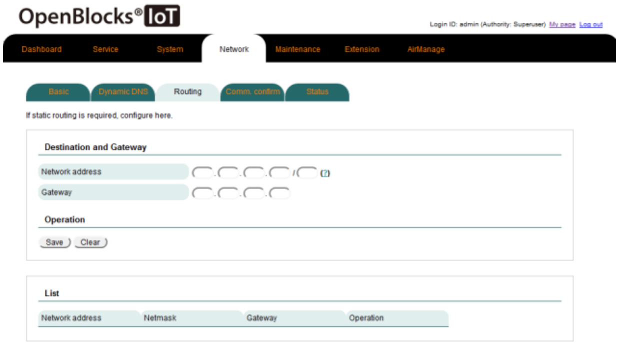
Sets up IP address attributes to be notified to DDNS.

After completing settings, press the Save button. To make settings effective, reboot the unit.

9-13 Adding static routing

To set up static settings when router is in AP mode, etc., it is possible to make the necessary setups from here.

Can make this setting use the **[Network]-[Routing]** tab.



Login ID: admin (Authority: Superuser) My page Log out

If static routing is required, configure here.

Network address	Netmask	Gateway	Operation

Designate a network address and net mask, specify IP address of the machine to serve as a gateway and press the Save button.

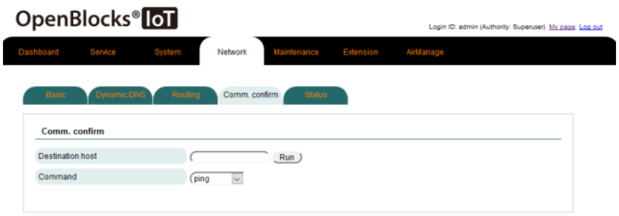
Can register more than one static routing.

To make settings effective, reboot the unit.

9-14 Checking communication

Can test if the network is working by using a ping command, etc.

Can carry out this test using the **[Network]-[Comm. confirm]** tab.



Login ID: admin (Authority: Superuser) My page Log out

Command: ping

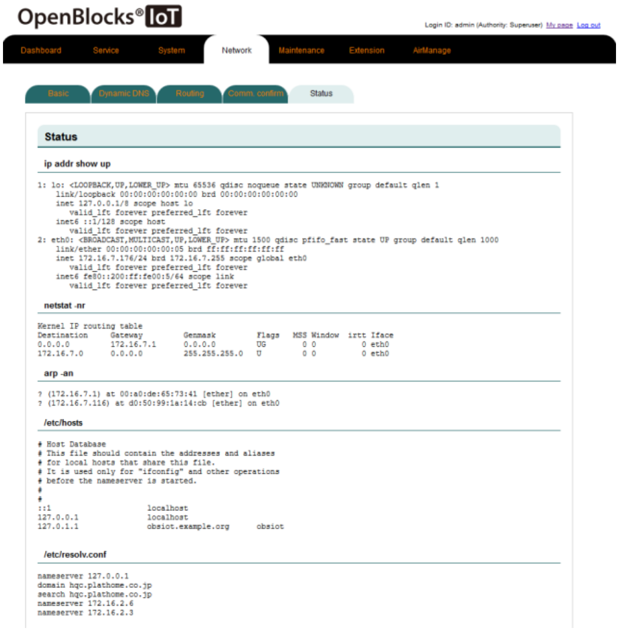
Can choose a command to use (ping / traceroute / nslookup) from the pull-down menu.

Choose a command and press the Run button. Result will be immediately displayed below.

9-15 Checking network status

Can check the status of the network.

Can check this information using the **[Network]-[Status]** tab.



Status

ip addr show up

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:00:00:00:00:05 brd ff:ff:ff:ff:ff:ff
    inet 172.16.7.176/24 brd 172.16.7.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::200:ff:fe00:5/64 scope link
       valid_lft forever preferred_lft forever
```

netstat -nr

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         172.16.7.1      0.0.0.0         UG        0 0          0 eth0
172.16.7.0      0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

arp -an

```
? (172.16.7.1) at 00:a0:de:65:73:41 [ether] on eth0
? (172.16.7.116) at d0:50:99:1a:14:cb [ether] on eth0
```

/etc/hosts

```
# Host Database
# This file should contain the addresses and aliases
# for local hosts that share this file.
# It is used only for "ifconfig" and other operations
# before the nameserver is started.
#
#
::1                     localhost
127.0.0.1               localhost
127.0.1.1               obsiot.example.org      obsiot
```

/etc/resolv.conf

