# Industrial wireless router

# 『CPTrans-MJW/CPTrans-MGW』

# Application Manual

**Hitachi Industrial Equipment Systems Co., Ltd.**

<Notice>

Please read the product specifications of the "CPTrans-MJW" and "CPTrans-MGW" (hereinafter referred to as "this product" or “CPTrans”) and the specifications of the related products carefully, and use the product correctly by following the instructions such as the knowledge of the device, safety information, precautions, operation, and handling methods.

The product must be used in accordance with the various operating ranges specified in the product specifications and instruction manuals.

Do not use parts other than those described in this manual, replace or modify parts other than those in our supply range, or use or operate in any manner other than those described in this manual. Failure to do so may cause a malfunction of the machine or personal injury. We are not responsible for any accidents caused by these.

In order to use this product correctly and safely, please start the operation after reading it to the end. Keep this manual in custody after the start of operation.

Revision History Table

| No | Description | Date of revision | Manual No. | Applicable firmware Ver |
|---|---|---|---|---|
| 1 | New | Sep 24, 2021 | NJ904 | mjw_generic_2021_09_24_4 or higher |
| 2 | - CPTrans-MGW<br>- Monitoring, band apps added<br>- Initial value for some apps changed | Feb 4, 2022 | NJ904A | mjw_generic_2022_02_03_5 or higher<br>mgw_generic_2022_02_03_5 or higher |

<Handling of this manual>

- Unauthorized reproduction of the contents of this manual is prohibited.
- The contents of this manual are subject to change without prior notice.
- We are not responsible for the costs incurred such as damage caused by incorrect use of this manual and the products described in this manual, and recovery from such damage.

<Name used in this manual>

- Windows 10 is a registered trademark of Microsoft Corp. of the United States.
- Ethernet is a registered trademark of Xerox Corp.
- Other product names are generally trademarks or registered trademarks of each company.

<About GPL license>

This product uses software that complies with the licenses of GPL version2 0. For GPL licensing, please refer to the following URLs.

http://www.gnu.org/licenses/gpl-2.0.html

Contact your distributor for software distribution.

The cost incurred during distribution will be borne by the customer.

## Safety Instructions

**To use the product safely, be sure to observe the following**

Important information to prevent injury to the user and other persons, as well as damage to property, and to use the product safely. Read this manual carefully and observe the following precautions after understanding the contents [indications and graphic symbols].

| | |
|---|---|
| **Warning** | This symbol indicates "risk of death or serious injury. |
| **Note** | This symbol indicates that there is a risk of personal injury or *2 of property damage that may result in *1. |

| Explanation of Symbols | |
|---|---|
| | "Warning and warning" is provided. |
| | This symbol indicates "prohibited" content that should not be used. |
| | This is the "forced" content to be executed without fail. |

*1: Injury refers to injuries, burns, electric shocks, etc. that do not require injuries or long-term hospitals for treatment.

*2: Physical damage refers to extended damage related to households, household goods, livestock, pets, etc.

| **Warning** | |
|---|---|
| **Prohibited** | - Do not disassemble, modify, or repair.<br>Failure to do so may result in fire, electric shock, or injury.<br>Modification violates the Radio Law, and punishment is imposed.<br>Contact your distributor or distributor for repair or inspection. |
| **Force** | - If you notice an unusual odor, noise, or smoke, immediately stop supplying power to the product.<br>Failure to do so may result in fire, electric shock, or injury.<br>Contact your distributor or distributor for repair or inspection. |
| **Force** | - If it is dropped or subjected to strong impact, immediately turn off the power and disconnect the power cable or AC adapter.<br>Fire or electrical shock may result.<br>Contact your distributor or distributor for repair or inspection. |
| **Force** | - Use the supplied AC adapter.<br>Doing so may cause smoking, fire, or electric shock. |
| **Prohibited** | - Do not turn on the power near flammable, combustible, or flammable materials.<br>(Kerosene, gasoline, thinner, benzene, toner, flammable gas (spray), cigarette butts, etc.)<br>Explosion or fire may occur. |
| **Force** | - When mounting the product on a car, etc., wire the product so that it does not interfere with driving and attach it securely.<br>Cables entangled with feet or driving equipment may cause accidents.<br>Failure to do so may result in an accident due to surprise and sudden braking when the product falls. |
| **Prohibited** | - Do not operate while driving a car.<br>Doing so may cause a traffic accident.<br>Stop the car in a safe place before using it when the driver operates it. |
| **Prohibited** | - Keep out of reach of children.<br>May cause injury. |
| **Prohibited** | - No voltage is applied to pins ① to ⑦ of the power connector "S08B-XASK-1" of 8Pin.<br>Doing so may cause smoking, fire, or electric shock. |

## ⚠Warning

**Observe the following precautions when using the device near a cardiac pacemaker or other medical device.**

**Prohibited**

- Do not bring the device to an operating room, intensive care unit (ICU), coronary artery condition monitoring unit (CCU), or the like.
- Do not turn on the power in a laboratory, medical room, hospital room, treatment room, etc.
- Even in a lobby, etc., do not turn on the power if there are medical devices nearby.
- Do not turn on the power in crowded places such as a full train because it may be in close proximity to those wearing medical devices such as cardiac

**Force**

- If you are wearing a medical device such as a cardiac pacemaker, carry and use the antenna at least about 22cm away from the pacemaker site.
- If medical institutions individually stipulate areas where use is prohibited or where carry-in is prohibited, they follow the instructions of the medical organization.
- When medical equipment is used outside a medical facility (home care, etc.), check with the medical equipment manufacturer individually about the effects of radio waves.

Radio waves may affect medical equipment and cause accidents due to malfunction.

## ⚠Warning

| | |
|---|---|
| **Force** | - Use the specified antenna.<br>It is a violation of the Radio Law and penalties are imposed. |
| **Prohibited** | - Do not touch with wet hands.<br>Electric shock or fire may result. |
| **Prohibited** | - Do not place containers containing liquids such as cups nearby.<br>If liquid spills and gets inside, it may cause electric shock or fire. |
| **Prohibited** | - Do not use or store the product in the following locations.<br>・A floor or other location exposed to water or high humidity.<br>・Locations subject to direct rain, fog, etc.<br>・Locations subject to high temperatures, such as near a fire or heating device.<br>・In direct sunlight or inside a car on a hot day.<br>Doing so may cause fire, electric shock, or malfunction.<br>・Do not place the unit on an uneven surface.<br>Failure to do so may result in injury or equipment damage. |
| **Prohibited** | - Do not touch the main unit during use at high temperatures.<br>Failure to do so may result in burns or injuries. |
| **Prohibited** | - Do not turn on the power near high-precision electronic devices or devices that handle weak signals.<br>Otherwise it affects to the electronic equipments and malfunction on them.<br>- When using the product, check with the electronic equipment manufacturer about the effects of radio waves. |
| **Prohibited** | - Do not turn the power on near phones, TVs, or radios.<br>Doing so may affect sound, images, etc.<br>Keep away from the product. |

| PRECAUTIONS ON USE<br>To avoid failure, loss of data, or damage, observe the following precautions. |
|---|
| - In the operating frequency band of this product, in addition to industrial, scientific, and medical equipment such as microwave ovens, premises radio stations for identifying mobile units (radio stations requiring a license), specified low-power radio stations (radio stations requiring no license), and amateur radio stations (radio stations requiring a license) used in the manufacturing lines of factories are operated. |
| - Before using this product, confirm that premises radio stations for identifying mobile units, specified low-power radio stations, and amateur radio stations are not in operation nearby. |
| - In the event that this product causes harmful radio interference to premises radio stations for identifying mobile units, immediately change the operating frequency or stop radio wave emission, and contact the supplier and consult with them regarding measures to avoid interference (e.g., installation of partitions). |
| - Contact your dealer if you notice any trouble, such as the occurrence of harmful radio interference from this product to specified low-power radio stations or amateur radio stations for identifying mobile units. |
| - Used and stored within the specified temperature range.<br>Malfunction may result.<br>Do not use or store in extremely high or low temperatures. |
| - Do not expose to abrupt changes in temperature.<br>Condensation may occur, resulting in failure, malfunction, or loss of stored contents.<br>If condensation occurs, dry the product naturally before use. |
| - Do not use or store the product in the following locations.<br>・Magnets, speakers, etc. are emitted. Close to objects.<br>・A place where generates salt damage and corrosive gases.<br>・A dusty place.<br>・Locations where vibration is high.<br>Otherwise failure or malfunction can result. |
| - When attaching to other equipment, etc., install the main unit so that it is not twisted.<br>Attaching the product to the equipment while it is twisted may cause failure or performance deterioration. |
| - Use the specified mounting bracket.<br>Otherwise, the main unit may be twisted, resulting in deterioration of performance. |
| - Do not use benzene, thinner, or an abrasive to clean the surface.<br>Otherwise, this may cause deterioration of the product or characters.<br>Wipe dirt with a soft, dry cloth. |
| - Do not turn off the power during access. Do not unplug the cable.<br>Otherwise, data may be lost or damaged. |
| - Do not allow liquids to enter the connectors.<br>Failure to do so may result in fire, burns, injury, or electric shock. |
| - Do not allow conductive foreign substances (metal fragments, pencil leads, etc.) to come into contact with the connector.<br>Failure to do so may result in fire, burns, injury, or electric shock. |
| - Do not perform continuous data communication for a long time at high temperature.<br>Doing so may affect communication quality. |
| - Do not peel off the nameplate seal.<br>If the contents of the nameplate cannot be checked, repair may not be possible. |
| - The customer is responsible for ensuring security. (It is recommended to close ports that are not required.)<br>As for the damage caused by the security failure<br>Please be aware that we are not responsible for this. |
| - In order to ensure security, please close any ports other than the minimum required ones. |
| - For security reasons, it is recommended that you change the password settings of this product regularly. |
| - We ask our customers to have spare parts in case of emergency. |

**Note**

- Unauthorized copying and distribution of this magazine is prohibited.
- The contents and images of this publication may differ from the actual ones. It may also differ depending on the software version or the conditions of the carrier. The contents of this manual are subject to change without prior notice due to improvements to the operating environment or other circumstances. Please note.
- Except for those directly related to the manufacture of this product, we are not responsible for any damage caused directly or indirectly by relying on the information described in this document and this product.
- Please note that we shall not be liable for any damage, injury, theft, or damage to the product caused by damage to the structure or work in a bad work environment during the installation work of this product.
- We shall not be held responsible for inconvenience, damage, or damage caused by malfunction, compatibility, or other system errors caused by the user modifying the registry settings or operation system software of the PC connected to this product.
- We are not responsible for any damage or malfunction caused by intentional or inadvertent use of the user (such as dropping, flooding, impact, damage, or unreasonable movement), theft, or injury.
- Before using this product, please understand that internet connection is dangerous, always obtain new information and take security measures on your own responsibility.
- This product is a device capable of wireless data communication. We are not responsible for any damage caused by malfunction, malfunction, power failure, line failure, or other external factors of this product.
- This product is intended for domestic use. The watch cannot be used overseas.
- The FOMA terminal can be used only in the service area of the carrier you are using.
- If radio wave conditions deteriorate more than a certain level, communication may be suddenly interrupted. However, even in areas with good signal quality, communication may be interrupted depending on the network environment.
- Mount the product on a flat surface that is not uneven as a wall mounting condition.
- We assume no responsibility for damage caused by incorrect mounting conditions.
- This product is made of resin molding. When mounting this product, be careful not to apply a strong force exceeding the specified torque (0.8N·m) as it may cause a failure.
- Be careful not to drop the product from a high place, as it may cause malfunction.
- As 10022 ports are used for our maintenance, do not use 10022 ports.
- Change the setting of this product from only one connected device.
- Wireless communication may not be possible depending on the operating environment.
- Especially when mounted on a mobile unit, handover (base station switching) tends to occur frequently. Therefore, thoroughly investigate countermeasures such as retransmission and the usage environment to ensure that communication is not interrupted due to handover before use.
- Please take the following precautions when supplying power to this product.
  1) Noise immunity standards
     The noise immunity of this product is at the following levels.
     a. Inductive noise: OK up to IEC61000-4-4 level 3 (NG for level 4)
     b. Electrostatic noise: OK up to IEC61000-4-2 level 3 (NG for level 4)
  2) ISO 7637-2 (Standards for Power Supply Testing Required for Automotive Equipment)
     This product does not comply with the above standards.
     · When connecting to an ACC-powered power supply of a car, etc., supply DC/DC converters between them, or supply them from a power supply that complies with the applicable standards. Otherwise, it may result in the destruction of this product.
     · In the amount of electrical energy and voltage fluctuation compared to the induced noise when supplied from a power source conforming to the above standards
       Otherwise, reset, malfunction, or damage to the equipment may result.
  3) Notes on the case that does not start up
     (1), If the power supply does not start even when (2) is complied with, there is a possibility of insufficient current in the power supply.

**Precautions When Using USIM Cards**

- Use only the specified USIM cards.
  If a product other than the specified one is used, it may cause data loss or failure.
- Do not use excessive force when installing or separating USIM card.
  Doing so may cause data loss, malfunction, etc.
- Do not contaminate the metallic contacts on USIM card.
  Doing so may cause data loss, malfunction, etc.
- Do not use USIM card for any other purpose.
  Doing so may cause data loss, malfunction, etc.
- Be careful not to transfer or lose USIM card to another person.
  We are not responsible for any damage caused by the transfer, theft, or loss of this product.

≪ Contents ≫

List of Names Handled in This Manual

| Name | Description |
|---|---|
| CRG | KDDI Closed Remote Gateway, a closed radio network service offered by KDDI Corporation. |
| GUI | Graphical User Interface |
| AP | Application |
| AF | Application Framework |
| LAN | Local Area Network |
| WAN | Wide Area Network |
| LAN IP | IP address of network device in LAN side |
| WAN IP | IP address of network device in WAN side |

# 1. Overview

## 1.1 Scope of Application

This manual applies to the Industrial wireless router “CPTrans”.

## 1.2 Product Overview

CPTrans is a cellular router with multi-carrier compatible LTE networks (hereinafter referred to as "cellular networks") such as KDDI, NTT, and Softbank.

Routing (address translation) is performed between the LAN communication device (Ethernet) and the WAN communication device. Communication between LAN and WAN can be realized with simple settings.

The main features of this product are as follows.

- ✧ The routing method supports static routing in addition to NAT (virtual servers), static NAT, NAPT (masquerade), and DMZ.
- ✧ Ethernet supports 100Mbps/10Mbps (full-duplex/half-duplex, auto-negotiation)
- ✧ Internet, KDDI CRG (Closed Remote Gateway) services, NTT-related networks, and Softbank networks can be connected
  * KDDI CRG servicing is available only for CPTrans-MJW
- ✧ Communication between cellular network and CPTrans can be disconnected automatically after certain period of time.
- ✧ Wireless LAN supports IEEE802 11b/11g/11n (2.4GHz) and 11a/11ac (5.0GHz).
  * 11a/11ac (5.0GHz) is available only for CPTrans-MJW
- ✧ Setting can be configured by CLI (command control) or GUI (web browser).
- ✧ Automatically connects to the cellular network by receiving SMS (Short Message Service) for starting the terminal from the CRG network.
- ✧ Built-in security function by MAC/IP/Port filtering
- ✧ With DNS relay function, LAN-side devices can specify CPTrans as a DNS server.
- ✧ A DHCP server function can be installed and assigned automatically to LAN-side devices or up to 16 devices can be assigned fixed at the specified IP-range.

[Caution]

Contact your network provider for closed network services for each carrier and for other networks.

## 1.3 System configuration

Figure 1.1 Example system configuration shows an example of system configuration using this product.

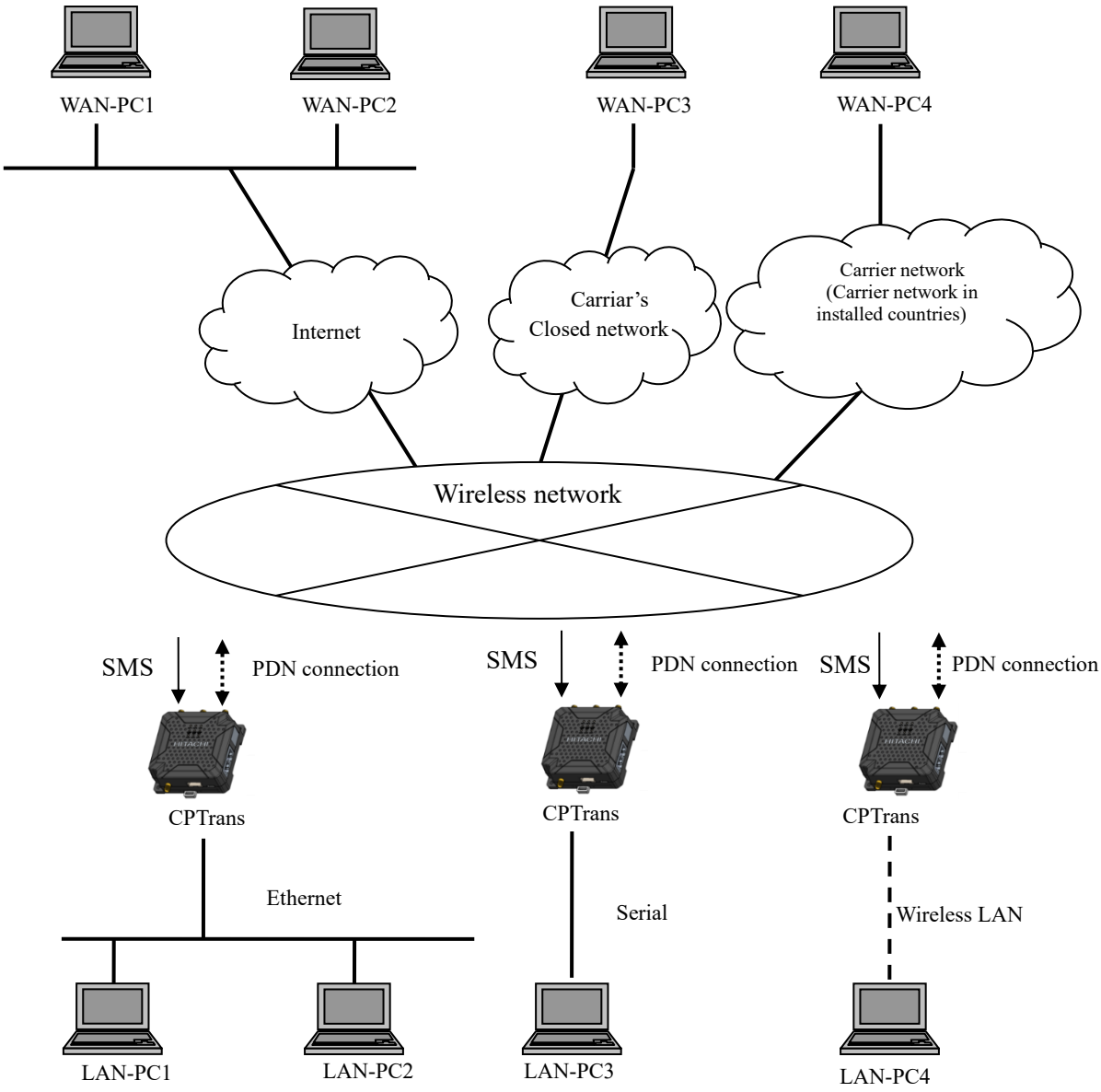



**Figure 1.1 Example system configuration**

# 2. Specifications

## 2.1 Components include

Table 2.1 CPTrans-MJW configuration and Table 2.2 CPTrans-MGW configuration show included components of CPTrans-MJW and CPTrans-MGW.

Please use official supported antennas for LTE and WLAN connection.

Using unsupported antennas for this unit may cause a violation related to radio law. Please contact supplier for usage of unsupported antennas.

**Table 2.1 CPTrans-MJW configuration**

| No | Name | QTY | Note |
|---|---|---|---|
| 1 | Industrial wireless router | 1 | CPTrans-MJW |
| 2 | User manual | 1 | Attached document |
| 3 | Caution label | 1 | Caution stickers for use of wireless LAN devices |

**Table 2.2 CPTrans-MGW configuration**

| No | Name | QTY | Note |
|---|---|---|---|
| 1 | Industrial wireless router | 1 | CPTrans-MGW |
| 2 | User manual | 1 | Attached document |
| 3 | Caution label | 1 | Caution stickers for use of wireless LAN devices |
| 4 | CE declaration | 1 | Attached document |

## 2.2 Appearance and dimensions

### 2.2.1 Outline

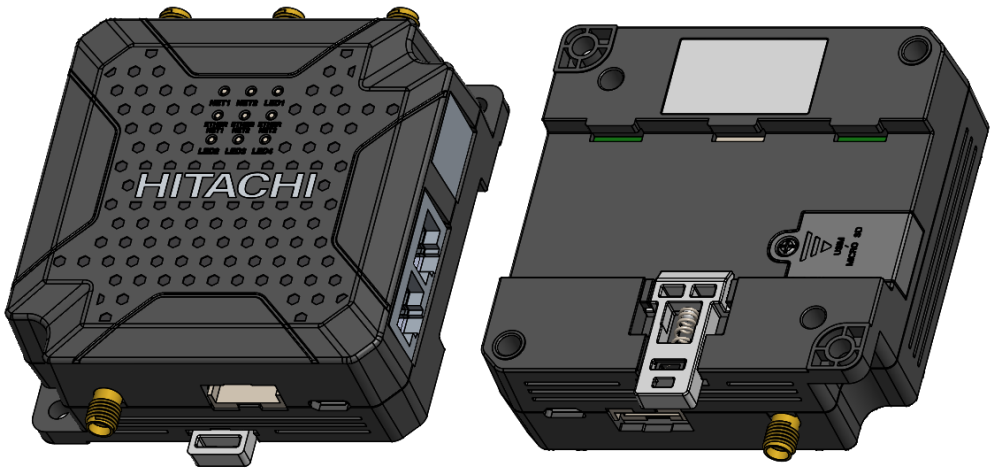



**Figure 2.1 Outline for CPTrans**

2.2.2 Dimension details

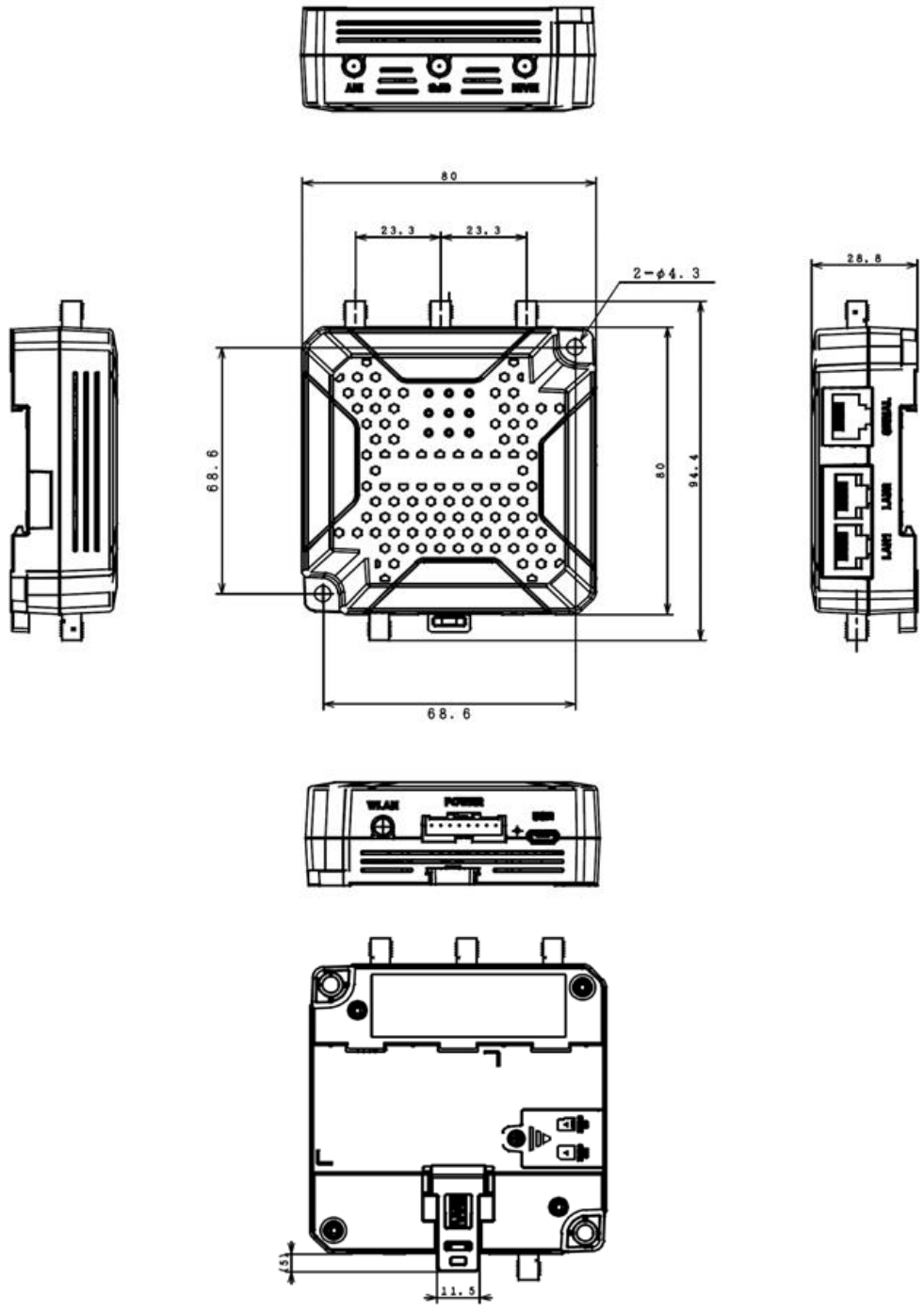



**Figure 2.2 Product dimensions [mm]**

## 2.3 Explanation on each detail

1) Product

Explanation of each part description are shown on below Figure 2.3 Explanation on each detail.