```
nameserver 127.0.0.1
domain hqc.plathome.co.jp
search hqc.plathome.co.jp
nameserver 172.16.2.6
nameserver 172.16.2.3
```

It is recommended to check the status of the unit from this screen after setting up and rebooting the unit.

Can check the following items:

・IP address

・Routing information

・arp information

・Host information

・DNS server information

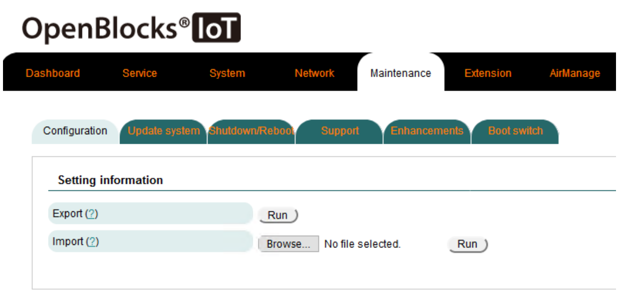
・Modem information

・SIM information

9-16 Backing up and restoring configuration

Can back up configuration to a web client setup via WEB UI. Can also restore configuration using the same file.

Can carry this out using the **[Maintenance]-[Configuration]** tab.



Press the Run button for Export, and a backup configuration file will be downloaded to the web client.

To restore configuration, choose a backup file using the Browse... button and then press the Run button. Configuration will be restored by using the backup configuration file.

*Each time any setting has been changed after completing the system setup of this unit, it is recommended backing up the configuration.

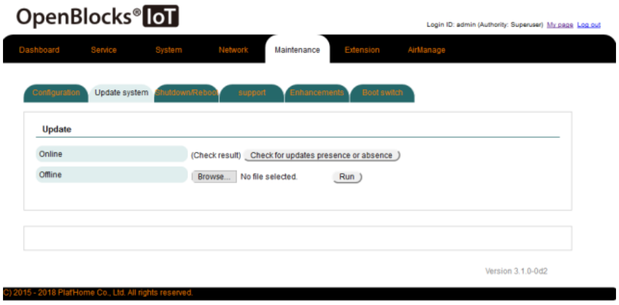
*Basically, we do not support editing of configuration files.

*When importing configuration files, the following replacement rules will apply.

Character string to be replaced	Contents	Remarks
@@SERIAL@@	Serial number of the unit	

9-17 System software update

Can check versions of firmware, OS and applications of this unit and update them.
Can carry this out using the **[Maintenance]-[Update system]** tab.



Login ID: admin (Authority: Superuser)

Update

Online (Check result)

Offline No file selected.

Version 3.1.0-0d2

C) 2015 - 2018 PlatHome Co., Ltd. All rights reserved.

Can carry out online updates if the unit is in an Internet environment.

Press the Check for updates presence or absence button next to Online. The unit will check updates based on repository information and if there are any updates, details will be displayed at the bottom of this screen. To update the program, apply the update.

Please note we offer an offline package if any significantly affective updates become available.

Download an update package to the web client (in consideration of file size, a PC is recommended), press the Browse... button to choose an update package on the PC and press the Run button.

As security updates are frequently released, we recommend that updates be applied as regularly as possible.

Depending on application packages, updates will become effective only after rebooting. We therefore highly recommend a reboot of the unit after applying any updates.

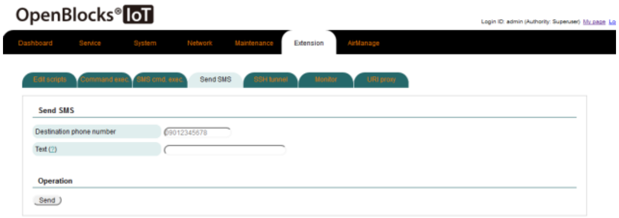
Depending on the contents of updates, web processes may be rebooted. If an immediate update is applied, communication with the web process may be interrupted, resulting in an unexpected error. Should this happen, check the update status.

9-18 SMS transmission

This unit supports SMS with some mobile network modem modules.

(If a mobile network contract does not include an SMS function, it cannot be supported. In addition, a SIM card must be inserted into this unit).

With this, can send SMS messages using the **[Extension]-[Send SMS]** tab.



Send SMS

Destination phone number 09012345678

Text (?)

Operation

Send SMS

Destination phone number:

Enter the telephone number to send SMS message.

Text:

Enter the text to be sent.

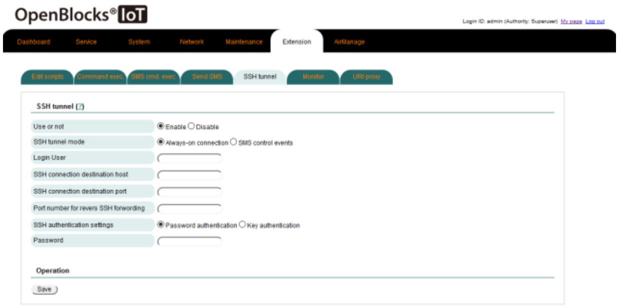