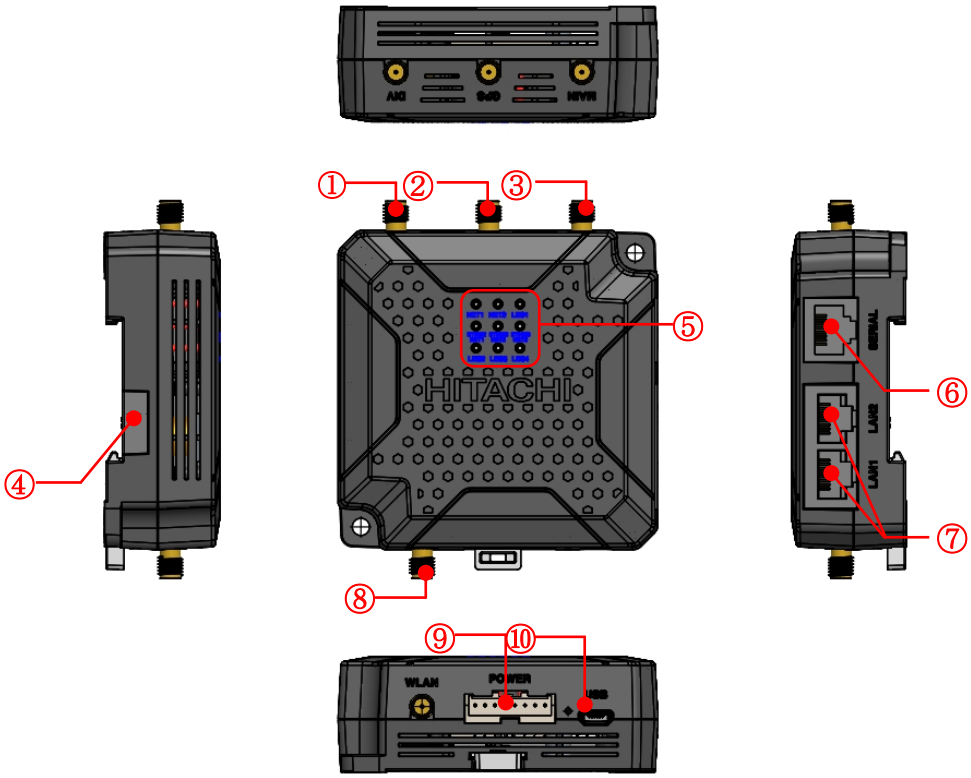



**Figure 2.3 Explanation on each detail**

**Table 2.3 Explanation on each detail**

| No. | Item | Detail |
|---|---|---|
| (1) | DIV(LTE) | Sub connection for LTE antenna. |
| (2) | GPS | Connection for GPS antenna. |
| (3) | MAIN(LTE) | Main connection for LTE antenna. |
| (4) | Micro SIM / SD Card slot | Insert Micro SIM／SD card by taking off its protection cover. |
| (5) | LED | Show LED status of this CPTrans-MGW |
| (6) | SERIAL | Serial connector for RS232C and RS485 |
| (7) | LAN1, LAN2 | Connection for Ethernet cable |
| (8) | WLAN | Connection for wireless LAN antenna |
| (9) | POWER | DC power will be collected from this 8Pin socket. |
| (10) | USB | Not supported |

*1 : In case of connecting LTE, please attach both MAIN & DIV antenna

Table 2.4 SIM / SD card slot to Table 2.7 Pin detail of LAN interfaces describe Table 2.8 describe each interface.

**Table 2.4 SIM / SD card slot**

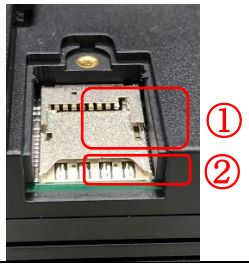
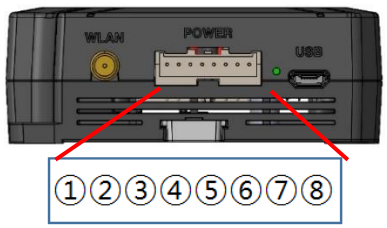
| Item | No. | Description | Remark |
|---|---|---|---|
|  | (1) | Micro SD card slot | Upper side |
| | (2) | Micro SIM card slot | Lower side |

**Table 2.5 8Pin connector**

| Item | | Details |
|---|---|---|
| S08B-XASK-1(JST) | Pin No. | 8-pin、2.5mm pitch |
|  | (1) | NC |
| | (2) | NC |
| | (3) | NC |
| | (4) | GND |
| | (5) | NC |
| | (6) | NC |
| | (7) | GND |
| | (8) | VCC (5 to 24 VDC wide range) |
| Input Voltage | | 5 to 24 VDC (In current loading condition) |

<Caution>: Do not connect (1) to (7) pin to voltage power supply.

For wiring to 8pin connector, please prepare following plug and contact.

- Vendor: JST
- Plug: XAP-08V-1
- Contact: SXA-001T-P0.6

Please prepare applicable cable (AWG# from 28 to 22) for the contact.

**Table 2.6 Pin detail of LAN interfaces**

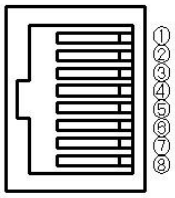
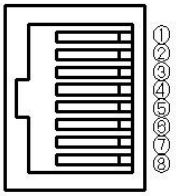
| Item | Pin | Signal | Note |
|---|---|---|---|
|  (RJ-45) | (1) | TXD+ | Send data (+) |
| | (2) | TXD- | Send data (-) |
| | (3) | RXD+ | Receive data (+) |
| | (4) | — | — |
| | (5) | — | — |
| | (6) | RXD- | Receive data (-) |
| | (7) | — | — |
| | (8) | — | — |

**Table 2.7 Pin detail of LAN interfaces**

| Item | Pin | Signal | Note |
|---|---|---|---|
|  (RJ-45) | (1) | SG | Ground for signal |
| | (2) | 485- | 485(-) signal |
| | (3) | 485+ | 485(+) signal |
| | (4) | NC | Not used |
| | (5) | 232SD | Data sending |
| | (6) | 232RD | Data receiving |
| | (7) | 485- | Terminating |
| | (8) | RT | Termination resistor |

<Note>: If termination resister is necessary for RS-485 communication, built-in termination resister (0.5W, 120ohm) can be wired to CPTrans-MGW by making short circuit between No.7 pin “485-” and No. 8 pin “RT”.

2) How to install the equipment

This product has holes for installation on the wall in the enclosure. When installing the unit on a wall, fix it with screws as shown in the following installation example.

- Refer to the section for the mounting positions of hole and sizes.
- Tighten with a torque of 0.8N·m.

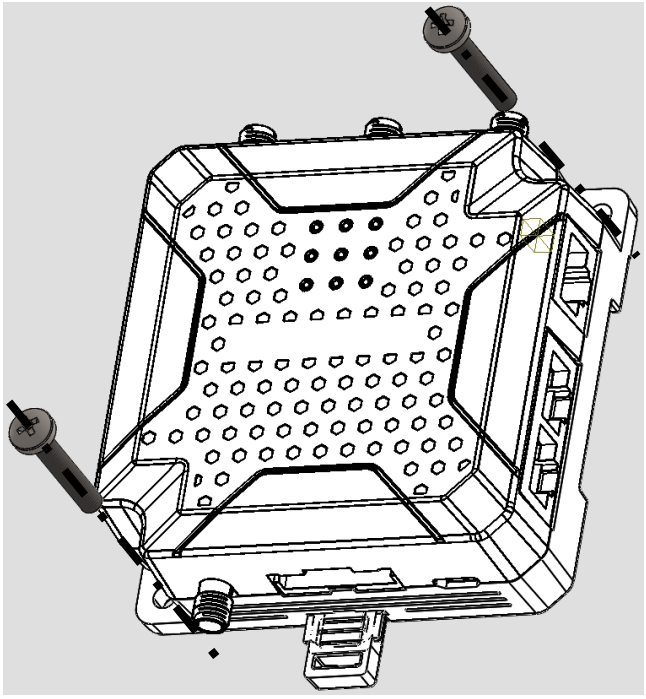


**Figure 2.4 Mounting to wall**

Below shows installation for this product by a DIN rail

(1) Mounting to a DIN rail

① Hook the claw of this product to the DIN rail.

② Press this product to the DIN rail until it clicks. Please mount brackets for fixing this product.

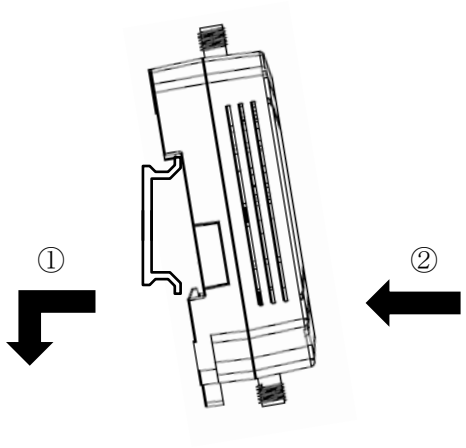



**Figure 2.5 Mounting to the DIN rail**

(2) Removing from the DIN rail

① Move the DIN rail fixing mounting lever toward the bottom.

② Raise this product upward to remove.

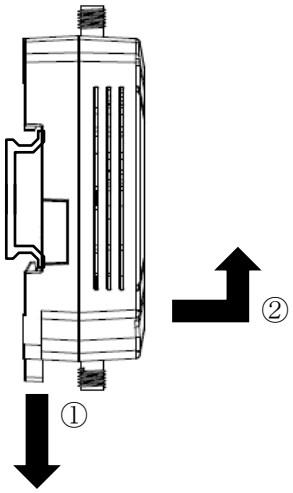



**Figure 2.6 Removing from the DIN rail**

3) Mounting SIM card to CPTrans

When inserting micro USIM, open the cap and insert USIM as shown in Figure 2.7 Insertion of micro USIM.

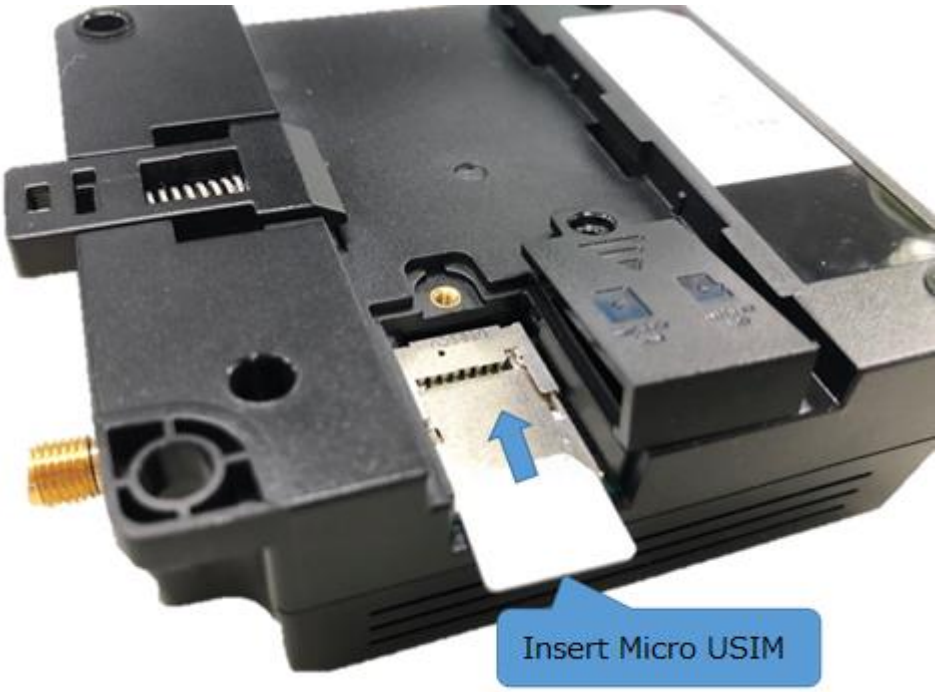



**Figure 2.7 Insertion of micro USIM**

[Caution]

- When inserting micro USIM, be careful not to pull the cap part too much.
  It may cause damage the cap.
- Insert micro USIM in the correct orientation as indicated on the silk.

## 2.4 Main specifications

From Table 2.8 CPTrans-MJW general specification to Table 2.10 CPTrans common specification show the main specifications of this product. The communication speed is the best effort value and actual speed is varies depending on the contract of using SIM card.

**Table 2.8 CPTrans-MJW general specification**

| Item | | Specifications | Remarks |
|---|---|---|---|
| Radio method | Apply chipset | EC25-J STD (LTE)<br>FC20 (WLAN) | |
| | Carrier network | LTE / WCDMA | |
| | Band | LTE FDD: B1/B3/B8/B18/B19/B26<br>LTE TDD: B41<br>WCDMA : B1/B6/B8/B19 | |
| | Data speed (max.) | FDD: 150Mbps(DL)/50Mbps(UL)<br>TDD: 130Mbps(DL)/35Mbps(UL)<br>WCDMA: 384Kbps(DL)/ 384Kbps(UL) | Best effort |
| | WLAN | 802.11b/g/n/a/ac<br>(Available only as access point) | Support both<br>2.4GHz and 5GHz |

**Table 2.9 CPTrans-MGW general specification**

| Item | | Specifications | Remarks |
|---|---|---|---|
| Radio method | Apply chipset | EC25-G STD (LTE)<br>FC20 (WLAN) | |
| | Carrier network | LTE Cat4、3GPP Rel.11 | |
| | Band | LTE FDD:<br>B1/B2/B3/B4/B5/B7/B8/B12/B13<br>/B18/B19/B20/B25/B26/B28<br>LTE TDD: B38/B39/B40/B41<br>WCDMA: B1/B2/B4/B5/B6/B8/B19<br>GSM: 850/900/1800/1900MHz | |
| | Data speed (max.) | LTE FDD: Max 150Mbps (DL)/ Max 50Mbps (UL)<br>LTE TDD: Max 130Mbps (DL)/ Max 35Mbps (UL)<br>DC-HSDPA: Max 42Mbps (DL)<br>HSUPA: Max 5.76Mbps (UL)<br>WCDMA: Max 384Kbps (DL)/ Max 384Kbps (UL) | Best effort |
| | WLAN | 802.11b/g/n (Available only as access point) | 2.4GHz only |

**Table 2.10 CPTrans common specification**

| Item | | Specifications | Remarks |
|---|---|---|---|
| External connection | Ethernet | 10BASE-T/100BASE-TX<br>(Full duplex, Half duplex applicable,<br>Auto MDI/MDI-X applicable) | |
| | Serial | RJ-45 connector (RS232C, RS485) | |
| | GNSS | GPS/GLONASS/BeiDou/Galileo<br>Power supply voltage for GNSS antenna is 3.8VDC | |
| | Antenna | LTE (External antennas / 2pcs)<br>GPS (External antennas)<br>WLAN (External antennas) | Not included |
| | External Interface | USIM Socket<br>Micro-SD Socket<br>8PIN Connector (POW, I/F, GND)<br>RJ45 Connector x3(x2 Ethernet, 1 Serial) | |
| LED | LED | Single color or Double colors | Refer 3.3.1 |
| POW | Voltage range | 5 to 24 VDC | |
| | Power consumption | 6W (3A@5VDC、MAX Power) | Excluding inrush power |
| Environment | Operating temp. | -20 to 60 °C | |
| | Storage temp. | -30 to 70 °C | |
| | Operating humid. | 20 to 95%RH (No condensation) | No condensation |
| | Vibration/Shock | Vibration:<br>JIS C 60068-2-6:2010 (IEC 60068-2-6:2007) compliant<br>Shock:<br>JIS C 60068-2-27:2011 (IEC 60068-2-27:2008) compliant<br>Shock and vibration tests:<br>JIS E4031：2013 (IEC 61373:2010) compliant<br>Category 1 Class B | |
| | Install location | No corrosive gases, no excessive dust | |
| Size | Size(W×D×H) | 80.0mm × 80.0mm × 28.8mm | Excluding protrusions |
| | Weight | Approx.109g | |

# 3. Operating Specifications

## 3.1 Application

Functions on CPTrans are divided in application units (hereafter referred as to AP).Table 3.1 Apps list shows a list of the applications which are installed in CPTrans.

**Table 3.1 Apps list**

| App name | Details |
|---|---|
| System | Setting for user interfaces or to check specific information of this device. |
| Router | Application to make communication setting such as LAN setting and LTE network settings. |
| Scheduled reboot | Application to automatically reboot based on assigned time or day of week. (*Recommend rebooting on certain period for stable operation) |
| Firmware update | Application to update firmware by either manual or automatically. |
| SMS control | Application to restart or to connect LTE network by receiving SMS from external device. |
| Proxy connection | Application to hookup TCP UDP packets by working as proxy server. |
| NTP | Application to send time information by working as NTP server in connected network. |
| DDNS | When connecting to the Internet, this app permanently assigns a domain name to a host whose IP address changes frequently, immediately follows the address change, requests updating to DDNS server, and updates the DNS information. |
| Ping checking | Application to check connection availability by sending pings. Also, will report its diagnosis result or automatically reboot based on its result. |
| Positioning system | Application to show current position of this unit. |
| Iopoll | Application to access IO functions prepared on this product |
| modbusio | Application to write machine setting, read machine information via Modbus based on request of iopoll commands. |
| mqttio | Application to transfer as MQTT for information which received on iopoll commands. |
| RESTio | Application to transfer as HTTP for information which received on iopoll commands. |
| RS232 through | Application to convert RS232C and TCP communication |
| RS485 through | Application to convert RS485 and TCP communication |
| Datamanager | Application to collect the data from modbusio and sends the payloads to mqttio or RESTio. |
| Logsd | Application to saves logs generated from each application to the SD card. |
| Setting management | Applications to downloading / uploading parameters for each application. |
| Band | Control connection band for carrier communication. |
| Monitoring | Monitor status of CPTrans itself and save logs and inform alarm. |

## 3.2 Major functions

Major functions on this product are listed as below Table 3.2 Major functions.

**Table 3.2 Major functions (1/ 2)**

| Application | Function | |
|---|---|---|
| System | CLI connection setting | |
| | Web GUI setting | |
| | Device specific information | |
| Router | LAN Settings | |
| | | IP address setting |
| | | DHCP・DNS |
| | | Allocated status of DHCP server |
| | Ethernet Connection | |
| | | Ether port setting |
| | | Ether port status |
| | Wireless LAN connections | |
| | | Basic setting |
| | | Encryption setting |
| | | Access control |
| | | Connection status |
| | WAN Connection | |
| | | Basic setting |
| | | APN setting |
| | | Modem status |
| | Packet Transfer | |
| | | NAT・NAPT・DMZ |
| | | Ping response setting |
| | | Static routing |
| | Security functions | |
| | | Firewall |
| | | Access control |
| Schedule reboot | Activation setting | |
| | Reboot clock setting | |
| | Reboot time setting | |
| | Reboot limitation during APN connection | |
| Firmware update | Manual update | |
| | Auto update | |
| SMS | APN connection & reboot by SMS | |
| | Receiving log by SMS | |
| Proxy server | Proxy function application | |
| NTP | NTP server function | |
| | NTP client function | |
| DDNS | Dynamic Domain Name System client function | |

**Table 3.3 Major functions (2 / 2)**

| Application | Function |
|---|---|
| Ping communication check | Communication checking function |
| | Reboot setting after continuous fail |
| Position information | Map display |
| | Current status |
| Iopoll | Connection setting |
| | Current status |
| Modbusio | Modbus-RTU setting |
| | Modbus-TCP setting |
| | Connected device setting |
| | Current status |
| Mqttio | Resend, Backup setting |
| | Certificate setting |
| | MQTT setting |
| | Current status |
| RESTio | Resend, Backup setting |
| | Certificate setting |
| | REST setting |
| | Current status |
| 232 through | Socket Settings |
| | RS232 Setting |
| | TCP connection settings |
| 485 through | Socket Settings |
| | RS485 Setting |
| | TCP connection settings |
| Datamanager | Modbus Settings |
| | Buffer setting |
| | Trigger setting |
| | Individual data setting |
| | Payload setting |
| Logsd | Save each app log to the SD card. Download |
| | Basic setting |
| Setting management | Saving and Restoring App Settings |
| Monitoring | Log download |
| | Self-diagnosis setting |
| | Fault notification setting |
| | Failsafe setting |
| | General Settings |

### 3.2.1 System application

This application enables to show device specific information or able to set user interface settings.

#### 3.2.1.1 CLI (Management Port) Connection Configuration

This product provides user interface to control this unit by command input using TCP/IP socket. Details of CLI (Administration port) is shown in Table 3.4 CLI Administration port.

**Table 3.4 CLI Administration port**

| # | Item | Specifications |
|---|---|---|
| 1 | Communication I/F | Enable to access from following communication I/F.<br>- WAN<br>- Wireless LAN<br>- LAN(Ethernet) |
| 2 | Protocol | Non-procedure |
| 3 | Number of max session | 1 |
| 4 | Port No. | Available to set within 0 to 65535 |
| 5 | Authentication | Authentication base on password input.<br>Enable to skip authentication function by setting password empty. |
| 6 | Remark | This function is disabled in initial setting |

Following table show setting items via Administration port.

**Table 3.5 CLI connect setting**

| # | Item | Details |
|---|---|---|
| 1 | TCP Connection availability | Enable to connect CLI on this product via console<br>Setting range: Enable/Disable (Check BOX) |
| 2 | Port No. | Port number which this product will open for CLI.<br>Setting range: 0 to 65535<br>Note: Not overlap with port No. which used for packet transfer function |
| 3 | Access password availability | Enable/Disable password setting on CLI access<br>Setting range: Enable/Disable (Check BOX)<br>Note: In case of Disabled, password authentication shall be skipped. |
| 4 | Access password | Access password setting to access on CLI.<br>Format: Alphanumeric<br>Note: Password need to be at least 4 letters or more |

When the wireless network is not connected, CPTrans can connect specified APN by the following connection command from external communication device to CLI port on CPTrans. Table 3.6 Connection & disconnection commands lists the specifications of the connection and disconnection commands to the APN. For more information on CLI commands, please refer to "[CPTrans-MJW_MGW] Command Reference manual".

**Table 3.6 Connection & disconnection commands**

| # | Item | Specifications |
|---|---|---|
| 1 | Connection command | Connect with specific APN.<br>event router connect? *? is APN No. (1 to 5) |
| 2 | Disconnection command | Disconnect with specific APN.<br>event router disconnect? *? is APN No. (1 to 5)<br>Disconnect all APN<br>event router disconnectAll |

3.2.1.2 Web GUI Settings

This product supports Web GUI for controlling this product by Web browser. Web GUI setting details are shown as per below.

**Table 3.7 Specification of Web GUI**

| # | Item | Specifications |
|---|---|---|
| 1 | Communication I/F | Enable to access from following communication I/F.<br>- WAN<br>- Wireless LAN<br>- LAN(Ethernet) |
| 2 | Supporting Web browser | Following Web browser supports this setting<br>#1 Chrome<br>#2 Internet Explorer<br>#3 Firefox<br>*It may not show correctly depending on its software ver. |
| 3 | Port No. | Available to set within 1 to 65535 range |
| 4 | Authentication | - Authentication available by username and password inputs.<br>- Initial password is different depending on its product (Random password is applied when products are manufactured)<br>- Enable to skip authentication by setting username and password as Empty.<br>- Master password is not prepared for its safety |
| 5 | Notes | Enable to set port open/closed setting for connection to WAN. |

Web GUI setting items are shown in Table 3.8 Web GUI setting.

**Table 3.8 Web GUI setting**

| # | Item | Description | Remarks |
|---|---|---|---|
| 1 | Port No. | Port No. setting to be opened for connection of GUI (Web user interface) on this product.<br>Applicable range: 1 to 65535<br>Initial setting: 80 | Do not overlap with port No. which will be used for packet transfer function. |
| 2 | Username | Set username which will be used for Web GUI access.<br>Format: Alphanumeric (Max 32 letters) or empty<br>Initial setting: empty | If both username and password are set empty, authentication shall be skipped. |
| 3 | Password | Set password which will be used for Web GUI access.<br>Format: Alphanumeric (8 to 32letters) or empty<br>Initial setting: empty | If both username and password are set empty, authentication shall be skipped. |
| 4 | HTTP access control | Set whether this unit is allowed to access Web GUI from WAN.<br>Disable: No access control<br>Enable: Access from WAN are not allowed | Strongly recommend setting Enable on this setting. |

3.2.1.3 Device Specific Information Display

Displays device specific information. The display items are shown in Table 3.9 Device specific information.

**Table 3.9 Device specific information**

| # | Item | Description | Remarks |
|---|---|---|---|
| 1 | Product ID | Individual ID applied for each device. | |
| 2 | Project ID | ID to use for firmware version control | |
| 3 | Hardware ID | Individual ID to differentiate each hardware | |
| 4 | Ether MAC address | MAC address for Ethernet port | |
| 5 | Wireless LAN MAC address | MAC address for wireless LAN | |
| 6 | IMSI | IMSI (International Mobile Subscriber Identity) of USIM card. | |
| 7 | ICCID | IC card ID on USIM card. | |
| 8 | MSISDN | MSISDN (Mobile International ISDN Number) of USIM card. | It's displayed as Empty, depending on its used SIM card |
| 9 | IMEI | IMEI (International Mobile Equipment Identity) of USIM card. | |

### 3.2.2 Router application

This application able to make settings or show information of communication function of this product.

#### 3.2.2.1 LAN Settings

Enable to set common function setting for LAN communication.

(1) IP address

Set LAN IP address and subnet mask of this product. Setting items are shown below.

**Table 3.10 IP address setting**

| # | Item | Description | Remarks |
|---|---|---|---|
| 1 | IP address | LAN IP address of this product. | A common parameter for both Ethernet and Wireless LAN |
| 2 | Subnet mask | Subnet mask applied for IP address. | A common parameter for both Ethernet and Wireless LAN |
| 3 | Check overlapping IP address in LAN * | Check whether any overlapping of IP address exist in same LAN, | |

*Gratuitous ARP sending function:

In case this product check IP address overlapping, it will send Gratuitous ARP packets when it link up with Ethernet. In case any IP address overlapping is detected, it will show error on LED prepared on this product.

(2) DHCP・DNS

(a) DHCP server

This product supports DHCP server function which arrange IP address dispensing to DHCP client located in LAN. Two methods are supported for its dispensing, one is Dynamic IP address, and another is Fixed IP address. Details of DHCP server are explained as per below.

**Table 3.11 DHCP Server (Common details not related to IP address dispensing method)**

<table>
<tr><th>#</th><th>Item</th><th>Specifications</th></tr>
<tr><td>1</td><td>Supporting DHCP message</td><td>- DHCPDISCOVER<br>- DHCPREQUEST<br>- DHCPRELEASE<br>- DHCPDECLINE</td></tr>
<tr><td>2</td><td>Dispensing IP address, Noticing method of IP address information</td><td>Inform to DHCP client dispensing IP address, together with below information. Dispensing IP address shall be prepared based on DHCP sequence (DHCPDISCOVER – DHCPACK) which start from DHCP client.
<table>
<tr><th>#</th><th>Information</th><th>Details</th></tr>
<tr><td>1</td><td>IP address</td><td>IP address which applied based on either dispensing on Dynamic IP address or on Fixed IP address.</td></tr>
<tr><td>2</td><td>Primary DNS</td><td>Own IP address (Individual setting is not supported)</td></tr>
<tr><td>3</td><td>Secondary DNS</td><td>Own IP address (Individual setting is not supported)</td></tr>
<tr><td>4</td><td>Lease period of dispensed IP address</td><td>Lease period can be modified. Initial value is 3600second.</td></tr>
</table></td></tr>
<tr><td>3</td><td>Extend leasing period of dispensing IP address</td><td>Extend leasing period to target DHCP client in case receive extension request (DHCPREQUEST) from DHCP client within its leasing period.<br>In case extension request is not received even after leasing period passed, collect assigned IP address which used for this DHCP client and prepared to be reused for dispensing to other DHCP client.</td></tr>
<tr><td>4</td><td>In case assigned IP address was refused from client</td><td>In case refuse message (DHCPDECLINE) received from DHCP client for its assigned IP address, this product will not dispense same IP to the same client for certain period.</td></tr>
<tr><td>5</td><td>Condition of deleting packet</td><td>In case any packets which not following to supportive DHCP message, all packets shall be deleted and removed.</td></tr>
<tr><td>6</td><td>Special notes</td><td>Information of IP address assignment will not be saved on nonvolatile memory. In case this unit restart, IP address information which it assigned shall be all clear out as initial condition.</td></tr>
</table>

(b) DNS

This product run as a DNS server in LAN and supports to contact a DNS server in WAN on behalf of DNS clients in LAN. This product transfers Host name resolution request (DNS query request) to DNS server which located on WAN (When it connects to WAN, it collects IP address of DNS server from target WAN), once receive Host name resolution request from DNS client which located on LAN. After this product receive DNS response from DNS server, it transfers to the target DNS client. To use this function, this product need to set IP address and subnet mask for its LAN.

(c) Setting item

Following are setting items which related to DHCP and DNS function.

**Table 3.12 IP address setting for DHCP and DNS**

| | Item | | Description | Remarks |
|---|---|---|---|---|
| 1 | Enable DHCP server function | | Enable or disable DHCP server function. | |
| 2 | Start IP address | | Set start point of consecutive IP address which will be applied from DHCP server. | |
| 3 | End IP address | | Set end point of consecutive IP address which will be applied from DHCP server. | |
| 4 | Lease time | | Time setting until IP address becomes released after dispensing. | |
| 5 | DNS server mode | | Set DNS server mode.<br>*) This product will do DNS relay<br>*) Specify DNS server address | |
| 6 | DNS server address | | Address of DNS server which will be targeted to transfer request. | |
| 7 | Fixed Assignment | | Setting to dispense fixed IP address from DHCP. | |
| | | MAC Address | Set MAC address which will have Fixed IP address. | |
| | | IP Address | Set what IP address to be fixed and dispensed. | |

(3) Condition of DHCP server

Displays the assignment status of the IP addresses sent from DHCP servers. The display items are shown in Table 3.13 below.

**Table 3.13 DHCP server dispensing condition**

| # | Item | Description | Remarks |
|---|---|---|---|
| 1 | MAC address | Show MAC address which dispense IP address from DHCP server. | |
| 2 | IP address | Show IP address of above. | |
| 3 | Name | Show host name of target which dispense IP address. | |

#### 3.2.2.2 Ethernet communication

This product supports IP packet communication via Ethernet. Following shows Ethernet interface on this product.

**Table 3.14 LAN (Ethernet)**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Number of ports | 2 | — |
| 2 | IP address | 1 / Physical port | — |
| 3 | Communication type | - 10Mbps / Full duplex *2<br>- 10Mbps / Half duplex *1<br>- 100Mbps / Full duplex *2<br>- 100Mbps / Half duplex *1<br>- 10Mbps/100Mbps Auto (Default) | *3 |
| 4 | Auto-MDI / MDI-X | Support | *3 |
| 5 | Auto-Negotiation | Support | *3 |
| 6 | Support protocols | TCP, UDP, ICMP, IP, ARP | ARP only supports Echo request, Echo response, and Time-out message. |
| 7 | Receivable Ethernet packet type | Unicast packet addressed for this product<br>Multicast packet<br>Broadcast packet | — |
| 8 | MTU | 1500bytes (Default) | |

∗1 Back pressure style: In case receive buffer becomes close to its limit, this product will send out Jamming signal to another side to request interrupt on further sending.

∗2 IEEE802.3x style: Interrupt further sending when receive PAUSE frame signal from another side. If PAUSE release frame signal is received, this product will resume its signal sending.

∗3 There are several settings unable to connect (or non-recommendable) depending on this product and another side's communication setting.

Table 3.15 List of Communication availability on Ethernet settings

| CPTrans \ Other side | | 10Mbps | | 100Mbps | | Auto-Negotiation |
|---|---|---|---|---|---|---|
| | | Full Dup. | Half Dup. | Full Dup. | Half Dup. | |
| 10Mbps | Full Dup. | ○ | △ | × | × | ○ |
| | Half Dup. | △ | ○ | × | × | ○ |
| 100Mbps | Full Dup. | × | × | ○ | △ | ○ |
| | Half Dup. | × | × | △ | ○ | ○ |
| Auto-Negotiation | | △ | △ | △ | △ | ○ |

○: Available to communicate
△: Not recommendable (Unstable communication depending on setting)
×: Not able to communicate

(1) Ether port setting

Available to set MTU and Ether port communication speed. Settings are as per below shown.

Table 3.16 Ether port setting

| # | Item | Details | Note |
|---|---|---|---|
| 1 | LAN Communication Speed | Set communication speed.<br>- 10Mbps / Full duplex<br>- 10Mbps / Half duplex<br>- 100Mbps / Full duplex<br>- 100Mbps / Half duplex<br>- auto(10Mbps/100Mbps) | Default setting is auto |
| 2 | Ether Port MTU | Set MTU | Able to set in between of 576 to 1500. |
| 3 | Ether Flow control | Select target to apply flow control.<br>- Not available<br>- Receive | This function is prepared for sending PAUSE frame signal to target port in case buffer memory becomes close to its limit.<br>Flow control function is available at receiving frame only. |

**(2)** Ether port status

Show Ether port setting status and communication status. Status shown are as per below.

**Table 3.17 Ether port status**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | LAN Communication Speed [Mbps] | Show LAN communication speed setting | |
| 2 | duplex | Show duplex status (Full/Half) of Ether port. | |
| 3 | Link detection | Show link detection of Ether port | |
| 4 | Number of receiving byte | Show total receiving bytes on Ether port after this product start up. | |
| 5 | Number of receiving packet | Show total receiving packets on Ether port after this product start up. | |
| 6 | Number of sending byte | Show total sending bytes on Ether port after this product start up. | |
| 7 | Number of sending packet | Show total sending packets on Ether port after this product start up. | |

3.2.2.3 Wireless LAN communication

This product supports wireless LAN communication. Details are shown as per below.

**Table 3.18 Wireless LAN**

<table>
<tr><th>#</th><th colspan="2">Item</th><th>Specifications</th></tr>
<tr><td>1</td><td colspan="2">Communication standard</td><td>Supports the following:
<table>
<tr><th>Standard</th><th>Frequency band</th><th>Bandwidth</th></tr>
<tr><td>IEEE802.11a</td><td>5GHz</td><td>20MHz</td></tr>
<tr><td>IEEE802.11b<br>(Excluding ch14)</td><td>2.4GHz</td><td>20MHz</td></tr>
<tr><td>IEEE802.11g</td><td>2.4GHz</td><td>20MHz</td></tr>
<tr><td>IEEE802.11n</td><td>2.4GHz / 5GHz</td><td>20MHz / 40MHz</td></tr>
<tr><td>IEEE802.11ac</td><td>5GHz</td><td>80MHz</td></tr>
</table>
*CPTrans-MGW supports 2.4GHz only</td></tr>
<tr><td>2</td><td colspan="2">Access point function</td><td>Support</td></tr>
<tr><td>3</td><td colspan="2">AP client feature</td><td>Not supported</td></tr>
<tr><td>4</td><td colspan="2">AP bridging</td><td>Not supported</td></tr>
<tr><td>5</td><td colspan="2">Number of AP clients that can be connected</td><td>Max. 16 units</td></tr>
<tr><td>6</td><td colspan="2">Channel selection</td><td>Automatic</td></tr>
<tr><td>7</td><td colspan="2">Encryption standard</td><td>Supports the following:
<table>
<tr><th>#</th><th>Standard</th><th>Description</th></tr>
<tr><td>1</td><td>WEP</td><td>Wired Equivalent Privacy</td></tr>
<tr><td>2</td><td>WPA-PSK</td><td>WPA-Personal</td></tr>
<tr><td>3</td><td>WPA2-PSK</td><td>WPA2-Personal</td></tr>
</table></td></tr>
<tr><td>8</td><td colspan="2">Encryption scheme</td><td>Supports the following:
<table>
<tr><th>#</th><th>Standard</th><th>Description</th></tr>
<tr><td>1</td><td>TKIP</td><td>Temporal Key Integrity Protocol</td></tr>
<tr><td>2</td><td>CCMP</td><td>AES in Counter mode with CBC-MAC(CCMP-128)</td></tr>
</table>
※If "IEE802.11n" or "IEE802.11ac" is used, please set CCMP.</td></tr>
<tr><td>9</td><td rowspan="2">Other Support Function</td><td>SSID Stealth</td><td>Not output beacon signal to AP client for this product SSID</td></tr>
<tr><td>10</td><td>MAC address filter</td><td>- Enable to limit accessible AP client based on MAC address registration.<br>- Selectable either from Whitelist or Blacklist style.<br>- Max 32 records are available to register for its access control.</td></tr>
<tr><td>11</td><td></td><td>AP isolation</td><td>- Enable to communicate among devices which are connecting to AP.</td></tr>
</table>

(1) Settings on Wireless LAN

Available to set basic settings required for wireless LAN to be used. Details are shown below.

**Table 3.19 Wireless LAN setting**

| # | Item | Description | Remarks |
|---|---|---|---|
| 1 | Enable Wireless LAN | Setting for activate/deactivate WLAN | |
| 2 | Country code | Specify the country where you want to use the WLAN. | |
| 3 | SSID | Setting for SSID on this access point. | |
| 4 | SSID notification | Setting for SSID notification<br>Available setting:<br>・Show SSID<br>・Hide (Stealth mode)<br>・Reply no information (Null) | If Null is selected, user need to identify their connecting SSID in order to connect AP. |
| 5 | Communication mode | Setting for wireless LAN standard to be applied.<br>・ IEEE 802.11b (2.4GHz)<br>・ IEEE 802.11g (2.4GHz)<br>・ IEEE 802.11a (5GHz)<br>・ IEEE 802.11ac (5GHz)<br>・ IEEE 802.11n (2.4GHz, BW=20M)<br>・ IEEE 802.11ac (5GHz, BW=40M) | |
| 6 | Connecting number | Setting to limit maximum connecting number to this AP. | Enable to select from range 1 to 16. |
| 7 | Frequency channel | Setting to select which frequency channel to be used. | |

[Caution]

・The default setting of this function is "Disabled". When using this function, change it to "Enable" and change the passphrase from the initial value before use.

・Do not specify the same SSID for two or more wireless LAN access points including this product. Communication may not be established.

・This product is not guaranteed to be able to communicate with all wireless LAN units (regardless of the applicable standards). Depending on the wireless LAN units, communication may not work properly or communication speed may not be obtained sufficiently. Please limit the number of wireless LAN devices for system and be sure to perform thorough beforehand.

・If this function is enable on CPTrans-MGW, please enter the country code for using country.

(2) Encryption setting

This product supports encryption on the wireless LAN. The setting items are as shown in Table 3.20 **Wireless LAN encryption setting** below.

**Table 3.20 Wireless LAN encryption setting**

| # | Item | Description | Note |
|---|---|---|---|
| 1 | Encryption key standard | Setting for encryption key standard<br>- WEP<br>- WPA-PSK<br>- WPA2-PSK<br>WEP is not recommended. WPA2-PSK is recommended to be used as long as it can be applicable. | |
| 2 | Encryption style | Setting for encryption style<br>・TKIP<br>・CCMP/AES-CBC-MAC-128<br><br>If communication mode is either "IEEE802.11n" or "IEEE802.11ac", please set "CCMP/AES-CBC-MAC-128" for encryption style. | |
| 3 | Password setting | Setting for password connecting to wireless LAN.<br>Enable to support max 127 letters. | |

(3) Access control

Client's access to this product can be restricted by access control function. The setting items are shown in **Table 3.21 Access control setting on wireless LAN** below.

**Table 3.21 Access control setting on wireless LAN**

| # | Item | Description | Remarks |
|---|---|---|---|
| 1 | Isolation mode | Setting for isolation mode to be activated / deactivated.<br>(*Isolation mode: If activated, AP will not allow to access connected units which is located in same LAN) | |
| 2 | MAC address filter | Setting to activate / deactivate MAC address filtering. | |
| 3 | MAC filter style | Setting to select MAC address filtering style<br>- Blacklist style<br>(Block access from #4)<br>- Whitelist style<br>(Allow access only from #4) | |
| 4 | Target MAC address | Setting for MAC address which is used for MAC filter | |

(4) Connection Status

Available to show channel information and connection status of WLAN. Details are shown in **Table 3.22 Connection status of wireless LAN** below.

**Table 3.22 Connection status of wireless LAN**

| # | Item | Description | Remarks |
|---|---|---|---|
| 1 | Channel No. | Show channel number of using wireless LAN | |
| 2 | Frequency Band [MHz] | Show frequency band used for wireless LAN. | |
| 3 | Receiving Bytes | Show total receiving bytes on WLAN after this product start up. | |
| 4 | Receiving Packets | Show total receiving packets on WLAN after this product start up. | |
| 5 | Sending Bytes | Show total sending bytes on WLAN after this product start up. | |
| 6 | Sending Packets | Show total sending packets on WLAN after this product start up. | |

#### 3.2.2.4 WAN communication

This product supports IP packet communication via LTE network.

(1) Basic setting on WAN communication (LTE network)

Available for basic setting on WAN communication (LTE network). Details are shown in Table 3.23 **Setting on WAN communication (LTE network)** below.

**Table 3.23 Setting on WAN communication (LTE network)**

| # | Item | Description | Remarks |
|---|---|---|---|
| 1 | APN mode | Single APM mode:<br>Connect to only single APN.<br>Multi APN mode:<br>Enable to connect multi-APN at the same time (Max 5) | This product can register max 5APN for connection to WAN.<br>Multi APN mode is available for network carrier which support this function. |
| 2 | Connection fail reboot | Auto reboot setting when access to WAN continuously fail.<br>Disable: This product will not reboot<br>Enable: In case connection failed more than Reboot setting, this product will automatically reboot. | |
| 3 | Reboot setting | Setting for auto reboot when WAN connection fail. (5 to 20) | Counter will reset when connected to APN. |

(2) APN setting

Allows you to configure settings for connection to and disconnection from the APN. The setting items are shown in Table 3.24 **APN setting** below.

**Table 3.24 APN setting**

| # | Item | Description | Remarks |
|---|---|---|---|
| 1 | APN name | Input connecting APN name | |
| 2 | Username | Input username for APN connection | |
| 3 | Password | Input password for APN connection | |
| 4 | Authentication method | Select authentication method for APN connection | PAP・CHAP・AUTO can be selectable |
| 5 | Overwrite Netmask | Overwrite net mask when receive information during APN connection | |
| 6 | Overwrite value | Overwrite value of netmask | |
| 7 | WAN network address | Input WAN side network address | For option use. Able to connect w/o this setting. |

| | | | |
|---|---|---|---|
| 8 | WAN netmask | Input WAN side net mask | For option use. Able to connect w/o this setting |
| 9 | Alive monitoring setting | Described in following pages | |
| 10 | Auto connection setting | Described in following pages | |
| 11 | Auto disconnect setting | Described in following pages | |

(3) Alive monitoring

This product supports alive monitoring function for WAN network (LTE network).

As a function to improve the mismatch in the connectivity with the base station, a ping is periodically issued to the specified destination for each APN, and the APN connection is disconnected starting from the "ping failed".

Table 3.25 **Alive monitoring setting** below lists the setting items related to alive monitoring.

**Table 3.25 Alive monitoring setting**

| # | Item | Specifications |
|---|---|---|
| 1 | Alive monitoring setting (n) | Ping sending setting to monitor WAN network connection availability.<br>0：Do not send PING signal<br>1：Send PING signal to gateway address<br>2：Send PING signal to primary DNS server<br>3：Send PING signal to assigned address |
| 2 | Alive monitoring address (n) | Set IP address as destination of network connection checking. |
| 3 | Alive monitoring numbers (n) | Set how many times to check network connection availability to target WAN. (Available range: 1 to 10 times) |
| 4 | Alive monitoring during connection (n) | Setting for enable / disable alive monitoring after connected to APN.<br>Disable: Not apply alive monitoring<br>Enable: Apply alive monitoring |
| 5 | Alive monitoring checking period (n) | Setting for checking period of alive monitoring.<br>Setting range: 1 to 60min |

* n means APN No. 1 to 5. The above sets exist in APN units.