Can enter up to 70 characters in the body of the message.

After entering phone number and text, press the Send button to send SMS message.

9-19 SSH tunnel

Can establish an SSH connection to the SSH server and build a tunnel, using the **[Extension]-[SSH tunnel]** tab. This enables SSH access from the SSH server to OpenBlocks IoT Family via a tunnel.

*To use this function, SSH filtering must be permitted in advance, as described in "9-5 Filter permissions."



SSH tunnel (?)

Use or not	● Enable ○ Disable
SSH tunnel mode	● Always-on connection ○ SMS control events
Login User	
SSH connection destination host	
SSH connection destination port	
Port number for revers SSH forwording	
SSH authentication settings	● Password authentication ○ Key authentication
Password	

Operation

Save

SSH tunnel

To be use:

Determines if this function is used or not. To use it, choose "To be use."

SSH tunnel mode:

Sets up the mode to build an SSH tunnel.

If choosing "Always-on connection," the unit will attempt to build an SSH tunnel during operation.

If "SMS control event" is selected, an SSH tunnel will be built by using SMS or running SMS control direct.

*In the case of SMS, an SSH tunnel will be built for a maximum of 30 minutes.

Login user:

Specify the user to log into the SSH server.

SSH connection destination host:

Sets up IP address and FQDN of the SSN server to be connected.

SSH connection destination port:

Sets up port number of the SSH server to be connected. Normally, this is "22."

SSH number for reverse SSH forwarding:

Sets up port number for connection source to access this unit at the SSH server.

SSH authentication settings:

Sets up authentication method for connecting to the SSH server.

Password:

Enter password if the authentication method uses a password.

Pass phrase:

Enter pass phrase if the authentication method uses keys.

Private key file:

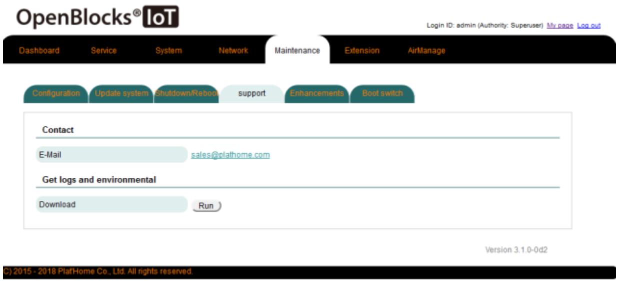
Enter private key file path if the authentication method uses keys.

*Private key file for key authentication should be uploaded using the **[System]-[File Management]** tab.

After completing setup, press the Save button. This function will become effective after rebooting the unit.

9-20 Support information

Check our contact information, using the **[Maintenance]-[Support]** tab.



Contact

E-Mail sales@plathome.com

Get logs and environmental

Download Run

Version 3.1.0-0d2

C) 2015 - 2018 PlatHome Co., Ltd. All rights reserved.

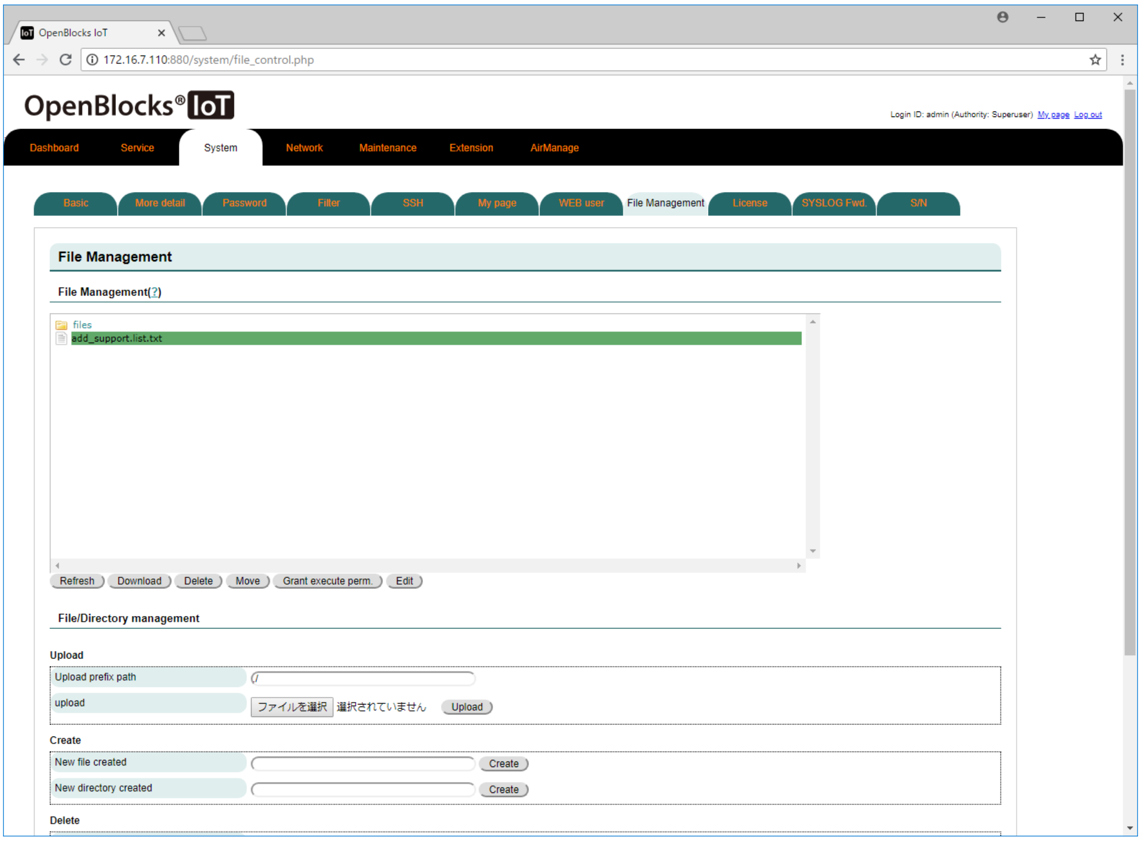
*This image is a sample.

Contact details may change. Please check the latest information via WEB UI.

By executing the Run button in the Get log and environmental menu, It can obtain log information etc. necessary for support.

In order to acquire log information etc, only information necessary for support by us at WEB UI etc. is included standardly.

If you want to include logs etc of your own application in this part, Upload the file with the file name "add_support.list" with the pathname of the data you want to include using the **File Management** menu in the **[System]-[File Management]** tab.



172.16.7.110:880/system/file_control.php

Login ID: admin (Authority: Superuser) My page Log out

File Management

File Management(?)

files
add_support.list.txt

File/Directory management

Upload

Upload prefix path	/
upload	選択されていません

Create

New file created	
New directory created	

Delete

*Example of “add_support.list”.