(4) Auto connection setting

This product can set auto connecting condition depending on below conditions listed.

**Table 3.26 Auto connection setting**

| # | Auto connect timing | Condition details | Note |
|---|---|---|---|
| 1 | Activation | Automatically try to connect to LTE network when this this product start to activate. | |
| 2 | During idling | Automatically try to connect to LTE network when status move to idle condition (disconnected from LTE network). | |
| 3 | DNS Request | Automatically try to connect to LTE network when DNS request receive from device connected on LAN. | |
| 4 | NTP Request | Automatically try to connect to LTE network when NTP request receive from device connected on LAN. | |
| 5 | Pattern match | Automatically try to connect to LTE network when this product receives packet signal which match with registered details. | Details show on appendix sheet |
| 6 | Command from CLI (Admin port) | Try to connect to LTE network when this product is not connected on wireless network and receiving command from CLI (Admin port). | Refer system application details also |
| 7 | SMS receiving | Automatically try to connect to LTE network when receive any SMS. | |

This product will connect to LTE network based on following pattern match setting.

**Table 3.27 Pattern match setting**

<table>
<tr><th>#</th><th>Item</th><th>Description</th></tr>
<tr><td>1</td><td>Auto connection via pattern match (n)</td><td>Setting whether to enable or deactivate pattern match connection.<br>Deactivate: Do not connect on pattern match<br>Activate: Connect if pattern match condition detected</td></tr>
<tr><td>2</td><td>Pattern match rule (n)<br>Max 32 tables</td><td>Pattern conditions can be set on each APN (n) as per listed below.
<table>
<tr><th>#</th><th>Item</th><th>Details</th></tr>
<tr><td>1</td><td>Protocol</td><td>Referring protocol for pattern match.<br>0: ANY<br>1: TCP<br>2: UDP<br>3: ICMP</td></tr>
<tr><td>2</td><td>LAN IP range<br>(Source IP)</td><td>Set LAN IP address.</td></tr>
<tr><td>3</td><td>LAN port<br>(Source Port)</td><td>Set LAN port No.</td></tr>
<tr><td>4</td><td>WAN IP range<br>(Destination IP)</td><td>Set WAN IP address.</td></tr>
<tr><td>5</td><td>WAN port<br>(Destination Port)</td><td>Set WAN port No.</td></tr>
</table>
*: This function will have different handling on ICMP packet, depending on its setting condition to each port No.<br>1）If condition applied<br>ICMP packet will not be condition of auto connection<br>2）If condition not applied (Start= 0, End=0)<br>ICMP packet will be condition of auto connection<br>3）If condition not applied (Start= 0, End= 65535)<br>ICMP packet will not be condition of auto connection</td></tr>
</table>

※The evaluation order of the table is in the lower order.

※ n means APN No. 1 to 5. The above sets exist in APN units.
This function also tries to connect when a pattern-matched packet is received when all APNs are disconnected and reconnection has not been retried. Each APN attempts to connect up to three times. Note that internal processing is performed at 1-second intervals, and those that occur within this 1-second interval are considered to be simultaneous.

(5) Auto disconnection setting

This product can automatically disconnect from target APN on following settings.

Table 3.28 Auto disconnection setting

| # | Disconnect timing | Condition details | Note |
|---|---|---|---|
| 1 | Packet monitoring | Check sending or receiving (or both) packet during wireless connection and will automatically disconnect if certain time no transmission detected. | Enable to set each pattern |
| 2 | WLAN alive monitoring | Automatically disconnect from target APN if alive monitoring is active and no response for its set checking values. | Refer to alive monitoring settings also |
| 3 | Elapsed time setting | Automatically disconnect whenever elapsed time reach to its setting. | Details shown on appendix sheet |
| 4 | Scheduled time setting | Automatically disconnect whenever scheduled time arrive during its connecting. | Disconnect schedule is different depending on product ID.<br>(To avoid heavy load on APN by disconnect ➔ reconnect many units at same timing) |
| 5 | Command from CLI (Admin port) | Disconnect from LTE network by sending command from CLI (Admin port). | Refer to chapter 3.2.1 “system application” |
| 6 | No network service | Automatically disconnect whenever signal strength of antenna is detected to be zero. | Reconnect based on connection timing when signal resume.<br>(Always active) |
| 7 | Force disconnection | Disconnected from network side automatically. | Depending on network service provider setting. |

This product support automatic disconnection from target APN after certain elapsed time passed on its connection. Following shows its related settings.

Table 3.29 Auto disconnection on elapsed time

| # | Item | Specifications |
|---|---|---|
| 1 | Setting condition for elapsed time disconnection (n) | Setting whether to automatically disconnect from target APN after certain elapsed time passed on its connection.<br>0：Not disconnect<br>1：Automatically disconnect and re-connect<br>2：Automatically disconnect |
| 2 | Elapsed time setting (n) | Setting of target elapsed time.<br>Setting range: 0 to 60min |

∗ (n) shows number of APN (1 to 5). This product can set individual setting on each APN.

(6) Modem condition

This product can monitor modem condition. Following items show related monitoring details.

**Table 3.30 Monitoring modem information**

| # | Item | Details |
|---|---|---|
| 1 | mobile country code | Show mobile country code of network provider |
| 2 | mobile network code | Show mobile network code of network provider |
| 3 | location area code | Show location area code of connected base station |
| 4 | cell ID | Show cell ID of connected base station |
| 5 | earfcn | Show frequency band of connection |
| 6 | Tracking area code | Show tracking area code of its connection |
| 7 | Reference signal received power(rsrp) | Show rsrp information |
| 8 | Reference signal received quality(rsrq) | Show rsrq information |
| 9 | Received signal strength indication(rssi) | Show rssi information |
| 10 | Signal−to−Interference plus Noise power Ratio(sinr) | Show sinr information |
| 11 | Select RX level | Show receiving strength of radio signal |
| 12 | operator | Show information of network provider |
| 13 | accessTechnology | Show type of LTE band (FDD, TDD etc.) |
| 14 | bandName | Show name of band which is connected |

3.2.2.5 Packet forwarding

This product support following methods for packet transferring.

Table 3.31 Packet transferring method

| # | Method | Overview |
|---|---|---|
| 1 | Static NAT<br>(IP address translation) | A permanent mapping of WAN IP address to a LAN IP address.<br>Packets are converted between WAN IP and LAN IP by this product. |
| 2 | NAT<br>(Network address translation as virtual server: one on one) | Open applicable protocol + port number to WAN, and transfer received IP packets to addressed IP and port No. on LAN, which converted by this product. |
| 3 | NAT<br>(Network address translation as virtual server: range) | Open applicable protocol + a range of port number to WAN, and transfer received IP packets to addressed IP on LAN, which converted by this product. |
| 4 | NAPT (masquerade) | Transfer IP packets received from LAN, which address to WAN, by translating IP address and port No. |
| 5 | DMZ | Transfer special IP packets (only applicable for limited transferring method) received from WAN, to addressed LAN destination by translating IP address and port No. |
| 6 | Ping response setting | This setting can control / drop or transfer to LAN ping echo received from WAN. |
| 7 | Static routing | Packets can be sent to other network segment though gateway in LAN by static routing table. |

* Priority of Packet transfer rule is from #1 to #7

**(1) NAT (Virtual Server)**

NAT will transfer packet by translating address IP & Port No. to applicable LAN IP and Port No. so that this product can work as virtual receiving server from designated WAN IP address and Port No. NAT details are shown below.

Table 3.32 Specification of NAT (Virtual server)

| # | Item | Specifications |
|---|---|---|
| 1 | Supporting protocol | TCP, UDP |
| 2 | Registerable records | Max 32 records |
| 3 | Available session number | Max 1 session per record |
| 4 | Limitation | Not supporting protocols which required to change payload information (except FTP) |

Following will be NAT (virtual server) settings.

Table 3.33 NAT (virtual server) setting

| # | Setting item | | Specifications |
|---|---|---|---|
| 1 | NAT enable | | Setting to activate / deactivate this function<br>No Check mark: Deactivate this function<br>With Check mark: Activate this function |
| 2 | NAT (Virtual Server) Rules | | Sets conversion rules for this function. |
| 2-1 | | Protocol | TCP/UDP |
| 2-2 | | WAN side IP | TCP / UDP |
| 2-3 | | WAN port | Forwarding IP address which is opened to WAN. |
| 2-4 | | LAN side IP | Forwarding port No. which is opened to WAN. |
| 2-5 | | LAN port | LAN IP address which is transferring address |

Following will be expected operation of NAT (Virtual server).

① Open forwarding port to WAN.

② Device located on WAN will send transferrable packets by setting [Destination IP address = WAN IP address of this product], and [Destination port No. = Forwarding port No.]

③ This product will transfer received packets to destination device located on LAN, based on setting of LAN IP and LAN port.

NAT will transfer packets only when WAN side will access to LAN side.

Packet translation details shall be as per below.

Table 3.34 NAT (Virtual server: one on one) translation details (WAN ➔ LAN)

| # | Conversion Items | Conversion Procedure |
|---|---|---|
| 1 | Source of transmission IP | Do not convert |
| 2 | Source port | Do not convert |
| 3 | Destination IP | Convert to "IP address of LAN side device" set by "LAN side IP" |
| 4 | Destination port number | Convert to "Port No. of LAN side device" set in "LAN side port" |

**(2) NAT (Virtual Server: Range)**

NAT (Virtual Server: Range) transfers packet by translating address IP & range of Port number to applicable LAN IP so that this product can work as virtual receiving server from designated WAN IP address and Port No. NAT details are shown below.

Table 3.35 NAT (Virtual server: range)

| # | Item | Specifications |
|---|---|---|
| 1 | Supporting protocol | TCP, UDP |
| 2 | Registerable records | Max 32 records |
| 3 | Available session number | Max 1 session per record |
| 4 | Limitation | Not supporting protocols which required to change payload information (except FTP) |

The setting items of NAT (Virtual Server: Range) are shown below.

Table 3.36 Setting items of NAT (Virtual server: range)

| # | Settings | Details |
|---|---|---|
| 1 | NAT enable | Setting to activate / deactivate this function<br>No Check mark: Deactivate this function<br>With Check mark: Activate this function |
| 2 | Supporting Protocol | TCP / UDP |
| 3 | WAN IP range | Forwarding IP address which will be opened to WAN. |
| 4 | WAN Port range | Forwarding port No. which will be opened to WAN. Port No. on LAN which will be transferred from WAN is used the port No. received at port number of WAN. |
| 5 | LAN IP | LAN IP address which will be transferring address |

※The evaluation order of the table is in the younger order.

Following will be expected operation of NAT (Virtual server: range).

① Open forwarding port to WAN.

② Device located on WAN will send transferrable packets by setting [Destination IP address = WAN IP address of this product], and [Destination port No. = Forwarding port No.]

③ This product will transfer received packets to destination device located on LAN, based on setting of LAN IP and LAN port.

NAT will transfer packets only when WAN side will access to LAN side.

Packet translation details shall be as per below.

Table 3.37 NAT (Virtual server: one on one) translation details (WAN -> LAN)

| # | Translating item | Translating details |
|---|---|---|
| 1 | Source IP | No translation |
| 2 | Source port No. | No translation |
| 3 | Destination IP | Translate to LAN IP based on this product setting |
| 4 | Destination port No. | No translation |

**(3) Static NAT (IP Address Translation)**

Static NAT provides a permanent mapping of WAN IP address to a LAN IP address. Packets are converted between WAN IP and LAN IP by this product.

Table 3.38 Specification of NAT (IP address translation server)

| # | Item | Specifications |
|---|---|---|
| 1 | Supported Protocols | TCP、UDP |
| 2 | Available number of conversion rules | Maximum 32 |
| 3 | Available session number | Max 1 session per record |
| 4 | Limitation | Not supporting protocols which required to change payload information (except FTP) |

The static NAT (static IP) setting items are shown below.

Table 3.39 NAT (IP address translation server) setting

| # | Setting item | | Description |
|---|---|---|---|
| 1 | Static NAT enable | | Activate / deactivate this function |
| 2 | Conversion rule | | |
| 2-1 | | WAN IP | WAN IP address which is used for Static NAT. |
| 2-2 | | LAN IP | IP address for transferring destination on LAN. |

Following will be expected operation of Static NAT.

① Once this product receives packets from WAN, which its source IP match with WAN IP registration of Static NAT setting, this product will translate destination IP as LAN IP which registered 1:1 on NAT rule.

② Once this product receives packets from LAN, which its destination IP match with WAN IP registration of Static NAT setting, this product will translate source IP as WAN IP address of this product.

When Static NAT activate, this product translates from WAN to LAN destination IP address as per below. (Expected operation of above ①)

Table 3.40 NAT translation details (from WAN to LAN)

| # | Translating item | Translating details |
|---|---|---|
| 1 | Source IP | No translation |
| 2 | Source port No. | No translation |
| 3 | Destination IP | Translate to LAN IP based on this product setting |
| 4 | Destination port No. | No translation |

When Static NAT activate, this product translates LAN ➔ WAN source IP address as per below. (Expected operation of above ②)

Table 3.41 Static NAT operation (from LAN to WAN)

| # | Translating item | Translating details |
|---|---|---|
| 1 | Source IP | WAN IP address of this product |
| 2 | Source Port No. | No translation |
| 3 | Destination IP | No translation |
| 4 | Destination Port No. | No translation |

**(4) NAPT (masquerade)**

NAPT will translate source IP address of received packets, which sent from device located in LAN, as IP address of this product (= CP Trans) to enable WAN communication from LAN devices. In this process, NAPT also randomly change source Port No. Details of NAPT IP masquerade are shown below.

Table 3.42 NAT (masquerade)

| # | Item | Specifications |
|---|---|---|
| 1 | Supported Protocols | TCP、UDP、ICMP |
| 2 | Available number of conversion rules | Maximum 32 |
| 3 | Available session number | Max 1 session per record |
| 4 | Limitation | Not supporting protocols which required to change payload information (except FTP) |

NAPT settings are shown below.

Table 3.43 NAPT settings

| # | Settings | Details |
|---|---|---|
| 1 | NAPT enable | Setting to activate / deactivate this function |

Following will be expected operation of NAPT.

① Device located on LAN will send packet as [Destination IP = IP address of destination device located on WAN] & [Destination port No. = Listening port No of destination device located on WAN].

② This product will transfer packets received from LAN device and translate its setting to send out destination device located on WAN.

③ Once packets received as a response of above WAN device, this product will take opposite direction of ② and return back its response to original source located on LAN.

This product will translate from LAN to WAN packets (expected operation ②) on following methods

Table 3.44 NAPT translation (from LAN to WAN)

| # | Translating item | Translating details |
|---|---|---|
| 1 | Source IP | WAN IP address of this product |
| 2 | Source Port No. | Randomly selected. Able to apply fixed port No. |
| 3 | Destination IP | No translation |
| 4 | Destination Port No. | No translation |

This product will translate from WAN to LAN packet response (expected operation ③) on following methods.

Table 3.45 NAPT translation (from WAN to LAN)

| # | Translating item | Translating details |
|---|---|---|
| 1 | Source IP | No translation |
| 2 | Source Port No. | No translation |
| 3 | Destination IP | IP address of original sending device located on LAN |
| 4 | Destination Port No. | Port No. or original sending device located on LAN |

**(5) DMZ**

DMZ enable to split LAN into two areas which designed for internal disclose service area and external disclose service area. DMZ details are shown below.

Table 3.46 DMZ

| # | Item | Specification |
|---|---|---|
| 1 | Supporting Protocol | TCP, UDP, ICMP |
| 2 | Limitation | During DMZ is activated, access cannot be made from WAN side to server area of this product. |

DMZ setting items are shown in below.

Table 3.47 DMZ setting

| # | Settings | Details | Default |
|---|---|---|---|
| 1 | DMZ enable | Setting to activate / deactivate this function | “Deactivate” |
| 2 | DMZ IP address | IP address setting for transferring area of DMZ. | “0.0.0.0” |

Following will be expected operation of DMZ.

① This device translates packets received from WAN and transfer to LAN target device, only if these packets are “Transferrable packets which DMZ is allowed to take care”.

② In case packet respond back from target LAN device (as a result of above① procedure), this product transfers this response to its original source of above①.

If DMZ is active, this product will translate destination IP and send packet to LAN device once receive packet from WAN. (Expected operation ①)

Table 3.48 DMZ translation (Packet receiving)

| # | Translating item | Translating details |
|---|---|---|
| 1 | Source IP | No translation |
| 2 | Source Port No. | No translation |
| 3 | Destination IP | DMZ IP address of Chart48 |
| 4 | Destination Port No. | No translation |

If DMZ is active, this product translates sending packet information and send response back to original sending device which located on WAN. (Expected operation ②)

Table 3.49 DMZ translation (Packet response)

| # | Translating item | Translating details |
|---|---|---|
| 1 | Source IP | WAN IP address of this product |
| 2 | Source Port No. | Source Port No. which receive during operation ② |
| 3 | Destination IP | No translation |
| 4 | Destination Port No. | No translation |

**(6) Ping response setting**

This setting can be set an action on this product when it receives ping echo from WAN. Settings are shown below.

Table 3.50 Ping response setting

| # | Action | Description |
|---|---|---|
| 1 | Ignore ping echo | Drop ping echo received at WAN |
| 2 | This product responds ping echo | CPTrans responds ping echo received at WAN |
| 3 | Transfer ping echo to a device in LAN | Transfer ping echo received at WAN to a LAN device |
| | Destination LAN IP address | LAN IP address which will be transferring address |

**(7) Static routing**

If other gateway device is existing in the LAN, packets can be sent to other network segment through the gateway device by adding static routing table into user's original routing rule.

Table 3.51 Static routing setting

| # | Settings | Details | Default |
|---|---|---|---|
| 1 | Enable | Setting to activate / deactivate this function | "Deactivate" |
| 2 | Destination IP address | LAN IP address which will be transferring address | "0.0.0.0" |
| 3 | Subnet mask | Subnet mask for LAN | "0.0.0.0(/0)" |
| 4 | Gateway | Gateway IP address existing in LAN | "0.0.0.0" |

Example of static routing table is shown below. Based on below setting, a server can communicate to YYYY (IP address is 192.168.1.1) port of the LAN device existing other network segment as shown in Figure 3.1 Example of static routing via accessing XXXX (IP address is X.X.0.60) port at WAN IP of CPTrans.

① Setting in “Static NAT”

| Network address | Subnet mask | Gateway address |
|---|---|---|
| 192.168.0.0 | 255.255.192.0 | 192.168.128.1 |

② Setting in “NAT (Virtual server: one on one) setting

| Protocol | WAN IP range | WAN port range | LAN IP | LAN port |
|---|---|---|---|---|
| TCP | * | XXXX | 192.168.1.1 | YYYY |

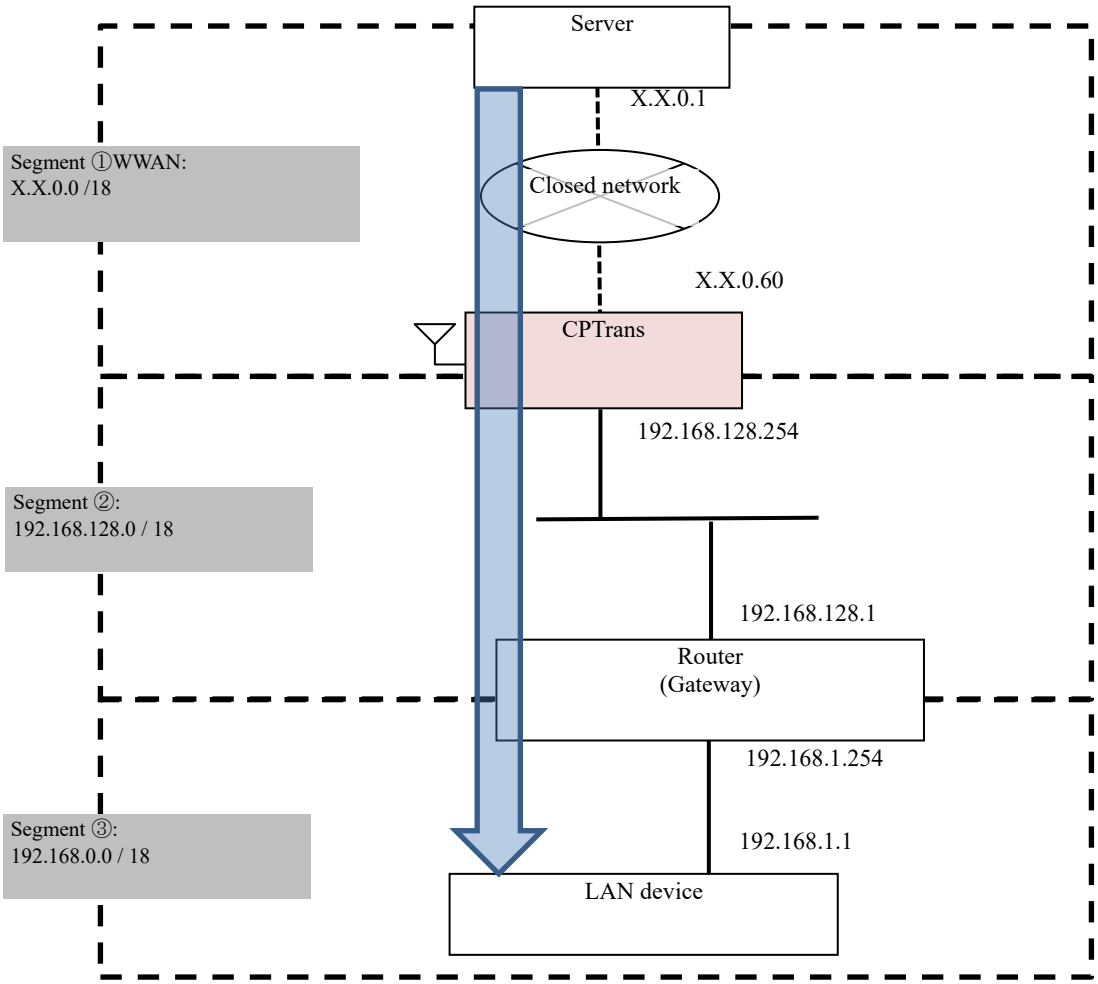



**Figure 3.1 Example of static routing**

3.2.2.6 Security function

This product supports following functions to deploy security functions.

**Table 3.52 Security function**

| # | Function | Details |
|---|---|---|
| 1 | Firewall | Enable to choose either to accept or block receiving packets |
| 2 | Access control | Support protection from malicious attach such as DoS etc. |

(1) Firewall

This product supports two types of firewall functions, “IP packet firewall” which based on protection defining its target IP address, Port No., and Supporting protocols, and “MAC address firewall” which based on protection defining its target MAC address. Firewall settings are shown as per below.

**Table 3.53 Firewall settings**

| # | Settings | Details |
|---|---|---|
| 1 | Firewall activation | Activate / deactivate IP packet firewall.<br>If it’s deactivate, all packets are allowed to be transferred to LAN side. |
| 2 | Firewall style | Operation mode either whitelist or blacklist style.<br>Accept: Whitelist style<br>(Packets which match with conditions are allowed)<br>Reject: Blacklist style<br>(Packets which match with condition are blocked and others are allowed) |
| 3 | Firewall list *(n=1～64)* | Allow which packet either to enter (in case of Accept mode), or to block (in case of Reject mode).<br>Available settings are as per below. |
| 4 | MAC address firewall activation | Setting to activate / deactivate MAC address firewall.<br>If it’s deactivate, all packets are allowed to be transferred to LAN side. |
| 5 | MAC address firewall style | Same as #2 |
| 6 | MAC address firewall list (n=1 to 64) | List up target MAC address which will be handled accept / reject on condition set on #5. |

| # | Item | Details |
|---|---|---|
| 1 | Protocol | Target protocol<br>TCP, UDP, ICMP, ANY is selectable. |
| 2 | LAN IP | LAN IP address range |
| 3 | LAN Port | LAN Port No. range |
| 4 | WAN IP | WAN IP address range |
| 5 | WAN Port | WAN Port No. range |

(2) Access control

This product supports to protect malicious attack from WAN. By using this function, access limitation can be applied on access from WAN to protect server functions operating on this product (Proxy server, Admin web server, Administration console). Default setting is blocking all access from WAN. Any packets which access to unauthorized ports shall be immediately discarded and not respond back SYN NAK or Unreachable packets which enable to notice attacker its existence. Also this product supports protection from malicious attacks, such as DoS attack and Stealth scanning etc. Details of security block settings are shown as per below.

**Table 3.54 Security block setting**

<table>
<tr><th>#</th><th>Settings</th><th>Details</th></tr>
<tr><td>1</td><td>WAN access authorization (n)<br>*(n) = Max 64<br>*Operate as whitelist style</td><td>Set following items
<table>
<tr><th>Item</th><th>Details</th></tr>
<tr><td>Protocol</td><td>Setting for monitoring protocol<br>1：TCP<br>2：UDP</td></tr>
<tr><td>Port No.</td><td>Setting for monitoring port No.</td></tr>
<tr><td>WAN IP</td><td>Setting for WAN IP address monitoring</td></tr>
</table></td></tr>
<tr><td>2</td><td>Protection from DoS on SYN packet</td><td>Set activate / deactivate protection from DoS via SYN packet<br>Deactivate: No protection from DoS attack<br>Activate: Protection applied from DoS attack on SYN packet</td></tr>
<tr><td>3</td><td>Max allowable SYN packet per second</td><td>Set Max limit of allowable SYN packet number per second.<br>Default Max: 20 (Available range: 0 – 2147483647)</td></tr>
<tr><td>4</td><td>Protection from DoS on ICMP packet</td><td>Set activate / deactivate protection from DoS via ICMP packet<br>Deactivate: No protection from DoS attack<br>Activate: Protection applied from DoS attack on ICMP packet</td></tr>
<tr><td>5</td><td>Max allowable ICMP packet per second</td><td>Set Max limit of allowable ICMP packet number per second.<br>Default Max: 20 (Available range: 0 – 2147483647)</td></tr>
<tr><td>6</td><td>Protection from DoS on UDP packet</td><td>Set activate / deactivate protection from DoS via UDP packet<br>Deactivate: No protection from DoS attack<br>Activate: Protection applied from DoS attack on UDP packet</td></tr>
<tr><td>7</td><td>Max allowable UDP packet per second</td><td>Set Max limit of allowable UDP packet number per second.<br>Default Max: 200 (Available range: 0 – 2147483647)</td></tr>
<tr><td>8</td><td>Protection from SYN flood attack</td><td>Set activate / deactivate protection from SYN flood attack.<br>Deactivate: No protection from SYN flood attack<br>Activate: Protect from SYN flood attack</td></tr>
<tr><td>9</td><td>Protection from stealth scan attack</td><td>Set activate / deactivate protection from stealth scan attack<br>Deactivate: No protection from stealth scan attack<br>Activate: Protect from stealth scan attack ※</td></tr>
</table>

* Packets which has possibility of stealth scanning shall be all discard.(Packet starting from SYN+ACK, Packet which all flags are zero including ACK, SYN & FIN are set both 1, SYN and RST are both 1, FIN & RST are both 1, ACK 0 but FIN/PSH/URG flag are holding 1, etc.)

### 3.2.3 Scheduled reboot

This product support function to reboot itself based on setting schedule. Details of scheduled reboot application are shown as per below.

**Table 3.55 Scheduled reboot setting**

| # | Item | Details |
|---|---|---|
| 1 | Reboot timing | Setting assigned as Day of week and Time.<br>Actual reboot timing will not be same of its setting time. To minimize effect on network system, this product will reboot only after random time passed. |
| 2 | Special notes | This product will reboot not depending on WAN connection status (Connect / Disconnect) and also will reboot even WAN-LAN IP packet communication is ongoing or not. |

Scheduled reboot application settings are shown as per below.

**Table 3.56 Schedule/Elapse time reboot setting**

| # | Settings | Details |
|---|---|---|
| 1 | Operation mode | Setting to activate / deactivate this function.<br>0：Deactivate<br>1：Reboot on schedule time<br>2：Reboot on elapse time<br>3：Reboot on schedule time after elapse time passed |
| 2 | Schedule reboot [H] | Setting for schedule reboot hour (24h)<br>Applicable range: 0 to 23 [Hour] |
| 3 | Schedule reboot [M] | Setting for schedule reboot minute.<br>Applicable range: 0 to 59 [Minute] |
| 4 | Random value for reboot | Setting for allowable random range for its actual reboot.<br>Applicable range：10 to 1440 [Minute]<br>Note：Actual reboot will be decided after random second passed from its scheduled time. This setting is to fix max random range. |
| 5 | Time zone [M] | Setting for time zone on reboot schedule.<br>Applicable range: -1440 to 1440 [Minute] |
| 6 | Day of week | Setting for Day or week which not allowed for reboot |
| 7 | Operating time | Setting for allowable operating time until this product will reboot.<br>Applicable range: 1 to 24 [Hour] |
| 8 | Reboot limitation during APN connection | Limit reboot during connection of target APN.<br>Applicable range: APN 1 to 5<br>• In case limitation is activated and connection is made on APN1, this product will not reboot even setting Day of week, hour, operating time arrive. It will immediately reboot once network connection with APN 1 becomes disconnected. |

### 3.2.4 Firmware update

This product has function to download firmware & update to this product by firmware update application. Following methods are supported for this function.

**Table 3.57 Update method**

| # | Item | Details |
|---|---|---|
| 1 | Manual update | Firmware update is manually possible by Web GUI by download update file from connected PC. |
| 2 | Auto update | This product can automatically download firmware file and extract itself, by periodically accessing to Hitachi Industrial Equipment Co. Ltd server and check its latest firmware version. |

(1) Manual Update

Manual update will operate firmware update by providing update file by Web GUI.

Following will be its update process.

① Open [Manual Update] from Update application, select [File select] button.

② Select firmware image file which administrator would like to download to this product.

③ Selected firmware image file shall be download to this product.

④ Once download complete, image file will be activated, and firmware shall be renewed.

⑤ After firmware becomes updated, this product will automatically reboot.

CPTrans doesn't reboot automatically after manual update. It is necessary to reboot CPTrans manually in order to apply the new firmware.

(2) Auto update

Auto update will periodically check whether any firmware update available and will download whenever found any updates. Schedule can be set for its periodical checking. Following shows details of auto update schedules settings.

**Table 3.58 Auto update schedule setting**

| # | Setting item | Description |
|---|---|---|
| 1 | Enable automatic installation | Enables or disables the automatic installation.<br>Disabled: Do not perform automatic installation. (Not recommended)<br>Enabled: Do not perform automatic installation. |

| # | Setting item | Description |
|---|---|---|
| 2 | Automatically reboots after patching. | Specifies whether to automatically reboot or not after the update.<br>Disabled: After the firmware is installed, it is not updated and is updated when the unit is restarted.<br>Enabled: After the firmware is installed, the unit is automatically rebooted and the firmware via<br>is updated. |
| 3 | APN number to be connected | Specifies the APN of the WAN connection that triggers a session with the server.<br>Options:<br>・Arbitrary (any APN)<br>・APN1～5 |

[Caution] : Since CPTrans-MJW is operated and maintained remotely, the auto update function is enabled by default. Once a day for random time, but for access to the server, the packet is sent. For downloading communication charges and update files, the customer shall be responsible for the communication charge. Please note.

Auto-update defaults to "Disabled" in CPTrans-MGW. Set to "Enable" according to your environment.

This product can monitor download status during its auto update. Monitor details are as per below.

**Table 3.59 Download status**

| # | Item | Description | Remarks |
|---|---|---|---|
| 1 | Elapse time [Second] | Elapse time after last auto update. | |
| 2 | Left time [Second] | Left time for next automatic update | |
| 3 | Download time | The elapsed time since the last automatic update. | |
| 4 | Result | Displays the results of the last automatic update.<br>Display contents:<br>0: No execution<br>1: No schedule<br>2: Running<br>11: Success (no data)<br>12: Success (with data)<br>21: Interruption<br>22: Download failed<br>23: Deployment failure<br>24: Busy<br>25: Failure without WAN connection | |
| 5 | Data size | Displays the downloaded data size. | |
| 6 | CRC | Displayed when a CRC (Cyclic Redundancy Code) error occurs during firmware updating. | |
| 7 | Error code | If the status is invalid, an error code is displayed. | |

### 3.2.5 SMS control

This product support to connect APN or reboot itself by setting action rule on receiving SMS from external device. Following are details of action rules which can be set.

**Table 3.60 SMS control**

| # | Item | Details |
|---|---|---|
| 1 | Action rule | Set basic action rule when receiving SMS.<br>0: No action<br>1: Execute action when same text string received<br>2: Execute action when certain text string included |
| 2 | Text string | Set text string which will be key to execute its action. |
| 3 | Action setting | Set action when it matches with above 1 & 2 rules.<br>0: No action<br>1: Connect to APN1<br>2: Connect to APN2<br>3: Connect to APN3<br>4: Connect to APN4<br>5: Connect to APN5<br>101: Reboot this product |

This product will show SMS receiving logs. Monitoring details are shown below.

**Table 3.61 SMS receiving log**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Receive time (UTC) | Show SMS receiving time as UTC zone | |
| 2 | Source information | Show information of SMS source | |
| 3 | Receive text | Show text string of receive SMS. | |

### 3.2.6 Proxy

This product will support to relay receiving packets as proxy server. Function and its setting rule are shown as per below.

**Table 3.62 Proxy setting**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Enable Proxy | Set proxy application to be enabled or disabled. | |
| 2 | Proxy rule | Set communication rule when to relay packets as proxy. | Refer appendix |

**Table 3.63 Proxy rule setting**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Protocol | Set protocol, which proxy shall be activated. | |
| 2 | Port No. | Set Port No., which proxy shall be activated. | |
| 3 | Destination IP | Set destination IP, which proxy shall be activated. | |
| 4 | Destination port No. | Set destination port No., which proxy shall be activated. | |

[Caution]

If this application is working for communication from WAN devices to LAN deices, packet transferring function on router application doesn’t work.

### 3.2.7 Ping checker

Ping checker application periodically sends a ping command to external devices for monitoring whether a communication with the external devices is working or not. Depends on the result of ping communication, this product reboot itself.

Basic settings of Ping checker application are shown below.

**Table 3.64 Basic setting for Ping checker**

| # | Item | Description | Note |
|---|---|---|---|
| 1 | Enable ping check | Enables or disables this application. | |
| 2 | Ping rules | specify rules for ping communication | See Appendix |

This application works according to the rule from ping rules. Items for ping rule are shown.

**Table 3.65 Ping rule setting**

| # | Item | Description | Note |
|---|---|---|---|
| 1 | dest. IP | Destination IP address of Ping command | |
| 2 | repeat | Number of ping command sent to the destination. | |
| 3 | interval [min] | Interval for ping command. | |
| 4 | continuous failure threshold | Threshold count for consecutive failure of ping command. If #5 is enabled, this product start reboot itself after exceeding this value. | Default value :5<br>Minimum value :1 |
| 5 | reboot | Enables the reboot function when the number of consecutive failures exceeds the threshold. | |

This application displays the communication status for ping command. Each status is shown below.

**Table 3.66 Status of ping checker**

| # | Item | Description | Note |
|---|---|---|---|
| 1 | dest. IP | Destination IP address of Ping command. | |
| 2 | last failure count | Last number of consecutive failures. | |
| 3 | last success ratio | Previous success rate. | |
| 4 | min [ms] | The smallest RTT* in the previous ping. | |
| 5 | avg [ms] | RTTs of the mean in the last ping. | |
| 6 | max [ms] | The highest RTTs in the previous ping. | |
| 7 | mdev [ms] | Deviation of the RTTs in the last ping. | |

※RTT= Round Trip Time (ping measured round-trip delay between destination IPs)

### 3.2.8 Location application

This product supports the function to acquire position information.

This function collects internal GNSS information and show its location map.

Details of this function will be shown as per below.

**Table 3.67 Location information**

| # | Item | Description | Remarks |
|---|---|---|---|
| 1 | Latitude | Latitude [degree] | In case unable to receive GNSS signal, all values will be shown as zero. |
| 2 | Longitude | Longitude [degree] | |
| 3 | Altitude | Altitude [m] | |
| 4 | Height | Geoid height [m] | |
| 5 | Hdop | Horizontal Dilution of Precision | |
| 6 | Geohash | GeoHash | Shown as 12 digits.<br>In case unable to receive GNSS signal, empty text is shown. |
| 7 | LastLatitude | Displays the last latitude acquired. | |
| 8 | LastLongitude | Displays the last longitude acquired. | |
| 9 | LastAltitude | Displays the last altitude acquired. | |
| 10 | LastHeight | Displays the last geoid height acquired. | |
| 11 | LastHdop | Displays the last Horizontal Dilution of Precision acquired. | |
| 12 | LastGeohash | Displays the last geoHash acquired. | Shown as 12 digits.<br>In case unable to receive GNSS signal, empty text is shown. |
| 13 | Sentence | This displays the sentences of the acquired GNSS. | |

### 3.2.9 NTP application

This product supports the function of distributing the time from this product to connected devices through NTP applications.

By enabling this function, the time is delivered from this product in response to the time request from the connected device.

Basic setting for this application is shown below.

**Table 3.68 Basic setting for NTP application**

| # | Item | Description | Note |
|---|---|---|---|
| 1 | Synchronization type | Method of time synchronization. | |
| 2 | Time offset during WAN time synchronization [sec] | Offset time during WAN time for synchronization. | Not supported |
| 3 | Start the NTP server on this device | Enable to work this product as NTP server. | |
| 4 | Host name of destination NTP server | Host name for the NTP server. | |

Source of time information is selectable either NTP or WAN (base station). In addition, priority of source of time information is selectable. Items for synchronization type are shown below.

**Table 3.69 Synchronization type**

| # | Item | Description | Note |
|---|---|---|---|
| 1 | Synchronize to WAN-time only once | Time synchronization to WAN is taken only once when LTE connection is established. | Default setting |
| 2 | Periodically synchronize to WAN-time | Time synchronization to WAN is taken periodically when LTE connection is established. | |
| 3 | Synchronize to NTP | Time synchronization to an external NTP server is taken periodically. | |
| 4 | Synchronize to NTP and WAN (NTP priority) | Time synchronization is taken to either WAN or external NTP server. A priority of the external NTP server for time synchronization is higher than WAN. | |
| 5 | Synchronize to NTP and WNA (WAN priority) | Time synchronization is taken to either WAN or external NTP server. A priority of WAN for time synchronization is higher than the external NTP server. | |

[Caution]

- The clock time of this product is obtained from the connected LTE base station or the external NTP server. If LTE is not connected, an incorrect clock time value is stored in this product.
- Synchronized time depends on a time-zone setting in system application.
- There may be deviations depending on the connected carrier and network.

### 3.2.10 DDNS generic applications

DDNS (Dynamic Domain Name System) generic application allows external devices connected to WAN network to access this product. By setting fixed domain name on this product, the external devices can access to this product even if a variable WAN IP address is set on this product.

The basic setting items of this function are shown below.

**Table 3.70 Basic setting of DDNS application**

| # | Item | Description | Note |
|---|---|---|---|
| 1 | APN number of target | An APN number for DDNS function.<br>non: Disabled<br>1 to 5: APN1 to APN5 | |
| 2 | Select a DDNS service | Specify DDNS service.<br>0: Custom Specification<br>1: ieserver.net<br>2: mydns<br>3: no-ip | "ieserver.net" is not supported. |
| 3 | Account | Account name (username or master ID) for accessing DDNS service. | When DDNS service="Customized" is selected, this value is ignored. |
| 4 | Password | Enter the security code (password) for accessing DDNS service. | When DDNS service="Customized" is selected, this value is ignored. |
| 5 | Hostname of DDNS service | Hostname (or domain name) of the application to be registered with DDNS service. | When DDNS service="Customized" or "mydns" is selected, this value is ignored. |
| 6 | URL | URLs for DDNS servers when customized DDNS service is selected. | Configure the settings according to the specifications of your DDNS service. |

<<Caution for using DDNS service>>

- DDNS services "No-IP" and "mydns" are verified to work with this product. If other DDNS services is used for application, please evaluate it beforehand.
- An account for free DDNS service needs account user to login regularly. Otherwise, the account may be deleted.
- Free DDNS service may suddenly stop without any notification.
- If a refresh request is sent to a DDNS server, it may take few minutes to apply the request on the DDNS server.
- Depending on the software protocol stack on the client side, the previous DNS results may continue to be cached, and the update by DDNS may not be reflected.
- DDNS entry isn’t be deleted even if this product is disconnected from the WAN. The registered IP address may be used by another device for WAN connection. In this case, packets filled with the domain in use forward to the device.

- Some APNs use CGN (Carrier Grade NAT). In this case, the WAN assigns an address for NAT instead of a global IP address. Even if this address is registered in DDNS, it cannot be accessed from other devices.

### 3.2.11 Iopoll application

This product supports to receive & transfer information of its connected device to external device.
Modbus protocol is supported for communication between its connected devices.
MQTT or HTTP (REST) is supported for communication between external devices. (In case other protocol need to be supported, additional application required to be installed. Contact local supplier in case of any additional requirements.)

This function sends request to Modbus application and sends transfer request to MQTT or REST application. Connection setting is made from each protocol application. This function periodically sends requests to each application based on prepared access list on its settings. Setting details of access list are shown as per below.

**Table 3.71 Access list setting**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Destination | Set destination of this application (MQTT or REST). | In case of MQTT: mqtt.[key]<br>In case of REST: rest.[key]<br>※[key] is value which user can define to differentiate among several applications. |
| 2 | Text | Set text information which will be send out | Enable to reuse data which collect by Modbus apps. |
| 3 | Input side timeout [ms] | Set timeout on input side (Collect information from Modbus application).<br>Applicable range: 1-10000ms | |
| 4 | Output side timeout [ms] | Set timeout on output side (Request send out to MQTT or REST).<br>Applicable range: 1-10000ms | |
| 5 | Interval [s] | Set interval time to collect information and send out to other application as text.<br>Applicable range: Same or above 1s | |

This function can reuse data which collect by Modbus application by describing in following methods.
Below shows example of its use.

Description: Using Modbus to get data

**${#modbus. deviceName.[addrType]address[type][length] [*mag]}**

Depending on its connected condition, change description of italic fonts.
Details of each description is shown as per below.

**Table 3.72 Text setting**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | *deviceName* | Set device name of Modbus application. | Refer Modbus application (modbusio) |
| 2 | *addrType* | Combine following letters to define proper address type.<br>C: Coil<br>I: Input register (Default)<br>H: Holding register<br>A: Register address<br>N: Register number<br>S: Force to “Write Single Coil” or “Write Single Register” | C, I, H cannot set several conditions.<br>A, N cannot set several conditions.<br>In case no description on address type, N (Register number) will be applied. |
| 3 | *address* | Set Modbus address based on below.<br>・Numerical text consisted from 0～9<br>・Hexadecimal text (0-9, a-f, A-F) starting from x or X | |
| 4 | *type* | Set data type by combination of following letters.<br>H: Big endian (Upper ➔ Lower byte: Default setting)<br>L: Small endian (Lower ➔ Upper byte)<br>N: Binary coded decimal value (BCD)<br>S: Signed 16bit integer value<br>U: Unsigned 16bit integer value<br>X：Directly output as binary data | H, L cannot set several conditions.<br>S, U, X cannot set several conditions.<br>In case no description on data type, S (Signed 16 bit integer value) will be applied. |
| 5 | *length* | Set register data length to be collected. | In case no description, it will be taken care as 1. |
| 6 | Item | Details | Note |
| 7 | ErrorValue | Specifies the string to be replaced if Modbus application cannot successfully retrieve the data. | The default is an empty string. |

By setting the following in the text part of this function, this product sends the contents that depend on the individual of this product and the contents that change dynamically to the destination application.

**Table 3.73 $ substitute**

| # | Description | Description | Note |
|---|---|---|---|
| 1 | ${DID} | Replaced with the serial number of this product. | |
| 2 | ${ETHMAC} | This is replaced by Ethernet MAC address of this product. | |
| 3 | ${IMSI} | It is replaced with IMSI of the SIMs inserted in the PAT. | This value is read from SIM at startup. This value does not change if SIM is replaced after boot. |
| 4 | ${ICCID} | It is replaced by ICCID of the SIMs inserted into this product. | This value is read from SIM at startup. This value does not change if SIM is replaced after boot. |
| 5 | ${MSISDN} | It is replaced by the SIM phone number inserted into the product. | This value is read from SIM at startup. This value does not change if SIM is replaced after boot. It may not be stored depending on the SIM. |
| 6 | ${IMEI} | It is replaced with IMEI of the appliance. | |
| 7 | $n | It is replaced by a line feed (\n). | |
| 8 | $r | It is replaced with a carriage return (\r). | |
| 9 | $$ | It is replaced by '$'. | |
| 10 | ${date:string} | As described in string, it is replaced with a date/time string. String can be any combination of the following strings:<br>・ L:Use local time for deployment. Use the time zone set for System app. To use, specify at the beginning of string.<br>・ a: Day of Week (Sun-Sat)<br>・ b: Month (Jan-Dec)<br>・ y: Year (Western)<br>・ g: Year (last two digits of the western calendar year)<br>・ m: Month (01-12)<br>・ d: Day (01-31)<br>・ H: Time (00-23)<br>・ M: Minute (00-59)<br>・ S: Second (00-59)<br>・ t: Milliseconds (000-999)<br>・ z (lower case): Zone (+hh:mm) (time zone specified by System app)<br>・ Z (uppercase): Zone (+ hhmm) (System app-specified time zone)<br>・ Strings enclosed in ' ' or "" are output as is. | |
| 11 | ${errorCode} | Replaced with the error code of the last error that occurred. | |
| 12 | ${errorText} | Replaces with the error text of the last error that occurred. | |

Error codes and error text use the following values:

**Table 3.74 Error code and text**

| # | Error code | Error text | Description | Note |
|---|---|---|---|---|
| 1 | 0 | OK | No error | |
| 2 | 1 | ERROR_CONNECTION | Cannot connect to the target app | |
| 3 | 2 | ERROR_NORES | No response from target app | |
| 4 | 3 | ERROR_NOTSUPPORT | The target app does not support the requested communication | |
| 5 | 4 | ERROR_KEY | Key is incorrect | |
| 6 | 5 | ERROR_DATA | Data is incorrect | |
| 7 | 6 | ERROR_NOTFOUND | The result for the key was not returned. | |
| 8 | 7 | ERROR_IOERROR | IO is incorrect. IO setting error, etc. | |
| 9 | 8 | ERROR_DEVICEERR | The access destination device returned an error response. | |
| 10 | 9 | ERROR_TIMEOUT | A timeout occurred after access. | |
| 11 | 10 | ERROR_METATEXT | Configuration text expansion error. Grammar error, etc. | |
| 12 | -1 | ERROR_UNKNOWN | Other errors. | |

Example ①-Sensor reading by Modbus:

In Modbus device dev1, register 1 is temperature (in units of 0.1°C),

Suppose that a sensor is connected so that register 2 returns humidity (in %).