```
/var/log/apt
/usr/src
```

The specification of the root directory (/) and the first layer (/ tmp, / var etc.) will be ignored.

9-21 Support site of OpenBlocks IoT Famiry

The URL of the support page of OpenBlocks IoT Family is as follows.

http://www.plathome.com/service/

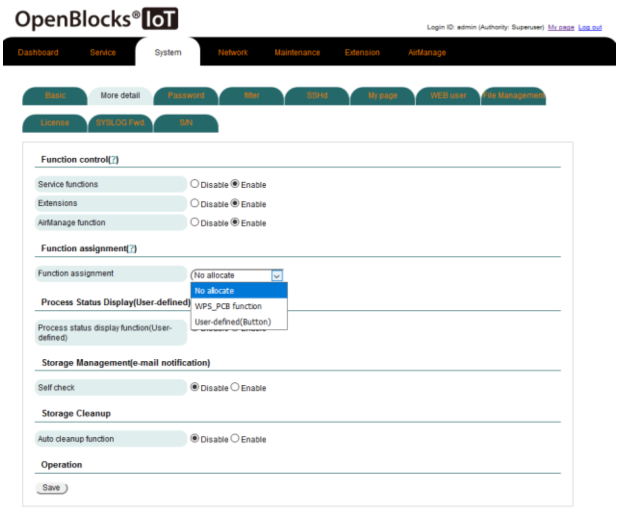
9-22 Assigning functions to FUNC switch

Use the **Function assignment** menu in the **[System]-[More detail]** tab, can assign functions to the FUNC switch. The following functions can be assigned.

・No allocation

・WPS_PCB function

・User-defined (Button)



Function control(?)

Service functions ○Disable ●Enable

Extensions ○Disable ●Enable

AirManage function ○Disable ●Enable

Function assignment(?)

Function assignment: No allocate

Process Status Display(User-defined)

Process status display function(User-defined)

Storage Management(e-mail notification)

Self check ●Disable ○Enable

Storage Cleanup

Auto cleanup function ●Disable ○Enable

Operation

If WLAN is in AP mode and setup to use the WPS function, the WPS_PCB function will become effective.

In addition, "User-defined (Button)" will become effective only if a relevant script has been created by using the Edit scripts tab in the Extension tab.

9-23 Monitoring function

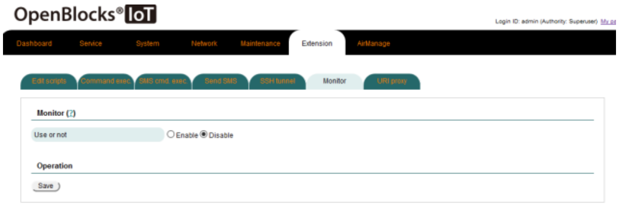
Log files and operating processes in OpenBlocks IoT Family can be monitored, using the **[Extension]-[Monitor]** tab.

In log file monitoring, when a particular keyword is outputted, attention is called for.

In process monitoring, when any of the preset processes are not running, attention is called for. Any process that is calling for attention because the subject process is not running will not be subject to monitoring.

It is possible to reset the attention calling condition from the Dashboard.

This function is linked with the AirManage function. If the AirManage function is effective, can check the attention information on the side of the AirMange remote management server.

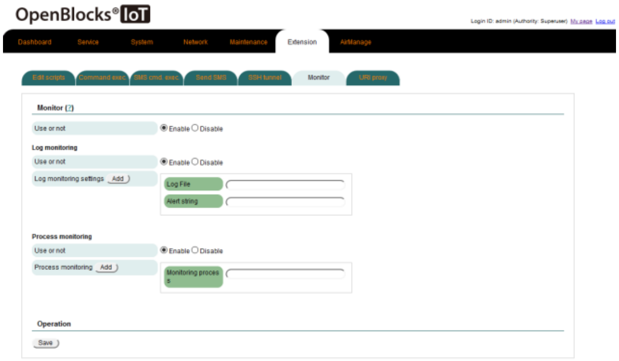


Monitor (?)

Use or not ○ Enable ● Disable

Operation

To make the monitoring function effective, choose "To be use" for the To be use setting.



Monitor (?)

Use or not ● Enable ○ Disable

Log monitoring

Use or not ● Enable ○ Disable

Log monitoring settings

Log File

Alert string

Process monitoring

Use or not ● Enable ○ Disable

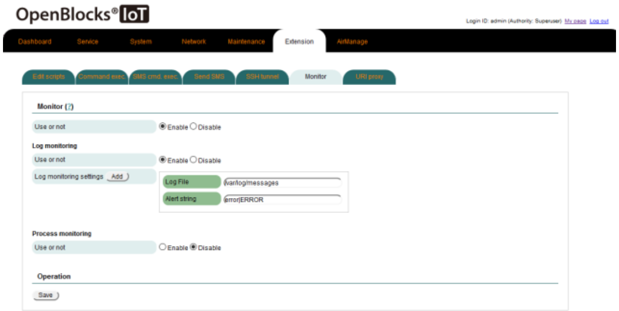
Process monitoring

Monitoring proces s

Operation

To make the log monitoring function effective, choose "To be use" for the To be use line in the Log monitoring section.

To make the process monitoring function effective, choose "To be use" for the To be use line in the Process monitoring section.



Monitor (?)

Use or not ● Enable ○ Disable

Log monitoring

Use or not ● Enable ○ Disable

Log monitoring settings

Log File: /var/log/messages

Alert string: error|ERROR

Process monitoring

Use or not ○ Enable ● Disable

Operation

Log monitoring

To be use:

To make the log monitoring function effective, choose "To be use" for the To be use line in the Log monitoring section. If not, choose "Disable."

Log monitoring settings:

Use the Add button to increase items for monitoring settings (maximum of eight settings).

Log File path:

Sets the file path of the log to be monitored.

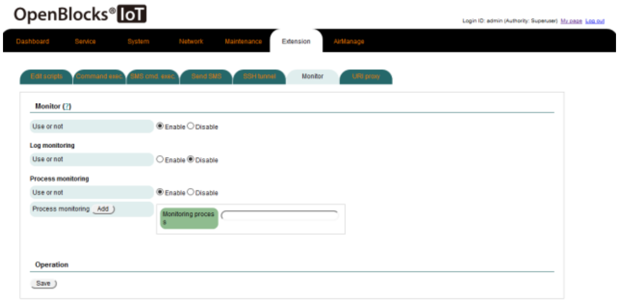
(ex. /var/log/messages)

Alert string:

Sets a string to be dealt with as an alert (attention).

To setup multiple conditions, divide by using "|".

(ex. error|ERROR)



Monitor (?)

Use or not ● Enable ○ Disable

Log monitoring

Use or not ○ Enable ● Disable

Process monitoring

Use or not ● Enable ○ Disable

Process monitoring

Monitoring process:

Operation

Process monitoring

To be use:

To make the process monitoring function effective, choose "To be use" for the To be use line in the Log monitoring section. If not, choose "Disable."

Process monitoring settings:

Use the Add button to increase items for monitoring settings (maximum of eight settings).

Monitoring process:

Sets process to monitor.

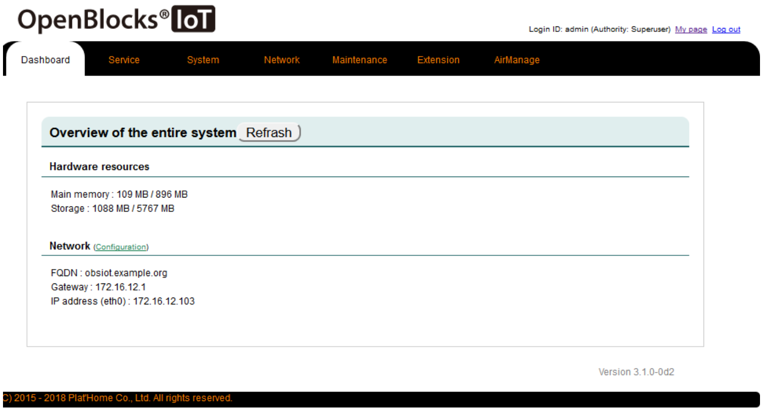
For accurate checking, it is recommended to set this up, including the path.

After completing setup, press the Save button to finish monitoring settings.

When the Save button is pressed, any process already in an attention calling status will be released from such status.

Can check the attention status from the Dashboard.

●If no attention has occurred



Overview of the entire system

Hardware resources

Main memory : 109 MB / 896 MB
Storage : 1088 MB / 5767 MB

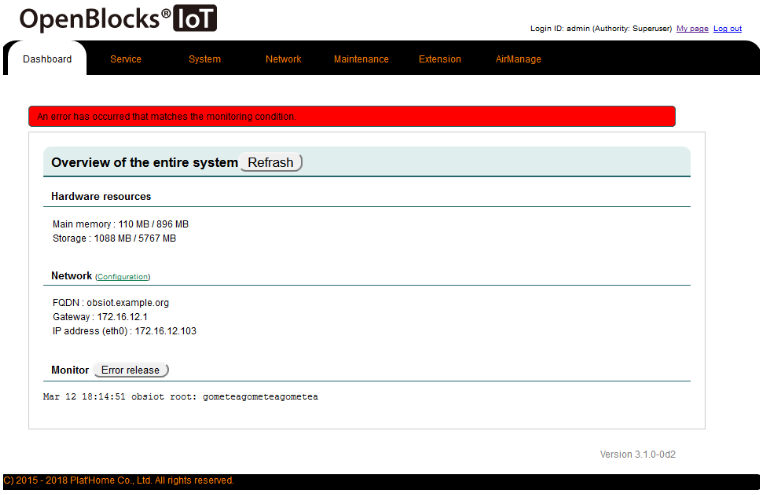
Network

FQDN : obsiot.example.org
Gateway : 172.16.12.1
IP address (eth0) : 172.16.12.103

Version 3.1.0-0d2

C) 2015 - 2018 Plat'Home Co., Ltd. All rights reserved.

●In an attention calling state



An error has occurred that matches the monitoring condition.

Overview of the entire system

Hardware resources

Main memory : 110 MB / 896 MB
Storage : 1088 MB / 5767 MB

Network

FQDN : obsiot.example.org
Gateway : 172.16.12.1
IP address (eth0) : 172.16.12.103

Monitor