The following information is included in the text section.

```
{"temp":${#modbus.dev1.IA1S*0.1},"hum":${#modbus. dev1.IA2S*0.1}}
```

If the temperature is 23.4°C and the humidity is 56%, the following content is sent to the destination application:

```
{"temp":23.4,"hum":56}
```

Example ②-Example of how to describe various deviceName.[addrType]address[type][length:

Various descriptive examples are shown below. Refer to the description method close to the intended use.

| # | Example of description | Meaning | Note |
|---|---|---|---|
| 1 | Dev1.123 | 16-bit signed integer of Input register at address 123 | |
| 2 | Dev1.x123U | 16-bit unsigned Input register at address 0x123=291 | |
| 3 | Dev1.H123S2 | A 32-bit signed value that acquires Holding register of addresses 123 and 124, with the value of address 123 as the high order and the value of address 124 as the low order. | |
| 4 | Dev1.123LS2 | A 32-bit signed value that acquires Input register of addresses 123 and 124, with the value of address 123 as the low order and the value of address 123 as the high order. | |
| 5 | Dev1.123X16 | Binary type with 16 registers taken from address 123 and ordered by big-endian from the Datamanager register | |
| 6 | Dev1.C1 | Coil value of address 1. Numerical value of 1 if ON and 0 if OFF | |
| 7 | Dev1.C1H4 | A 4-bit value obtained by arranging the coil values of addresses 1, 2, 3, and 4 from the upper level. | |
| 8 | Dev1.C1X8 | Binary value obtained by arranging the coil values of addresses 1, 2, 3, 4, 5, 6, 7, 8 from the upper level | |

This function shows request sending status of access list. Details are show as per below.

**Table 3.75 iopoll status monitor**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Destination | Show destination of this application. | |
| 2 | Success number | Number of requests successfully send to destination app. | |
| 3 | Fail number | Number of requests failed to reach to destination app. | |
| 4 | Value | Text details which sent during last operation. | |
| 5 | Error | Error information which received during last request. | |
| 6 | Elapse time | Elapse time after sending last request [second] | |
| 7 | Response time | Response time required for receiving text during last request. [second] | |
| 8 | Delay time | Delay time occur during last request [second] | In case any requests are operating, delay time will occur during its waiting period. |

### 3.2.12 Modbusio application

This product operates as Modbus master and read/write register values of slave devices.

Modbus settings and showing status are listed as per below.

**Table 3.76 Modbus settings / status**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Modbus-RTU setting | Set Modbus-RTU settings. | |
| 2 | Modbus-TCP setting | Set Modbus-TCP settings. | |
| 3 | Slave device setting | Set slave device details. | |
| 4 | Modbus comm. status | Show Modbus communication status. | |

(1) Modbus-RTU Settings

This product supports Modbus-RTU communication. Modbus-RTU settings are shown as per below.

**Table 3.77 Modbus-RTU setting**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Enable Modbus-RTU | Set enable/disable this function.<br>Box checked: Activated (enable)<br>No checked: Deactivated (disable) | |
| 2 | Port Name | Describe port name which will be used as slave device setting. | |
| 3 | Baud rate | Set baud rate of Modbus-RTU comm.<br>Applicable range: Same or below 1000000 | |
| 4 | Bit size | Set data bit size.<br>7: 7bit<br>8: 8bit | |
| 5 | Parity | Set parity bit setting<br>0: None 1: Even 2: Odd | |
| 6 | Stop bit | Specify the stop bit setting.<br>Options:<br>0: 1 bit<br>1: 1.5 bits<br>2: 2 bits | |
| 7 | Interval [ms] | Set interval time before sending.<br>Applicable range: 1000ms or below | |

(2) Modbus-TCP Settings

This product supports Modbus-TCP communication. Modbus-TCP settings are shown as per below.

**Table 3.78 Modbus-TCP setting**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Enable Modbus-TCP | Set enable/disable this function<br>Box checked: Activated (enable)<br>No checked: Deactivated (disable) | |
| 2 | Port Name | Describe port name which will be used as slave device setting. | |
| 3 | IP address | Set IP address of target TCP slave. | |
| 4 | Port Number | Set port number of target TCP slave.<br>Applicable range: 0-65535 | |
| 5 | Idle Timeout | Sets the time to disconnect TCP when communication is interrupted for a certain period.<br><br>Setting range: 0 to 65535 | |

(3) Slave device setting

This product supports Modbus communication among several devices. To operate several devices to be connected, need slave device setting for each connection.

Setting details are shown as per below.

**Table 3.79 Slave device setting**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Device Name | Set target device name which will be used in iopoll application.<br>Format: 1or more characters | |
| 2 | Port Name | Set port name which set on either Modbus RTU setting or Modbus—TCP setting to differentiate connection on RTU or TCP.<br>Format: 1or more characters | |
| 3 | Device address | Set Modbus slave address to differentiate its connecting slave. | |
| 4 | Time out setting | Set timeout setting for this operation. | |
| 5 | ID | Set the alias for the key name. | |
| 6 | Device name | Set any device-name specified in Iopoll application.<br>Format: 1 or more characters | |

| | | | |
|---|---|---|---|
| 7 | Function | Set the function code.<br><br>Setting range: 0 to 2<br>0: Coil<br>1: Input register<br>2: Holding register | |
| 8 | Register address | Sets the register address. | |
| 9 | Data length | Specify the number of registers to be acquired consecutively.<br><br>Setting range: 1 to 64 | |
| 10 | Order of data | Set the order of data to be read.<br><br>Setting range: 0 to 1<br>0: H-L order<br>1: L-H order | |
| 11 | Data type | Sets the data type.<br><br>Setting range: 0 to 3<br>0: Unsigned<br>1: Signed<br>2: BCD<br>3: Binary | |

(4) Status

This product supports to monitor Modbus communication status.

Monitor statuses are shown as per below.

**Table 3.80 Modbus monitor status**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Device name | Device name of target slave. | |
| 2 | Read Success number | Success number of reading register. | |
| 3 | Read Fail number | Fail number of reading register | |
| 4 | Error code | Error code receive on last read operation | |
| 5 | Elapse time [sec] | Elapse time from last operation [sec] | |
| 6 | Response time [ms] | Response time of last operation [ms] | |
| 7 | Write Success number | Success number of writing register. | |
| 8 | Write Fail number | Fail number of writing register. | |
| 9 | Error code | Error code receive on last write operation. | |

### 3.2.13 Mqttio application

This product supports to upload various data by MQTT protocol.

Related settings and status on MQTT communication are shown as per below.

**Table 3.81 MQTT settings / monitors**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Resend & Backup setting | Set resend and backup settings to be prepared for communication failure and sudden power failure. | |
| 2 | Certificate setting | Certification registration setting required to communicate on MQTTS. | |
| 3 | MQTT setting | Set subscribe topics related to MQTT destination, authentication info, quality of service level, etc. | |
| 4 | MQTT status | Show MQTT communication status. | |

(1) Resend & Backup setting

This product will support resend and backup functions to prepare for communication failure and sudden power failure. Details are shown as per below.

**Table 3.82 Resend & Backup setting (MQTT)**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Retry if communication failure | Specifies whether the retransmission function is enabled or disabled.<br>Setting range:<br>Check ON: Enabled<br>No check: Disabled | |
| 2 | Maximum retries count | Specifies the number of retransmissions when communication fails. | |
| 3 | Retry interval [sec] | Specify the time interval between retransmissions when communication fails. | |
| 4 | Retry when new data is received | Specify whether the retransmission is executed when new data is received or not. | |
| 5 | Maximum size of data buffer for retries | Specify the maximum data size to be saved when communication fails.<br>Setting range: Up to 1000000 | |
| 6 | backup for power lost | Enables or disables the function to save the transmitted data to the backup file in case of power off.<br>Setting range:<br>Check ON: Enabled<br>No check: Disabled | |
| 7 | Backup interval [sec] | Specify the time interval for saving the transmitted data to the backup file in case of power off.<br>Setting range :60～65535 | |

If "Retry if communication failure" is disabled, the data is discarded at communication failure.

If "Retry if communication failure" is enabled, retransmission is performed every specified number of seconds in the retry interval. In addition, data that failed to communicate is stored up to the maximum data size, and when the data size exceeds the maximum data size, data is discarded in order starting from the oldest data.
If "backup for power lost" is enabled, a backup file of the transmitted data is created when communication fails. After creating this backup file, if this product is restarted, it reads the backup file and resumes sending data from the contents of the file.

* Iopoll status increases the number of successes, even if the data to be sent is discarded.
  If the transmitted data is discarded, the number of failures of this application increases.

(2) Certification setting

This product supports encrypt communication function by MQTTS. Certificate settings which required for protocol encryption are shown as per below.

**Table 3.83 Certification setting**

| # | Item | Description | Note |
|---|---|---|---|
| 1 | Enable client certificate validation | Enables or disables the client certificate function that utilizes the client certificate.<br>Setting range:<br>Check ON: Enabled<br>No check: Disabled | Settings required to connect to the cloud service.<br>Client certificates indicate to the server that you are the correct source of the connection. |
| 2 | client certificates | Register the client certificate.<br>Select directly or select a file to register. | |
| 3 | client secret key | Register the client private key.<br>Select directly or select a file to register. | |

* This setting is required to realize MQTTS communication.

(3) MQTT Settings

This product support functions which set MQTT destination host etc. For its communication, MQTT basic settings are shown as per below.

**Table 3.84 MQTT Basic settings**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Enable MQTTS | Enable/disable MQTTS communication.<br>With Check: Enable<br>Without Check: Disable | MQTTS requires certificate setting |
| 2 | Destination host name | Set host name of connecting destination device. | |
| 3 | Destination port number | Set TCP port No. of connecting destination device. | |
| 4 | Username | Set username for authentication. | |
| 5 | Password | Set password for authentication. | |
| 6 | Client ID | Set client ID for session identification.<br>※MQTT server will identify each communication session by client ID. Each client ID must be unique ID to differentiate with other IDs. | If this setting is empty, session will be discarded. |
| 7 | Password type | Select password type depending on supporting style of each cloud service.<br>0: Non-procedure<br>1: Auto calculate SAS (Shared Access Signatures) token value | Normally non-procedure is enough to operate. |
| 8 | QoS (Quality of Service) | Set QoS value for MQTT communication.<br>0: 0 (Not resend)<br>1: 1 (Check at least reach 1 time)<br>2: 2 (Check to reach only 1 time) | Sending packet will be increased if 1 or 2 is selected.<br>Every QoS enable to have TCP resending function. |
| 9 | Keep connection | Set whether to keep MQTT connection.<br>With Check: Keep connection.<br>Without Check: Do not keep connection | |
| 10 | Discard session during reconnection | Set whether to discard past session during its reconnecting process.<br>With Check: Discard session<br>Without Check: Do not discard session | |
| 11 | Keep alive message interval | Set sending interval time for keepalive message. In order to keep MQTT connection, this function need to be set proper time.<br>Applicable range: 10sec or more | In case message does not reach, comm. will be disconnected approx. x1.5 of its setting time. |
| 12 | Allies | Able to register topic name for each key which include in iopoll destination info. | In case no allies' registration settings |

<table>
<tr><th>#</th><th>Item</th><th>Details</th><th>Note</th></tr>
<tr><td></td><td></td><td>Key value and topic name will be linked and registered to be used.<br><br><table><tr><th>Item</th><th>Details</th></tr><tr><td>Key</td><td>Key value when iopoll address after ‘mqtt.’ in its destination description.</td></tr><tr><td>Topic</td><td>MQTT topic name which actually send out.</td></tr></table></td><td>made, Key value will be directly used for its topic name.</td></tr>
</table>

In case connection is not kept, TCP connection will be individually opened during its data sending and will immediately close once data has been sent out.
If session is not discarded during reconnection, this product will try to keep same MQTT session during its reconnection. In such case, there will be a left possibility that past published message may be able to receive by using subscribe function.

Regarding Allies, following are its setting methods.

Example: Destination of iopoll address is ‘mqtt.topicA’

If following details are registered on Allies,

Table 3.85 Allies setting example

| Key | Topic |
|---|---|
| TopicA | Mqtt/iot/device/topicA |

In such case, topic name of actual sending MQTT message shall be ‘mqtt/iot/device/topicA’

This product also supports subscribe function of MQTT message.

Following details are its related settings.

**Table 3.86 MQTT subscribe setting**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | MQTT subscribe function | Set activate/deactivate MQTT subscribe function.<br>With Check: Activate (Enable)<br>Without Check: Deactivate (Disable) | |
| 2 | Binding rules | In case any message receives which having registered topics under this rule, this message can be transferred to Modbus application etc.<br><br>Item: Topic — Details: Set topic name to be handled as subscribe target.<br>Item: Matching rule — Details: Set matching rule for received topic. For its rule setting, glob command can be used.<br>Item: Destination — Details: Destination address of its target application. | For example, whenever receiving messages which following to this binding rules, it can change its register values by Modbus. |

(4) MQTT Status

This product support to monitor MQTT communication status. Followings are its monitoring details.

**Table 3.87 Monitoring status**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | success | Count number of MQTT comm. success. | |
| 2 | fail | Count number of MQTT comm. fail. | |
| 3 | queueCount | Data number which not yet sent. | |
| 4 | dropCount | Data number which has discarded due to communication failure. | |

### 3.2.14 RESTio application

This product support to upload various data by REST API using HTTP protocol.

Following are REST settings and its monitor topics.

**Table 3.88 REST settings / monitor**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Resend & Backup setting | Set resend and backup settings to be prepared for communication failure and sudden power failure. | |
| 2 | Certificate setting | Certification registration setting required to communicate on HTTPS. | |
| 3 | REST setting | Set certificate, destination address information for REST communication. | |
| 4 | REST monitor status | Show REST communication status. | |

(1) Resend & Backup setting

This product will support resend and backup functions to prepare for communication failure and sudden power failure. Details are shown as per below.

**Table 3.89 Resend & Backup setting (HTTP)**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Retry if communication failure | Activate / deactivate retry setting to resend data in case of communication failure.<br>With Check: Activate<br>Without Check: Deactivate | |
| 2 | Maximum retries count | Specifies the number of retransmissions when communication fails. | |
| 3 | Retry cycle [sec] | Set retry cycle time for next sending after communication failed. | |
| 4 | Max. data size | Set maximum data size to be saved in case of communication failure.<br>Applicable range: up to 1000000 | |
| 5 | Backup setting | Activate / deactivate backup setting to be prepared for sudden power failure.<br>With Check: Activate<br>Without Check: Deactivate | |

If "Retry if communication failure" is disabled, the data is discarded when communication failure.
If "Retry if communication failure" is enabled, retransmission is performed every specified number of seconds in the retry interval.
In addition, data that failed to communicate is stored up to the maximum data size, and when the data size exceeds the maximum data size, data is discarded in order starting from the oldest data.
If "Back up against power off" is enabled, a backup file of the transmitted data will be created when communication fails. After creating this backup file, if this product is restarted, it reads the backup file and resumes sending data from the contents of the file.

* Iopoll status increases the number of successes, even if the data to be sent is discarded.
If the transmitted data is discarded, the number of failures of this application increases.

(2) Certificate setting

This product supports encrypt communication function by HTTPS.
Certificate settings which required for protocol encryption are shown as per below.

Table 3.90 Certification setting (REST)

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Enable Client Certificates | Enables or disables the client certificate function that utilizes the client certificate.<br>Setting range:<br>Checked: valid, unchecked: invalid | Settings required to connect to the cloud service.<br>Client certificates indicate to the server that you are the correct source of the connection. |
| 2 | Client certificate | Register the client certificate. Select directly or select a file to register. | |
| 3 | Client private key | Register the client private key. Select directly or select a file to register. | |

* This setting is required to realize HTTPS communication.

(3) REST Settings

This product support functions which set HTTP destination host etc. For its communication, HTTP basic settings are shown as per below.

**Table 3.91 HTTP (REST) basic settings**

<table>
<tr><th>#</th><th>Item</th><th>Details</th><th>Note</th></tr>
<tr><td>1</td><td>Username</td><td>Set username for authentication.</td><td></td></tr>
<tr><td>2</td><td>Password</td><td>Set password for authentication</td><td></td></tr>
<tr><td>3</td><td>Binding rule</td><td>Register communication details depending on each key value which include in destination address information of iopoll.<br><br><table><tr><th>Item</th><th>Details</th></tr><tr><td>Key</td><td>Key value when iopoll address after ‘rest.’ in its destination description.</td></tr><tr><td>URL</td><td>Destination URL address</td></tr><tr><td>Header</td><td>Header details</td></tr><tr><td>Methods</td><td>HTTP method used in its request.<br>0: None<br>1: GET (no encode)<br>2: GET (URL encode)<br>3: POST<br>4: PUT</td></tr></table></td><td>・In case URL encode is selected, any URL which include multi byte letters will be encoded to single-byte alphanumeric characters.</td></tr>
<tr><td>4</td><td>Merge continuous data</td><td>Enable/disable function to merge continuous data as one group.<br>With Check: Enable (Activate)<br>Without Check: Disable (Deactivate)</td><td>If several messages exist for the same destination address, it will merge in one group.</td></tr>
</table>

(4) REST monitor status

This product support to monitor REST communication status. Followings are its monitoring details.

**Table 3.92 REST monitor status**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | key | Key value included in iopoll destination address information. | |
| 2 | success | Success numbers of REST communication. | |
| 3 | fail | Fail numbers of REST communication. | |
| 4 | queueCount | Data numbers which not yet sent. | |
| 5 | dropCount | Data number which has discarded due to communication failure. | |
| 6 | errorCode | Show error code of REST communication result which failed to complete. | |

| # | Item | Details | Note |
|---|---|---|---|
| 7 | errorText | Show text information of REST communication result which failed to complete. | |

### 3.2.15 232 through application

This product support conversion function between TCP connection and RS232 connection.

Setting related to this RS-232 application are shown as per below.

**Table 3.93 232 through application**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | RS232 Setting | Setting for RS232 connection | |
| 2 | TCP setting | Setting for TCP connection | |

(1) RS232 Setting

Following are RS232 setting.

**Table 3.94 RS232 setting**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Baud rate | Specify the baud rate.<br>Setting range: Within 1000000 | |
| 2 | Size | Specifies the size of the data bit.<br>Options:<br>7: 7 bits<br>8: 8 bits | |
| 3 | Parity | These bits specify the parity bit setting.<br>Options:<br>0: None 1: Even 2: Odd | |
| 4 | Stop bit | Specify the stop bit setting.<br>Options:<br>0: 1 bit<br>1: 1.5 bits (not supported)<br>2: 2 bits | |

(2) TCP settings

Following are TCP connection setting.

Table 3.95 TCP Setting (For RS232)

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Connecting mode | Either to work as server, or work as client.<br>1: TCP server mode<br>2: TCP client mode | |
| 2 | [Server mode]<br>Port No. | TCP port No. during its waiting process.<br>Applicable range：0~65535 | |
| 3 | [Client mode]<br>Host Name | Destination host name to transfer RS232 data received during TCP client mode. | |
| 4 | [Client mode]<br>Port No. | Destination TCP port number to transfer RS232 data received during TCP client mode.<br>Applicable range：0~65535 | |

In case of server mode, this product will wait TCP communication and transfer to RS232 port.

In case of client mode, this product will transfer RS232 data to TCP addressed host and port No.

### 3.2.16 485 through application

This product support conversion function between TCP connection and RS485 connection.

Setting related to this RS-485 application are shown as per below.

**Table 3.96 485 through application**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | RS485 Setting | Setting for RS485 connection | |
| 2 | TCP Setting | Setting for TCP connection | |

(1) RS485 Setting

Following are RS485 setting.

**Table 3.97 RS485 setting**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Baud rate | Specify the baud rate.<br>Setting range: Within 250000 | |
| 2 | Size | Specifies the size of the data bit.<br>Options:<br>7: 7 bits<br>8: 8 bits | |
| 3 | Parity | These bits specify the parity bit setting.<br>Options:<br>0: None 1: Even 2: Odd | |
| 4 | Stop bit | Specify the stop bit setting.<br>Options:<br>0: 1 bit<br>1: 1.5 bits (not supported)<br>2: 2 bits | |

(2) TCP settings

Following are TCP connection setting.

**Table 3.98 TCP setting (RS485)**

| # | Item | Details | Note |
|---|---|---|---|
| 1 | Connecting mode | Either to work as server, or work as client<br>1: TCP server mode<br>2: TCP client mode | |
| 2 | [Server mode]<br>Port No. | TCP port No. during its waiting process<br>Applicable range：0~65535 | |
| 3 | [Client mode]<br>Host Name | Destination host name to transfer RS485 data received during TCP client mode. | |
| 4 | [Client mode]<br>Port No. | Destination TCP port number to transfer RS485 data received during TCP client mode.<br>Applicable range: 0~65535 | |

In case of server mode, this product will wait TCP communication and transfer to RS485 port.

In case of client mode, this product will transfer RS485 data to TCP addressed host and port No.

### 3.2.17 Datamanager application

This product supports data acquisition and transmission to external devices. Compared to iopoll application, datamanager application supports sending triggers by retrieving data from connected devices and sending at any time. In addition, it is possible to process and shape the data acquired from the connected device to generate the optimum transmission data on the external device side.
Modbus is supported for communication protocols with connected devices, and MQTT, HTTP (REST) are supported for communication protocols to external devices.
* Other protocols are individually supported by creating additional applications. Please contact local supplier.

This function sends a request (Modbus query) to Modbus application and a request to send the collected information (payload) to MQTT, REST application.
The connection settings for each protocol are made by the application dedicated to each protocol.

**Table 3.99 Datamanager application**

| # | Item | Specifications |
|---|---|---|
| 1 | Modbus queries | Up to 100 channels |
| 2 | Supported function codes | FC3: Read holding register<br>FC4: Read input register |
| 3 | Maximum read size | FC3, FC4:1～50 |
| 4 | Transmission cycle | 1000～86400000[ms] |
| 5 | Modbus error behavior | ・ Retaining the Last Acquired Value<br>・ Stores the value specified when the threshold is exceeded. |
| 6 | Acquisition buffer | Two-dimensional array buffer [1 to 256, 1 to 256] |
| 7 | Trigger condition | Comparison between acquired and fixed values: 6 types (==, !=, >=, >, <=, <)<br>Comparison between the acquired value and the previous acquired value: 3 types (>, <, ==)<br>Comparison of buffer and fixed values: 6 types (==, !=, >=, >, <=, <) |
| 8 | Individual data | Data Abbreviation, Byte Order Specification |
| 9 | Individual data format | Unsigned integer, signed integer, signed float,<br>Character (ASCII) |
| 10 | Payload sending opportunity | Periodic transmission, fixed time transmission, trigger transmission |
| 11 | Payload transmission format | Text format, binary format |

This function sets each of the following items. The configuration of the settings is shown in Figure 3.2 Configuration of the settings.

(1) Basic setting

Defines basic settings related to this function.

(2) Modbus Settings

To communicate with external devices in Modbus protocol. Define Modbus address, function code, register address, transmission cycle, and storage buffer of acquired data.

(3) Buffer setting

Defines the data buffer for storing the data acquired by Modbus communication and the response buffer for storing the latest acquired value by Modbus communication. The buffer can be specified in a two-dimensional array, and the historical data, maximum/minimum/average value, can be calculated using buffer data of depth.

(4) Trigger setting

Defines a comparison condition expression for the data buffer and response buffer for payload transmission. Modbus response data can be transmitted when it changes according to the content.

(5) Individual data setting

Defines the individual data and source data buffers to be included in the payload. The maximum / minimum / average values can be calculated from the buffers of two-dimensional arrays.

(6) Payload data setting

Define the payload data to be sent to external devices / servers and the transmission timing. By specifying the data generated by the individual data setting, the processed data of Modbus response data can be transmitted as a payload.

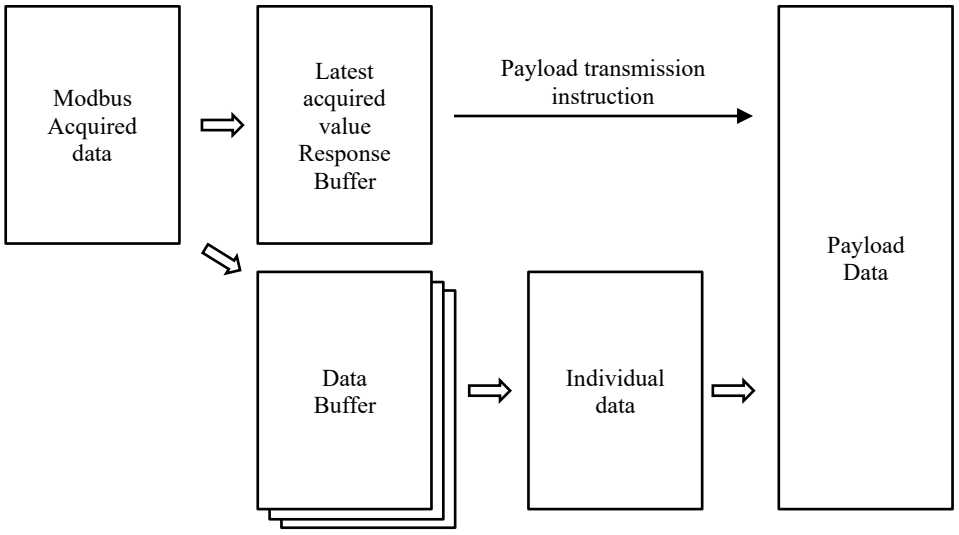



**Figure 3.2 Configuration of the settings**

#### 3.2.17.1 Basic setting

Table 3.95 lists the basic settings.

**Table 3.100 Basic setting**

| # | Item | Description | Note |
|---|---|---|---|
| 1 | Enable for this application | Enables or disables this function.<br>When disabled, this function does not work. | |
| 2 | Start communication after startup | Specifies whether to start communication with peripherals when this application is started. | |

If "Start communication after startup" is enabled, datamanager application starts operation automatically after startup of this product. After datamanager application starts operation, it starts communicating with external devices after 35 seconds have elapsed.

#### 3.2.17.2 Modbus Settings

Modbus setting items are shown below.

**Table 3.101 Modbus setting**

| # | Items | Description | Note |
|---|---|---|---|
| 1 | Modbus socket | Specifies the socket name of modbusio application. | |
| 2 | Modbus querying setting | Specifies whether to start communication with peripherals when this application is started. | |
| (1) | Device name | | |
| (2) | Query Name | | |
| (3) | Function code | | |
| (4) | Query start address | | |
| (5) | Number of registers | | |
| (6) | Query send period | | |
| (7) | Response timeout | | |
| (8) | Modbus response error judgment | | |
| (9) | Number of modbus response error judgment | | |
| (10) | Set value when error judgment threshold is exceeded | | |
| (11) | Data buffer name | | |
| (12) | Start index | | |
| (13) | Update period | | |
| (14) | Trigger condition | | |
| (15) | Response Buffer Name | | |

(1) Device name

Specifies the destination device name for this Modbus querying. Specify the connection destination device name defined in the connection destination device name field of Modbusio application.

Setting range: 1 to 100 characters

(2) Query name

Defines Modbus queryname.

Setting range: 1 to 100 characters

(3) Function code

Specifies the function code of Modbus query.

Options:

3: Function code 03 (Read Holding Register)

4: Function code 04 (Read Input Register)

(4) Query start address

Specifies the starting address of Modbus query.

Setting range :0～65535

(5) Number of registers

Specifies how many registers Modbus queries request.

Function codes 03 and 04: 50 max.

(6) Query send period

Specifies the interval for sending Modbus queries.

Setting range: 1000 to 86400000 [ms]

Depending on the loading condition of modbusio application, Modbus queries may not be sent in the expected period.

(7) Response timeout

Specifies the wait time for a response to a Modbus query.

Setting range: 1 to 1000 [ms]

(8) Modbus response error judgment

Specifies whether to write the specified value stored in the data buffer when the response to Modbus query could not be received or the number of error responses exceeded the specified number of times. If Modbus response cannot be received when this setting is disabled, the data buffer value retains the last stored Modbus response.

(9) Number of modbus response error judgment

Specify the number of judgements when item (7) is enabled.

(10) Set value when error judgment threshold is exceeded

Specifies the value to be written to the data buffer when the threshold specified in item (8) is exceeded.

Setting range :0 x 00～0 xFF

By setting items (8) to (10) of Modbus query setting, the specified data can be stored when a response error occurs in Modbus query. This function allows CPTrans to send unique data to external devices when a Modbus communication error occurs.

Example: 3 words of Modbus registers

Modbus response error judgment: Valid

Modbus response error judgment count: 3

Setting value when error judgment threshold is exceeded: 0x56

With the above setting, if a Modbus response error occurs four times consecutively, the threshold value is exceeded and [0x56 56 56 56 56 56] is written to the data buffer. After that, Modbus response can be received normally and the response error is cleared, Modbus response data is stored in the data buffer.

(11) Data buffer name

Specifies the name of the data buffer in which the response data of Modbus query is to be stored.
Specifies the name of the data buffer defined in the data buffer setting.

(12) Start index

Specify the position from the beginning of the storage destination data buffer specified by item (10).

(13) Update period

Specifies the data buffer storage frequency for response data for Modbus queries.
Setting range: 1 to 86400 [sec]

(14) Trigger condition

Specifies the trigger name to be used for sending changes according to the content of the response data of Modbus query. This setting is not required when the transition transmission is not used.

(15) Response Buffer Name

Specifies the response buffer name to store the response data for Modbus query. Specifies the name of the data buffer defined in the data buffer setting. The response buffer is used as a judgment condition for transmission when it changes. This setting is not required when the transition transmission is not used.

3.2.17.3 Buffer setting

Below table is the buffer setting items. This setting item defines the data buffer and response buffer.

**Table 3.102 Buffer settings**

| # | | Item | Description | Note |
|---|---|---|---|---|
| 1 | | Data buffer | Defines the data buffer | |
| | (1) | Buffer name | | |
| | (2) | Buffer width | | |
| | (3) | Buffer depth | | |
| | (4) | Buffer initial value | | |

(1) Buffer name

Specifies the name of the buffer. Defines the data buffer and response data buffer specified in items (11) and (15) of Table 3.101 **Modbus setting**. If the data buffer/response data buffer specified in Modbus setting is not defined in this setting item, an error occurs and datamanager application stops operating.

(2) Buffer width

Specifies the width of the buffer. It needs to match the number of Modbus query request registers specified in Table 3.101 **Modbus setting** items of setting items (5). Since the unit of this setting item is byte, set the number of request registers for Modbus queries multiplied by 2.

Example: When the number of request registers for Modbus queries is 4 words, specify 4 × 2 = 8 bytes.

Setting range :1～256

(3) Buffer depth

Specifies the number of data items in the buffer. A data buffer with the same name as the number specified in this item is created. For the response data buffer, specify 1.

Example: When this setting is 3, 3 buffers are generated, and Modbus response data is stored from the lowest index. When data is stored in the third buffer, it returns to the first index.

Setting range :1～256

(4) Buffer initial value

Specifies the initial value of the buffer.

Setting range :0 x 00～0 xFF

3.2.17.4 Trigger setting

Below table lists the trigger setting items. Define the trigger condition with this setting item.

**Table 3.103 Trigger settings**

| # | | Item | Description | Note |
|---|---|---|---|---|
| 1 | | Trigger | Defines the trigger condition | |
| | (1) | Trigger name | | |
| | (2) | Data buffer name | | |
| | (3) | Start index | | |
| | (4) | Compare Data type | | |
| | (5) | Condition | | |
| | (6) | Compare value | | |

(1) Trigger Name

Specifies the name of the trigger condition. Specify the trigger condition name specified in Table 3.101 **Modbus setting** items (14) of Modbus setting item. If the trigger condition name specified in Modbus setting is not defined in this setting item, an error occurs and datamanager application stops operating.

(2) Data buffer name

If comparing the value is the data buffer value, specify the data buffer name specified in Table 3.102 **Buffer settings** item (1) of the buffer setting. This setting is not required when the data buffer is not used for the trigger condition.

(3) Start index

Specifies the start position of the data for trigger judgment.

Example: To determine the third byte of the response data buffer, specify 2 for this item.

Setting range :0～255

(4) Compare data type

Specifies the data format for trigger judgment. Comparisons are compared in big endian.

Setting range:

byte: Byte-type comparison (comparing 1-byte data from the starting position)

word: Compare by word type (compare 2-byte data from the starting position)

dword: Double-word type comparison (4-byte data from the starting position is compared)

(5) Condition

Specifies the condition for trigger judgment. Items in conditional expressions are shown below.

Payload is sent when the conditions of each setting item are satisfied.

Table 3.104 Trigger condition items

| # | Item | Trigger condition | Remarks |
|---|---|---|---|
| 1 | == Comparison value | The value of the response data buffer is equal to the comparison value. | |
| 2 | ! = Comparison value | Response data buffer value and comparison value are not equal | |
| 3 | > = Comparison value | Response data buffer value is greater than comparison value<br>Or equal | |
| 4 | > Comparison value | Response data buffer value is greater than comparison value | |
| 5 | <=Comparison value | The value of the response data buffer is smaller than the comparison value.<br>Or equal | |
| 6 | < Comparison value | The value of the response data buffer is smaller than the comparison value. | |
| 7 | ! = Previous value | The value of the response data buffer is not equal to the value of the response data buffer acquired last time. | |
| 8 | > Previous value | Response data buffer value is larger than the previously acquired response data buffer value | |
| 9 | < Last value | The value of the response data buffer is smaller than the value of the response data buffer acquired last time. | |
| 10 | Data buffer == Compare value | The value of the data buffer is equal to the comparison value. | |
| 11 | Data buffer! = Comparison value | Data buffer value is not equal to comparison value | |
| 12 | Data Buffer >= Compare Value | The value of the data buffer is greater than or equal to the comparison value | |
| 13 | Data Buffer > Compare Value | Data buffer value is greater than comparison value | |
| 14 | Data buffer <= Compare value | The value of the data buffer is less than or equal to the comparison value | |
| 15 | Data Buffer < Comparison Value | Data buffer value is smaller than comparison value | |

(6) Comparison value

Specifies the comparison value for trigger judgment.

Setting range :0 x 0～0 xFFFFFFFF

### 3.2.17.5 Individual data setting

Below table shows the individual data setting items. These setting items define the individual data for payload transmission.

**Table 3.105 Individual data setting**

| # | | Item | Description | Note |
|---|---|---|---|---|
| 1 | | Individual data | Individual data setting | |
| | (1) | Data name | | |
| | (2) | Data origin | | |
| | (3) | Data buffer name | | |
| | (4) | Depth index | | |
| | (5) | Width Index | | |
| | (6) | Length | | |
| | (7) | Add time to Data | | |
| | (8) | Data Omission Condition | | |
| | (9) | Retention time | | |
| | (10) | Threshold | | |
| | (11) | Datakey | | |
| | (12) | Binary format | | |
| | (13) | Calculation type | | |
| | (14) | Digit after the decimal point | | |
| | (15) | Interpretation of data type | | |
| | (16) | Byte order specification | | |
| 2 | | Fixed data | Defines fixed value data | |
| | (17) | Key | | |
| | (18) | Data | | |

(1) Data name

Specifies the name of the individual data.

(2) Data origin

Specifies the source of the individual data.

Setting items:

Data Buffer: Generates individual data from the data buffer.

Fixed Value: Generates individual data from fixed values.

(3) Data buffer name

If a data buffer is data origin, specify the data buffer name in this item. Specify the buffer name specified in Table 3.102 **Buffer settings** item (1).

(4) Depth index

Specifies the start index of the depth from the data buffer referenced by the individual data.

Setting range :0 to 255

(5) Width index

Specifies the start index of the width from the data buffer referenced by individual data.

Setting range :0～255

(6) Length

Specifies the number of bytes of data to be referenced by individual data.

Setting range :1～256

Example: If data buffer with a width of 8 and a depth of 3 is defined as shown in Figure 3.3 Generating individual data from data buffer and with data stored in the buffer as shown in Table 3.105 **Individual data setting** items (4) depth of 1, item (5) acquisition start position of 3, and item (6) byte number of 4 are defined, [0x0D, 0x0E, 0x0F, 0x10] will be stored in the individual data.

Data buffer width

Data buffer depth

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0x01 | 0x02 | 0x03 | 0x04 | 0x05 | 0x06 | 0x07 | 0x08 |
| 1 | 0x0B | 0x0C | 0x0C | 0x0D | 0x0E | 0x0F | 0x10 | 0x11 |
| 2 | 0x14 | 0x15 | 0x16 | 0x17 | 0x18 | 0x19 | 0x1A | 0x1B |

**Figure 3.3 Generating individual data from data buffer**

(7) Add time to data

Specifies whether the payload data contains the time at which the individual data was generated. If it's enabled, the time format includes time stamps in the YYYY/MM/dd/hh/mm/ss format. This setting is valid only when Table 3.107 item (12) Payload data Format is in Text Format.

(8) Data omission condition

Compares current individual data with last acquired individual data and skip inclusion of individual data into the payload if the specified condition is true. The conditions of data omission are shown below.

Table 3.106 Data omission condition

| # | Item | Omission condition | Note |
|---|---|---|---|
| 1 | Not omit | Omission doesn't work and store data in payload | |
| 2 | Equal data | The value of the individual data is equal to the previous data. | |
| 3 | Equal data and time | The value of the individual data and the acquisition time are equal to the previous data. | |
| 4 | Data difference exceeds threshold | The difference between the value of individual data and the previous data is below or equal to the threshold value. | |
| 5 | Time difference exceeds threshold | The difference between the acquisition time of the individual data and the acquisition time of the previous data is below or equal to the threshold value (seconds). | |
| 6 | Over | The value of the individual data is over than or equal to the previous individual data. | |
| 7 | Less than | The value of the individual data is smaller than or equal to the previous individual data. | |

(9) Retention time

Specifies the retention time for individual data. If the specified time has elapsed, the generated individual data is discarded. If 0 is specified, individual data is not discarded.

Setting range: 0 to 86400 [sec]

(10) Threshold

Specify the threshold value when "Data difference exceeds threshold" or "Time difference exceeds threshold" is specified in the data omission condition of the item (8). If the time difference is less than or equal to the threshold value, the data is omitted. Unit for this parameter is [sec].

Setting range :0～0 xFFFFFFFF

(11)Data key

Specifies the data key when a fixed value is specified as the data origin for item (2). Match with the data key specified in item (17).

(12)Binary format

Specify the binary format for individual data when sending payload is binary format.

If "num%fmt" is specified in this item, character strings (ASCII code) are stored in the payload.

"num%fmt" is interpreted as the format string of sprintf function in C.

Example: If 120 is stored in a 2-byte data buffer and "num%04d" is specified in the binary format, 4 bytes of individual data [0x30 31 32 30] are stored in the payload.

This setting is valid only when Table 3.107 items (11) Payload transmission format is in binary format.

(13)Calculation type

This item is to calculate the maximum, minimum, and average values of individual data.

If the operation of either the maximum value, minimum value, or average value is specified, the depth specification of item (4) is invalid, and the value is calculated by data buffer depth set in Table 3.102 **Buffer settings**.

Setting items:

- Not calculate
- Calculate the max value
- Calculate the min value
- Calculate the average value

(14)Digit after the decimal point

Specifies the number of decimal places for individual data when payload is sent in text format.

Generates individual data by rounding the digit under the digit specified by this item.

Setting range :0 to 5

(15)Interpretation of data type

Specifies how to treat the data from data origin and generate the individual data.

Setting range:

- Treat as an unsigned integer
- Treat as a signed integer
- Treat as signed floating point number
- Treat as characters (ASCII code)

(16)Byte Order Specification

Specifies the byte order. This setting is applied when a byte string is read from the data buffer and when this individual data is stored in the payload in binary format.

0: Treat as a big endian

1: Treat as a little endian

By setting these items from (13) to (16), maximum, minimum, and average value can be calculated on the individual data.

This function operates differently depends on the Table 3.107 item (11) Payload data format. Item (14) Digit after the decimal point is valid only in text format, and this setting is ignored in binary format. The item (16) byte order specification is valid only in binary format, and this setting is ignored in text format.

If the maximum value/minimum value/average value function is used, please note following points at setting phase. If setting is incorrect, this function doesn't work properly.

- If Table 3.105 **Individual data setting** item (15) "Interpretation of data type" is "Treat as an unsigned integer" or "Treat as a signed integer", please set 1, 2, 4 or 8 to item (6) "Length". If the other value is set, this application detects error and stop working.

- If Table 3.105 **Individual data setting** item (15) "Interpretation of data type" is "Treat as signed floating point number", please set 4 or 8 to item (6) "Length". If the other value is set, this application detects error and stop working.

- If Table 3.105 **Individual data setting** item (13) "Calculation type" is "Calculate the max value", "Calculate the min value" or "Calculate the average value", please do not set "Treat as characters (ASCII code)" to item (15) "Interpretation of data type". This application detects error and stop working.

- If Table 3.105 **Individual data setting** item (15) "Interpretation of data type" is "Treat as characters (ASCII code)", value which cannot be converted to character or ASCII code is skip storing to individual data and stored data length is shorter than specified length.

- If Table 3.107 item (11) Payload data format is "Binary format", average value is generated as 4 bytes floating point data. For other data is calculated according to Table 3.105 **Individual data setting** item (6) and (15)

Example: When 2 bytes are specified as an unsigned integer, the value to be acquired is stored as a 2-byte unsigned integer.

(17)Key

Specifies the key name when using a fixed value. The key name specified in this item is used in the payload setting.

Setting range: 0 to 128 characters

(18)Data

Specifies the setting value for the defined key name.

### 3.2.17.6 Payload setting

Table 3.107 **Payload setting** shows the payload setting items. This setting item defines the individual data for payload transmission.

**Table 3.107 Payload setting**

| # | Item | Description | Note |
|---|---|---|---|
| 1 | Level of gzip compression | Specifies the compression level for gzip compressing a text-formatted payload. | |
| 2 | Payload | Specify the payload data to be sent to external devices. | |
| (1) | Target application | | |
| (2) | Payload name | | |
| (3) | Send wake up | | |
| (4) | Send Timing | | |
| (5) | Send period [sec] | | |
| (6) | Send hour | | |
| (7) | Time zone mode | | |
| (8) | Time zone [min] | | |
| (9) | Random width [min] | | |
| (10) | Trigger enable | | |
| (11) | Key name | | |
| (12) | Payload data format | | |
| (13) | Response timeout [ms] | | |
| (14) | Trigger name | | |
| (15) | Payload | | |
| (16) | Compression enable | | |

(1) Target application

Specifies the payload data destination. Specify "mqttio" to use MQTT and "restio" to use REST.

(2) Payload name

Specify the payload name.

(3) Send wake up

Enables payload sending when Datamanager app starts.

(4) Send timing

Specify the payload transmission timing. Transmission timing is shown below.

Table 3.108 Send timing

| # | Item | Send timing | note |
|---|---|---|---|
| 1 | Periodical | Sends the payload at the specified periodic time. | |
| 2 | On-demand<br>(Not supported) | Payload is sent by a request from another application. | |
| 3 | Scheduled | Sends the payload at the specified time. | |
| 4 | Trigger | The payload is sent when the trigger condition is true. | |

(5) Send period

Specify the period for payload sending. This setting is valid only if the item (4) Send timing is set to "Periodical".

Setting range: 0 to 90000 [sec]

(6) Send hour

Specify the time to send the payload. This setting is valid only if the item (4) Send timing is set to "Scheduled".

Setting range: 0 to 23 [hour]

(7) Time zone mode

Time Specify the transmission time zone mode for fixed transmission. This setting is valid only when the item (4) Send timing is set to "Scheduled".

・Specify in system application

・Specify in this application

(8) Time zone

Set the time zone for fixed time transmission. This setting is valid only when the item (4) Send timing is set to "Scheduled". Set 0 to set the standard time (UTC) and set 540 to set the Japan time JST (UTC + 09:00).

(9) Random width

Specifies the random width at fixed-time transmission. This setting is valid only when the item (4) Send timing is set to "Scheduled". When this setting value is 10 and sent to 13:00, a payload is sent between 13:00 and 13:10.

Setting range: 10 to 1440 [min]

(10) Enable Trigger Transmission

Enables or disables trigger sending. This setting is valid only when the item (4) Send timing is set to "Trigger".

(11) Key name

Specifies the key name. When sending this payload using MQTT, this setting is a topic in MQTT communication.

Setting range: 1 to 512 [characters]

(12) Payload data format

Specifies the payload data transmission format.

- Text format
- Binary format

(13) Response Timeout

This bit specifies the timeout period when a payload send request is sent to MQTT or REST application that sends this payload.

Setting range: 1 to 1000 [ms]

(14) Trigger name

Specifies the trigger send name to be used. Specify the trigger name defined in Table 3.103 **Trigger settings** item (1).

(15) Payload

Specifies the contents of the payload to be sent. This setting differs according to Table 3.107 **Payload setting** item (12) Payload data format.

(a) Text format

In the case of text format, the payload data is described by the following types.

(i) Free description method

Write in json format.

Example:{"key1": {"key1-1": "123"、 "key1-2": 1, "key1-3": "abcdefg"} 、 "key2": {"key2-1": "456"}}

(ii) Environment value

$ substitution is available to store CPTrans's environment-variables, times, and so on in the payload.

Example: {"timestamp":${time}}

When written as above, the value stored in payload data is as follows.

{"timestamp":1599647420}

Below table shows the environment variables that can be referenced by $ substitution.

Table 3.109 Environment variables

| Environment variable | Description |
|---|---|
| ${DID} | Device ID: Device unique identifier |
| ${HWID} | Hardware ID: Identifier of the device HW |
| ${ETHMAC} | Ethernet MAC addressing |
| ${IMSI} | IMSI: A number that uniquely identifies the user of the cellular network stored in SIM |
| ${ICCID} | ICCID: Identifier of SIM at startup |
| ${MSISDN} | Phone number<br>※It may not be stored depending on SIM card. |
| ${IMEI} | Modem identification number |
| ${time} | Epoch time [sec] |
| ${time_ms} | Epoch time [milliseconds] |

(iii) Read from other applications

Status of other applications can be acquired and stored in the payload. Below table shows the format for obtaining information about other applications.