```
Mar 12 18:14:51 obsiot root: gometeagometeagometea
```

Version 3.1.0-0d2

C) 2015 - 2018 Plat'Home Co., Ltd. All rights reserved.

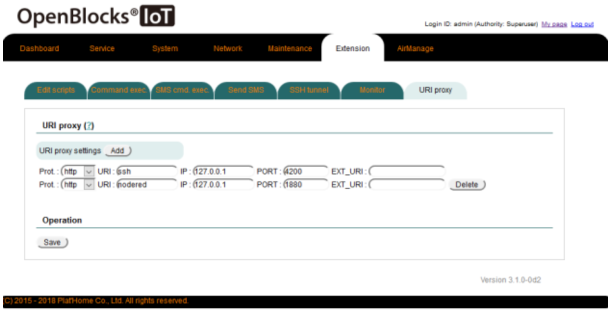
Pressing the Error release button to release the attention calling state.
If logs of attention calling exceeds a certain number of lines, a button showing all logs will be displayed. Press this button to check the logs of preset monitoring status.

9-24 URI proxy function

With the web process engine function in OpenBlocks IoT Family, can access the web on your own host or others' hosts via WEB UI, using the **[Extension]-[URI proxy]** tab.

By setting up this function, can access web processes from your own host or others' hosts. In consideration of security, it is recommended to use this function.

For web processes in operation or that can be operated in the chassis, refer to "10-4 List of ports to use."



URI proxy (?)

URI proxy settings

Prot. : http URI : ssh IP : 127.0.0.1 PORT : 4200 EXT_URI :

Prot. : http URI : nodered IP : 127.0.0.1 PORT : 1880 EXT_URI :

Operation

Set up web service to be accessed via WEB UI from the URI proxy tab in the Extension tab.

Prot.:

Choose "http" or "https" for the protocol of a webpage to access.

URI:

Set up a unique URI.

*Alphanumerical characters only are supported.

Ex.) Node-RED: nodered

IP:

Designate your own host or others’ host on which the web service to be accessed is running with an IP address in an IPv4 format.

Ex.) Node-RED: 127.0.0.1

PORT:

Set up the port number in which the web service to be accessed is running.

Ex.) Default example of Node-RED: 1880

EXT_URI:

Can set up additional URIs to access. To access a specific URI, set this item up.

Ex.)

Node-RED worldmap setting example: worldmap

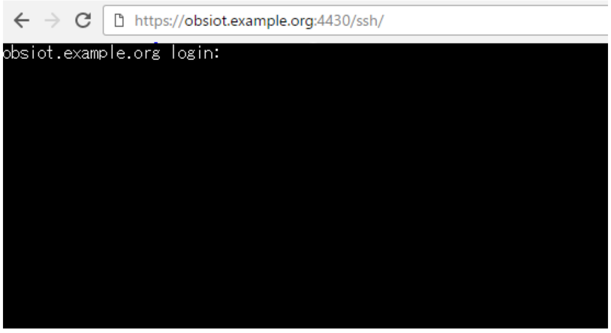
If the protocol of a web service this function references to is different, as to whether it can be accessed or not will differ.

WEB UI Access protocol	Reference web service Protocol	Access
HTTP	HTTP	Possible
HTTP	HTTPS	Impossible
HTTPS	HTTP	Possible
HTTPS	HTTPS	Possible

9-25 Web console function

A shell in a box runs in the OpenBlocks IoT Family. With this process, the console function can be used via a web browser. This function uses Port 4200. In terms of security, as the unit doesn't have a function to open this port by default, access it by using the URI proxy function.

*Supports access via HTTPS only.



```
obsiot.example.org login:
```

This is the screen for this function.

We have an account for which all sudo functions are effective for the sake of this function. Cannot login with the root account.

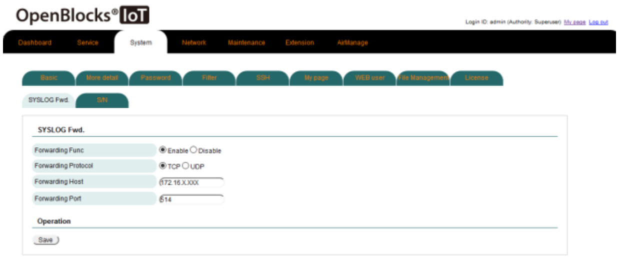
AC: obsroot

PW: 0BSI0T *"0" is zero.

*As the password may be compromised, change it using the password command.

9-26 SYSLOG forwarding function

All SYSLOG files outputted in this unit can be forwarded to an external SYSLOG server. Can make this setup from the SYSLOG Fwd, using the **[System]-[SYSLOG Fwd.]** tab.



SYSLOG Fwd.

Forwarding Func	● Enable ○ Disable
Forwarding Protocol	● TCP ○ UDP
Forwarding Host	172.16.X.XXX
Forwarding Port	514

Operation

SYSLOG Fwd.

Forwarding Func:

Sets the SYSLOG forwarding function.

To forward SYSLOG, choose "To be use."

Forwarding protocol:

Choose either "TCP" or "UDP" as the protocol for SYSLOG forwarding.

Forwarding host:

Sets the host to forward SYSLOG as an IP address or in an FQDN format.

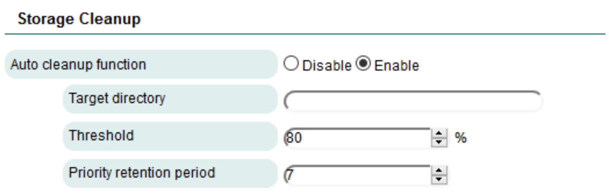
Forwarding port:

Sets the port number to forward SYSLOG. Normally, no need to change from "514."

After completing the settings, press the Save button to make settings effective.

9-27 Storage cleanup function

This function will delete previous files whose priority retention period has elapsed in a specific directory when storage has exceeded a threshold, using the **Storage Cleanup** menu in the **[System]-[More detail]** tab.



Storage Cleanup

Auto cleanup function	○ Disable ● Enable
Target directory	
Threshold	80 %
Priority retention period	7

Storage cleanup

Auto cleanup function

To use this function, choose "Enable." If not, choose "Disable."

Target directory:

Setup a directory to store files subject to cleanup.

Do not designate a directory with important files (such as commands and library).

Threshold:

Assign use percentage of the storage to be used as a threshold to apply this function.

Priority retention period:

Specifies how many days files must be retained.

Files retained within number of days specified will not be deleted.

9-28 Power supply monitoring function

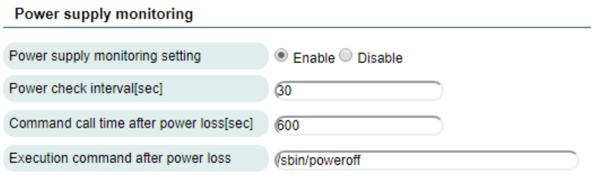
The OpenBlocks IoT VX2 can use an built-in battery module. If this module is used, operation is possible even if AC power supply is temporarily lost.

When a preset time elapses while the power supply is lost, the preset command is executed.

This function can be setup using the **Power supply monitoring** menu in the **[System]-[More detail]** tab.

* The **Power supply monitoring** menu will be displayed even if the built-in battery module is not installed as long as it is a model compatible with the built-in battery module. As a matter of course, this function does not work on a machine that does not have an built-in battery module.

* This function may not work if the built-in battery module is not fully charged.



Power supply monitoring

Power supply monitoring setting	● Enable ○ Disable
Power check interval[sec]	30
Command call time after power loss[sec]	600
Execution command after power loss	/sbin/poweroff

Power supply monitoring

Power supply monitoring:

To use this function, choose "Enable." If not, choose "Disable."

Power check interval[sec]:

Specify the interval time to check the power supply status in seconds.

Command call time after power lost[sec]:

Specify the time to execute the execution command after lost of power after switching to the operating state of the built-in battery in seconds.

Execution command after power lost:

Specify the pathane of command to shut down the stable system steadily such as “/sbin/poweroff”.

Also, if you need to shut down the system as well as other processes at the same time, create and specify a script.

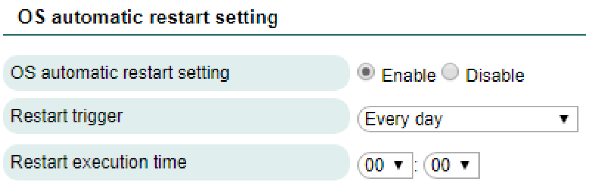
9-29 Periodic restart function

Applications developed independently by users due to continuous operation may accumulate memory fragments and make the operation of the OS unstable.

In this case, it can be solved by periodically restarting the OS.

This function can be setup using the **OS automatic restart** menu in the **[System]-[More detail]** tab.

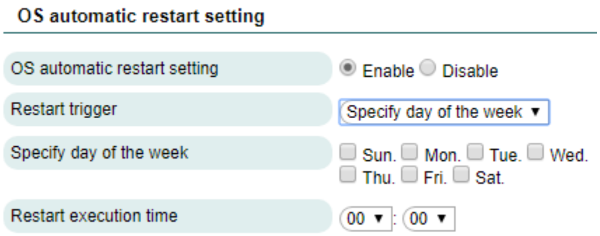
*Every day



OS automatic restart setting

OS automatic restart setting	● Enable ○ Disable
Restart trigger	Every day ▼
Restart execution time	00 ▼ : 00 ▼

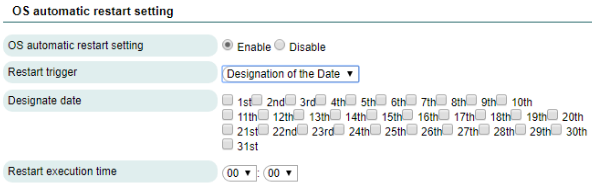
*Specify day of the week



OS automatic restart setting

OS automatic restart setting	● Enable ○ Disable
Restart trigger	Specify day of the week ▼
Specify day of the week	□ Sun. □ Mon. □ Tue. □ Wed. □ Thu. □ Fri. □ Sat.
Restart execution time	00 ▼ : 00 ▼

*Designation of the date



OS automatic restart setting

OS automatic restart setting	● Enable ○ Disable
Restart trigger	Designation of the Date ▼
Designate date	□ 1st □ 2nd □ 3rd □ 4th □ 5th □ 6th □ 7th □ 8th □ 9th □ 10th □ 11th □ 12th □ 13th □ 14th □ 15th □ 16th □ 17th □ 18th □ 19th □ 20th □ 21st □ 22nd □ 23rd □ 24th □ 25th □ 26th □ 27th □ 28th □ 29th □ 30th □ 31st
Restart execution time	00 ▼ : 00 ▼

OS automatic restart

OS automatic restart setting:

To use this function, choose "Enable." If not, choose "Disable."

Restart trigger:

Select either **Every day**, **Specify day of the week** or **Designation of the date**.

Specify day of the week:

Specify the date of the week on which OS restart is executed.

Multiple days can be specified.

Designate date:

Specify the date on which OS restart is executed.

Multiple days can be specified.

Restart exection time:

Specify the time to restart OS.

9-30 Public key addition function for package repository

There are cases where you want to use a nonstandard package repository for installing and updating software packages.

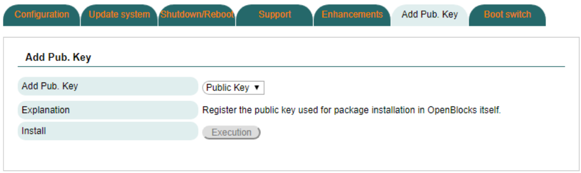
In this case, you need to add the public key of the target package repository to this machine.

Also, even if you unintentionally deleted the public key, please add using this function.

This function can be setup using the **Add Pub. Key** menu in the **[Maintenance]-[Add Pub. Key]** tab.

*If there is no public key that can be added, this menu and operation tab are not displayed.

*It need to add a package repository to browse, not just the public key. In this case, AirManage etc. recommends changing **source.list**.



Add Pub. Key

Add Pub. Key	Public Key ▼
Explanation	Register the public key used for package installation in OpenBlocks itself.
Install	Execution

Add Pub. Key

Add Pub. Key:

Select the Public key you want to add.

Explanation:

The description of the selected public key is displayed.

Install:

Installs the selected public key.

Since this function uses Internet communication, please be able to make the network settings beforehand on the Internet.

The public keys that can be installed from this function are as follows.

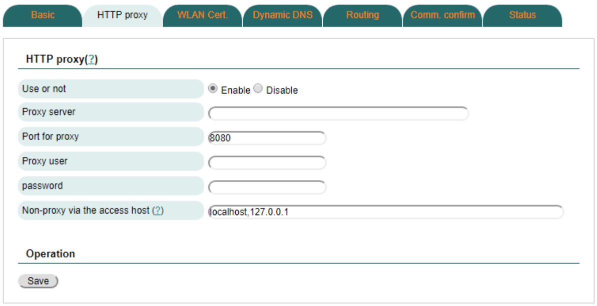
The public keys that can be installed	Remarks
Node.js	FW 3.0 or later is installed as standard.
Docker	FW 3.0 or later is installed as standard.
Microsoft	FW 3.2 or later is installed as standard.

9-31 HTTP proxy function for client

This function is a function to operate this machine on a network that goes out to the Internet only with the HTTP proxy.

This function can be setup using the **HTTP proxy** menu in the **[Network]-[HTTP proxy]** tab.

*Even if this function is switched to a mobile line etc., the setting will remain valid. In this case, the network environment becomes incompatible with the setting, so communication can not be performed. Therefore, please do not use with mobile line.



HTTP proxy(?)

Use or not	● Enable ○ Disable
Proxy server	
Port for proxy	8080
Proxy user	
password	
Non-proxy via the access host (?)	localhost,127.0.0.1

Operation

HTTP proxy

Use or not:

To use this function, choose "Enable." If not, choose "Disable."

Proxy server:

Specify the IP address or FQDN of the proxy server you want to go through.

Port for proxy:

Specify the port number of the proxy server you want to go through.

Proxy user:

If basic authentication for accessing the proxy server is required, specify the user name.

password:

If basic authentication for accessing the proxy server is required, specify the password.

Non-proxy via the access host:

Specify a host not accessing via proxy.

To specify more than one, please specify with "," separator.

It can not specify a network address.

Chapter 10: Cautions and supplementary information

10-1 Power supply of OpenBlocks IoT VX series

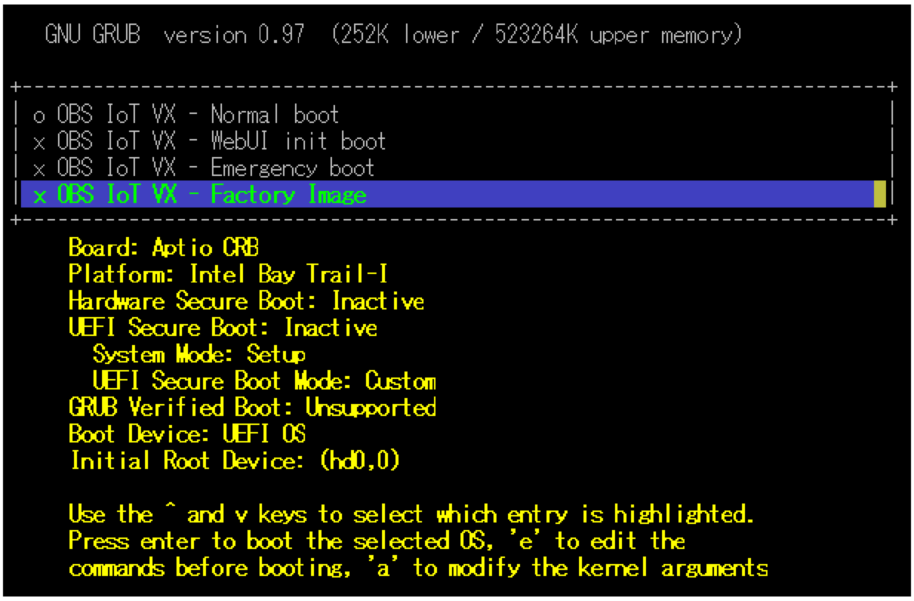
Using any power supply other than AC adapter or wide range PS input will not be covered by warranty. For this reason, please take due caution about the power supply being used.

10-2 Automatic reboot function

This WEB UI controls the modem for the mobile network. If the modem of the mobile network is unexpectedly unable to return to normal, the unit will be rebooted.

10-3 Factory Reset (reset to factory default)

To reset the unit to factory default, when a package to the storage domain has been added or if important data has been deleted with the OpenBlocks IoT VX series, choose "Factory Image" from the GRUB menu to do so.
Please note that if the unit is reset to factory default, data setup, etc. will be deleted.



```
  GNU GRUB  version 0.97  (252K lower / 523264K upper memory)

+---------------------------------------------------------------------+
| o OBS IoT VX - Normal boot                                          |
| x OBS IoT VX - WebUI init boot                                      |
| x OBS IoT VX - Emergency boot                                       |
| x OBS IoT VX - Factory Image                                        |
+---------------------------------------------------------------------+
    Board: Aptio CRB
    Platform: Intel Bay Trail-I
    Hardware Secure Boot: Inactive
    UEFI Secure Boot: Inactive
      System Mode: Setup
      UEFI Secure Boot Mode: Custom
    GRUB Verified Boot: Unsupported
    Boot Device: UEFI OS
    Initial Root Device: (hd0,0)

    Use the ^ and v keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    commands before booting, 'a' to modify the kernel arguments
```

10-4 List of ports to use

OpenBlocks IoT Family, including WEB UI uses or may use the following ports:

Service type	Port number	Remarks
SSH	22	Port number can be changed.
DNS	53	
DHCP	67	
NetBIOS	137	With Sama installed (UDP)
NetBIOS	138	With Sama installed (UDP)
NetBIOS	139	With Sama installed
Samba	445	With Sama installed
Modbus	502	With IoT data control installed
WEB UI (HTTP access)	880	
Node-RED	1880	With Node-RED installed (Port number can be changed).
Shell in a box (WEB SSH)	4200	
WEB UI (HTTPS access)	4430	

10-6 Automatic external storage mounting function

If a device with a particular volume label is found in WEB UI, it will be automatically mounted.
Please use when managing storage destination with WEB UI functions.

Volume label	Mounting destination	Remarks
WEBUI_STORAGE	/var/tmp/storage	Use NTFS as the file system.

OpenBlocks IoT Family WEB UI Set-up Guide

Version 3.2.0 (Aug 23, 2018)

Plat'Home Co., Ltd.
NIHON BUILDING KUDANBEKKAN, 3F
4-2-3, Kudankita, Chiyoda-ku, TOKYO 102-0073, JAPAN