Table 3.110 Format of reading status from other applications

| # | Item | Description |
|---|---|---|
| 1 | Overall format | Format:<br><key>':'<${#internal.[appid].[tag1].[tag2]…}> |
| 2 | Details | <key>: Specify an arbitrary string. Specify the name of value to be acquired.<br><${#internal.[appid].[tag1].[tag2]…} ><br>*Specifies appid of internal:internalio.*<br>*Appid: Specifies the identity of the application. See the command reference manual.*<br>*Tag-Specifies the tag name given to each application's parameters.*<br>For Array and object types, ". Tags can be narrowed down by continuing with ". |
| 3 | Examples | When obtaining signal strength from Router application.<br>Write "internal": ${#internal.router.modemInfo.rsrp} in payload[].text.<br>The result obtained is as follows and is used when sending payload.<br>{"internal":-81} *Reception strength is-81 |

(iv) Individual data

The generated individual data can be stored in the payload.

Example: "indData0001" and "indData0002" are defined for individual data settings and are included in this field.

{${%indData0001}, ${%indData0002}}

If the value stored in indData0001 and indData0002 is 100,2, then {"indData0001":100} and {"indData0002":2} are used.

(b) Binary Format

In binary format, the payload is described by the following three types.

(i) Fixed data description

Binary data can be written in two-digit hexadecimal numbers, one byte at a time.

Example: "text":"1 F,3 C,0 B,A 2"

(ii) Keyword description

${keyword} is available to use a specific value corresponding to a keyword as a binary.

Available keywords are listed in below table.

**Table 3.111 Available keyword**

| Environment variable | Description |
|---|---|
| ${year} | The year data when a payload data is created. It expresses as two bytes of big endian. Example: 0x07E4 in 2020 |
| ${month} | The month data when a payload data is created. It expresses month (from 1 to 12) in one byte. |
| ${day} | The day data when a payload data is created. It expresses day (from 1 to 31) in one byte. |
| ${hour} | The hour data when a payload data is created. It expresses hour (from 0 to 23) in one byte. |
| ${minute} | The minute data when a payload data is created. It expresses minute (from 0 to 59) in one byte. |
| ${second} | The second data when a payload data is created. It expresses second (from 0 to 59) in one byte. |
| ${WANIPn} | (n=1 to 5) The WAN side IP address is expressed in four bytes. n specifies the APN number. |

(iii) Description of individual data

The generated individual data can be stored in the payload. If the binary format is specified in Table 3.105 **Individual data setting** item (12), the acquired individual data is stored in the payload as a byte string. If the binary format specification is num%fmt, the data is interpreted as a string and ASCII code. And the individual data is stored in the payload as a byte string. fmt means the format string for sprintf function in C.

Example: Number of data buffers three: data001, data002, data003

Stored data: 10, 40, 120

Byte size :1,4,2

Binary format: None, None, num%04d

Specified as "text":"${%data001}, ${%data002}, ${%data003}

If above written, 9 bytes of data are stored in the payload.

0A 00 00 00 28 30 31 32 30

If the data origin is a fixed value, the binary format specification is invalid and is stored in hexadecimal in 1-byte increments.

(16)Compression enable

Specifies whether the payload is gzip compressed at payload sending (in text format).

### 3.2.18 Logsd application

Logsd application stores log (stderr) for each application on this product as a text file on the inserted SD card.

Logsd saves files in the following format:

```
SD card:/media/sdcard/log/(AP name)/(Index)-(YYMMDD)T (hhmmss).log
```

The location to save the log file is the SD card area only.
Index filename is incremented when the file size exceeds the specified value, and a new file is generated.
The file size and the maximum storage capacity for log files can also be specified in logsd settings.
(If the maximum capacity is exceeded, the oldest files are deleted first.)

[Caution]

- SD card is necessary for using this application. Please prepare the SD card separately.
- External factors such as external noise, vibration or impact may prevent the SD card from being recognized correctly and cause the log to remain (not be written).
- Please use SD cards whose maximum storage capacity is up to 32GB. Please note that the storage capacity SD card that exceeds this may not be recognized properly depending on the manufacturer and may not be used.
- Depending on the log output level of the app, save all the logs may not be saved.

### 3.2.19 Configuration management application

This product supports to download the setting of each app of this product s text file and upload the setting file into this product to restore parameters for each application.

### 3.2.20 Band application

This application supports to control band width for modem connection. Band for modem connection can be fixed or limited so that this product is able to connect proper band in each country.

Below table shows specification of band application.

**Table 3.112 Band application**

| # | Item | | Specification |
|---|---|---|---|
| 1 | Function | Carrier searching | Searching available carriers. Specification depends on the inserted USIM card. |
| 2 | | Select band | Select band for avoiding connection. |
| 3 | Remark | | Band setting by this application is applied to all APN connections (from APN1 to APN5). |

Setting items for band application is shown below. It is necessary to set band limitation for each bandwidth.

**Table 3.113 Band setting**

| # | Item | Description |
|---|---|---|
| 1 | Enable eliminate band setting | Specify enable/ disable individual band setting. |
| 2 | GSM bandwidth | Specify band limitation for GSM bandwidth.<br>Setting range: GSM900, GSM1800, GSM850, GSM1900 |
| 3 | WCDMA bandwidth | Specify band limitation for WCDMA bandwidth.<br>Setting range: WCDMA2100, 1900, 850, 900, 800, 1700 |
| 4 | LTE bandwidth | Specify band limitation for LTE bandwidth.<br>Setting range: from LTE 1 to LTE 42 |

[Caution]

- If all bandwidths are prohibited for connection, connecting to WAN fails.
- CPTrans-MGW needs to be set proper band limitations in each country. Please confirm band limitation in each country beforehand.

  Example: If CPTrans-MGW is used in Brazil, band 39 and 40 must be limited for connection.

### 3.2.21 Monitoring application

This application supports to monitor operation status of each application on this product. By referring log files generated by other applications, checking operation status of them, it can monitor operation status of this product itself, and saves error log of this products.

With use of the “Maintenance event log function”, this application generates event log files which record CPTrans’s internal events for maintenance purpose. It also supports “self-diagnosis” which judges presence of error on this product, “Malfunction report” which sends notifications at error occur, and “fail-safe function” which proceeds self-recover this product itself by executing reboot specified application or system.

Specification of this application is shown below.

**Table 3.114 Support functions on this product**

| # | Function | Specification |
|---|---|---|
| 1 | Self-diagnosis | ● By referring “operation status” managed by other applications, it judges presence of internal error and event which should be reported.<br>● If some error occurs on this product, or event for reporting is detected, it issues event ID and detected time stamp to “Malfunction report” and “Fail-safe”. |
| 2 | Malfunction report<br>(Not supported) | ● Based on the information from “Self-diagnosis”, create a message according to the content of detection and send it to management server. |
| 3 | Fail-safe | ● Based on the information from “Self-diagnosis”, execute reboot to specified application or system according to the content of detection for self-recovering. |
| 4 | Log download | ● This function saves following log to SD card, and those log files can be downloaded from Web GUI.<br>- Maintenance event log<br>Log records detected by analysis for maintenance event log<br>- Self-diagnosis log / operation status log<br>Log files detected by self-diagnosis<br>- Reboot application log<br>Log files generated at issuing request for reboot. |

Process flow for each function described in Table 3.114 **Support functions on this product** is shown below.

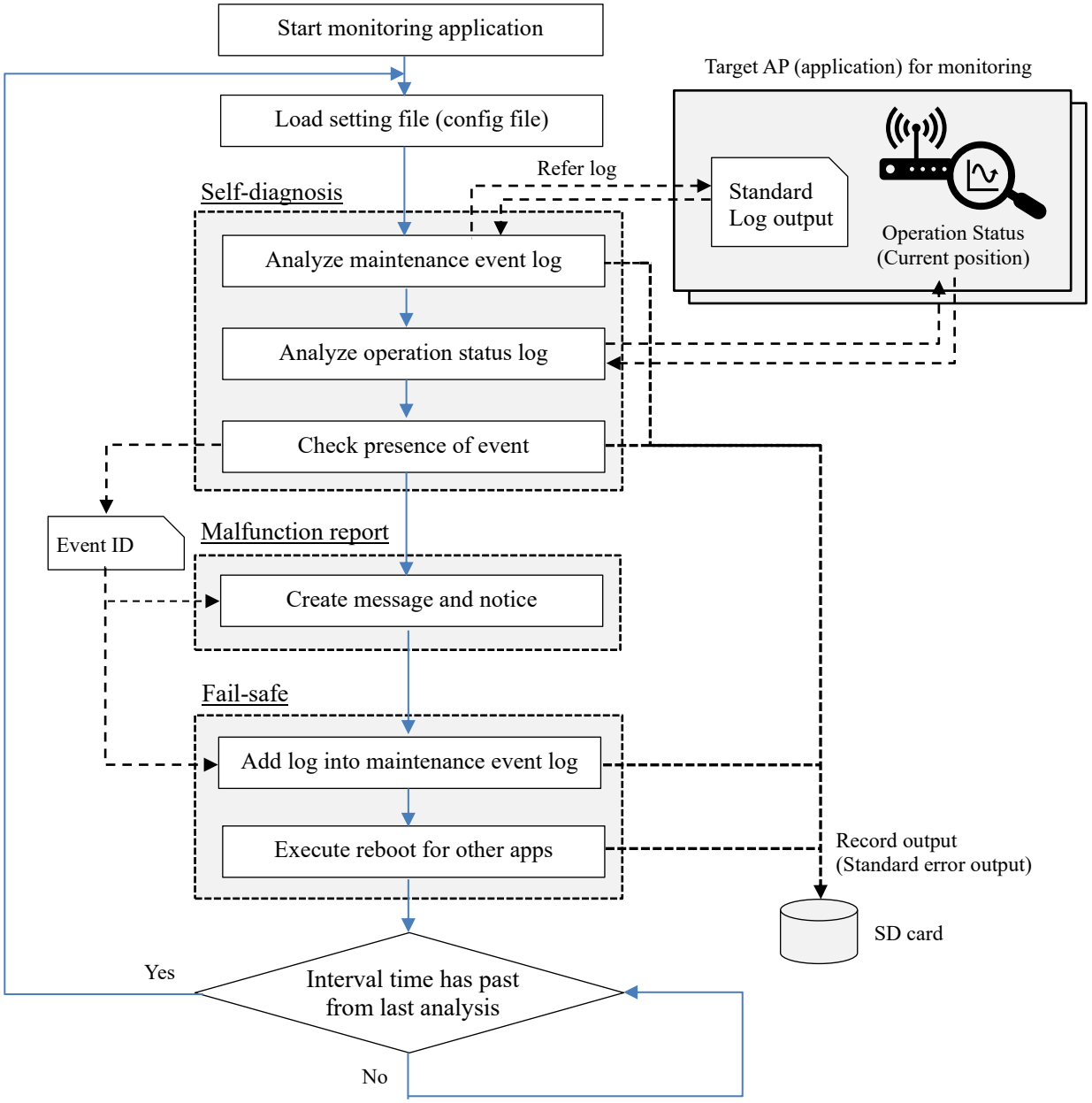



**Figure 3.4 Flow-chart of monitoring application**

[Details of monitoring process]

1) At startup, this application loads setting parameters which input and saved by Web GUI. Then start monitoring process periodically. Current time information is recorded as start analyzing time in every starting of monitoring process.
2) Firstly “Analyze maintenance event log” function refers standard output log from other applications and creates a maintenance event log.
3) “Self-diagnosis” function checks the maintenance event log and operation status managed by each application, diagnose internal events including error on this product and issues event IDs if some events which should be reported are detected.
4) “Malfunction report” sends message to the management server according to the event IDs issued by “Self-diagnosis”.
5) Based on the event IDs information, “Fail-safe” also judges whether self-recovering is necessary or not. If it decides as necessary, executes reboot to specified application or start system reboot.
6) If self-recovering is not processed at “Fail-safe” function or recovering is applied to only specified application (not system reboot), next monitoring process starts after interval time. If system reboot is executed, monitoring process starts after startup since this application is also rebooted by system reboot.

#### 3.2.21.1 Self-diagnosis

"Self-diagnosis" function refers each application's operation status and diagnoses events occurred in this product. If error occurs or some events which should be reported to the management server are detected, "Self-diagnose" function issues event IDs which indicates contents of detection, and detected timestamp, to "Malfunction report" and "Fail-safe" functions.

Each function regarding self-diagnosis is described below.

1) Analyze for Maintenance event log and output

This function loads a setting of event log and checks records whether contents of the records are matched with analysis conditions or not.

i) Make rules for Maintenance event log

Select a target application and define what record is created if specified strings are detected in a standard output log from the target application.

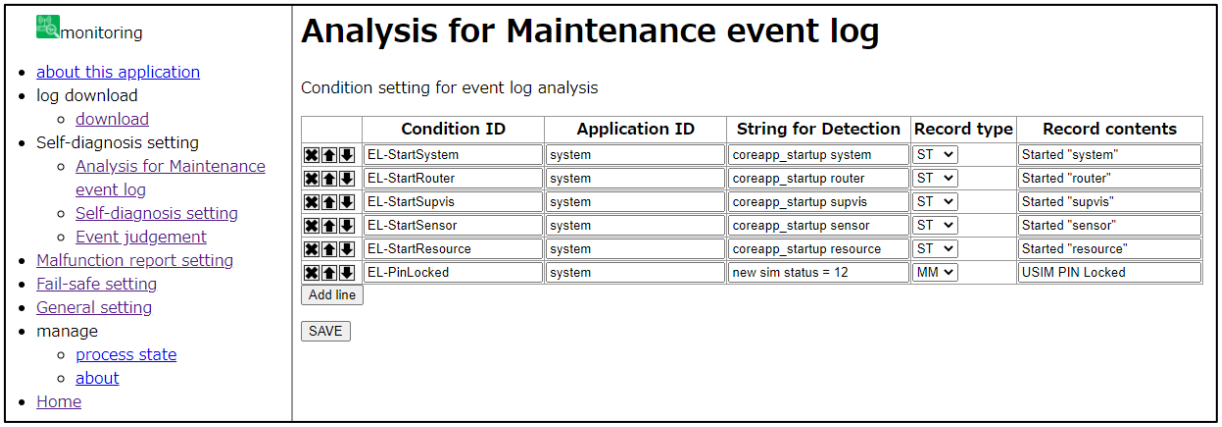



**Figure 3.5 Analysis for maintenance event log window**

Above items "Application ID", "String for Detection", "Record type" and "Record contents" are necessary for making rule for Maintenance event log. Each item is described in below.

As shown on Figure 3.4 Flow-chart of monitoring application, this application loads setting files at startup. Then the process for Analysis for maintenance event log is executed according to the setting defined in Figure 3.5 Analysis for maintenance event log window

- *Application ID:*

  Specify target application for referring standard output log.

  Maintenance event log refers standard output log from applications installed in this product.

- *String for Detection*

  Strings data for detection of trigger for record output. They are contained in standard output log. Maintenance event log function starts creating records if the string for detection data is exist in the standard output.

  This item can be specified either all strings in a line or a part of strings. If strings from the standard output is exactly same as this item, this function treats as detection even if other strings are contained in the standard output.

- *Record type*

  Specify type of record. A list of record types is shown below.

**Table 3.115 Support functions on this product**

| # | Type | Description |
|---|---|---|
| 1 | ST | Status for each application or transition of state on interface (**S**tate **T**ransition) |
| 2 | MM | Management function for connect and disconnect LTE / 3G network (**M**odem **M**anager) |
| 3 | ES | Error which occurred on an application (**E**rror **S**tate) |
| 4 | FS | Fail-safe function (**F**ail **S**afe) |
| 5 | WD | Self-diagnosis for process (software **W**atch-**D**og) |
| 6 | EV | Events operated by user (**E**vent) |
| 7 | OW | Other events which are not relevant to above (**O**ther**W**ise) |

- *Record contents*

  Descriptions for record data. This item can be specified unique strings.

[Example]

In case of first line displayed in Figure 3.5 Analysis for maintenance event log window, Maintenance event log function refers the standard output log from system application and creates below record data if strings “coreapp_startup system” (indicates startup of system application) is contained in the standard output log within target period.

YYYY/MM/DD hh:mm:ss (Timestamp) system ST Started “system”

Moreover, this function can specify multiple string for detection to same application. By clicking “Add Line”, additional string for detection, record type and record content can be specified. (For example, in case of figure3.5, two rules of maintenance event log for router application are specified at line 2 and line 6). A process for creating maintenance event log executes standard error output and save (output) it to external file as maintenance event log.

ii) Analyze maintenance event log

This process refers a standard output log from other applications, checks whether string for detection is contained in the log or not, judge a presence of a prescribed event (execute / reboot other application, connect / disconnect LTE network etc) and creates a record which is used for outputting to a maintenance event log at event detection.

The standard output log is described as shown below. Log data is added in series, and each log normally includes timestamp.

<Example of standard output from system application>

[2021-06-08T07:48:30.061+00:00]coreapp_startup system

[2021-06-08T07:48:30.088+00:00]coreapp_startup supvis

[2021-06-08T07:48:30.100+00:00]coreapp_startup router

…

[2021-06-08T07:48:31.306+00:00]2021-06-08 07:48:31: (server.c.1521) server started (lighttpd/1.4.54)

This process refers a standard output log which is output in a period between previous start analyzing time to current start analyzing time, judge a presence of a prescribed event.

If the event is detected this process generates each event information as a record.

[Analysis condition]

A condition for analysis is defined by GUI as described in Figure 3.5 Analysis for maintenance event log window.

Setting items for analyses maintenance event log are condition ID, application ID, record type and record contents.

- *Condition ID*

  An ID information for recognizing an analysis condition. ID can be set unique string but describing EL (Event Log) to the beginning of ID is recommend.

- *Application ID:*

  Specify target application for referring standard output log.

  Maintenance event log refers standard output log from applications installed in this product.

- *Record type*

  Specify type of record. A list of record types is shown in Table 3.115 **Support functions on this product**.

- *Record contents*

  Descriptions for record data. This item can be specified unique strings.

[Example for analysis]

This function refers a generated event log and analyses whether the log data contains record contents according to the analysis condition setting. Example is shown below.

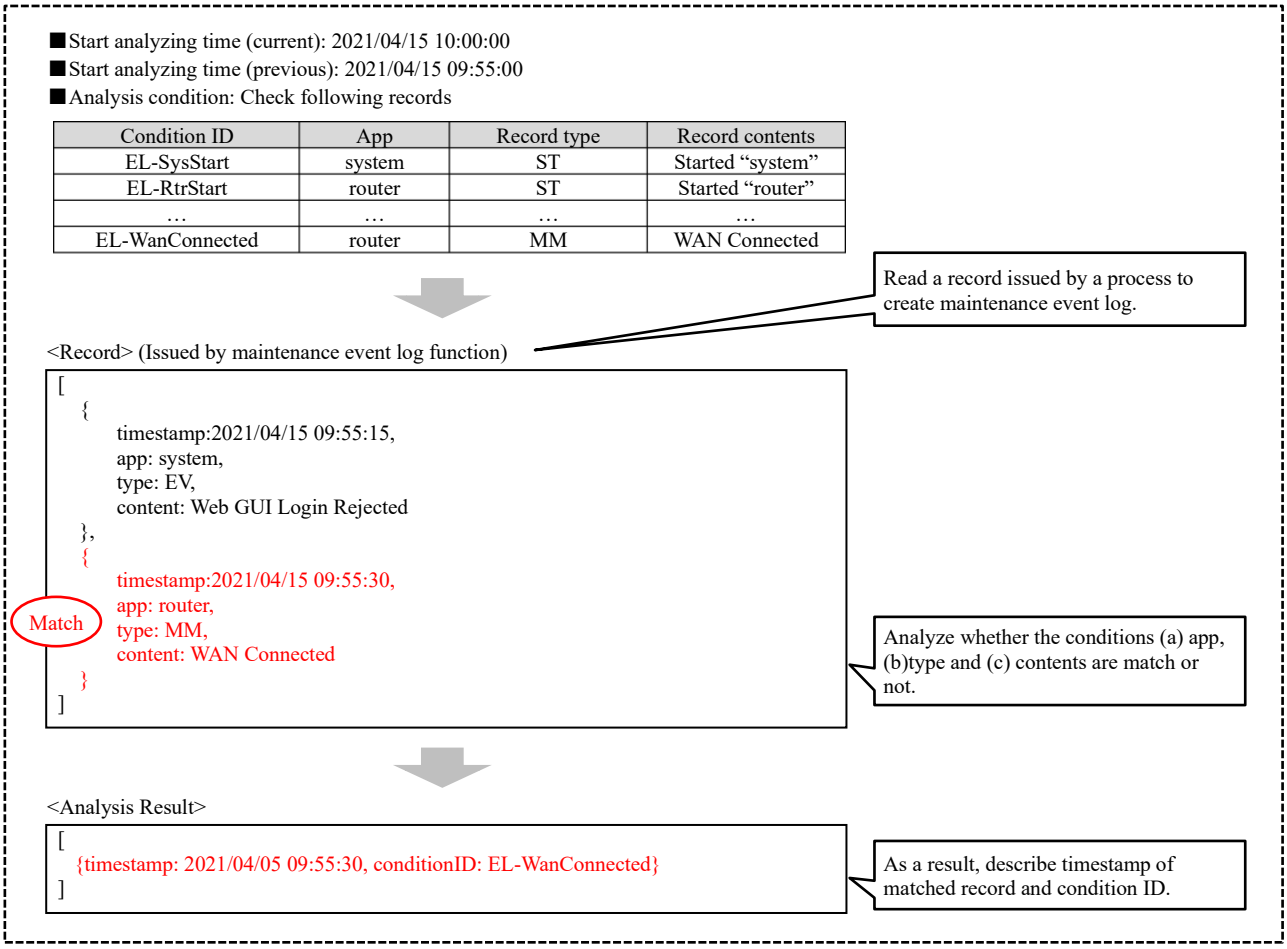



**Figure 3.6 Example of Analyzing maintenance event log**

- [Step 1] Read a maintenance event log
  - Read a record issued by a process to create maintenance event log
  - If the record is not exist, move “analyze operation status” process. If it’s existed, this process analyses the record as step 2.

- [Step 2] Analyze the record with the conditions
  - Analyses the record read at step 1 whether the conditions are matched or not.
    Analysis condition is defined by combination of (a) app, (b)type and (c) contents.
    If (a), (b) and (c) are satisfied, it treats as “condition is match”.
    On Figure 3.6 Example of Analyzing maintenance event log, red description is the record which is matched by condition.
  - Each analysis condition can be defined by unique condition ID. If a record which is matched by analysis condition, timestamp of record and condition ID are recorded as an analysis result.
    An analysis result created in JSON format. The result is recorded in array type to record multiple results as shown below.

<Format of analysis result>

```
[
    {timestamp: (timestamp of record), conditionID: (condition ID)},
    {timestamp: (timestamp of record), conditionID: (condition ID)},
    …
]
```

iii) Output maintenance event log

Specification of this function is shown below.

Record format: [timestamp app type contents]

- *Timestamp*

  A timestamp of event detection. This item is referred form standard output log of each application. If timestamp is not contained in the standard output log, start analyzing time is used as timestamp of event detection.

- *Application ID:*

  Specify target application for referring standard output log.

  Maintenance event log refers standard output log from applications installed in this product.

- *Record type*

  Specify type of record. A list of record types is shown in Table 3.115 **Support functions on this product**.

- *Record contents*

  Descriptions for record data. This item can be specified unique strings.

[Example]

In case of first line displayed in Figure 3.5 Analysis for maintenance event log window, Maintenance event log function refers the standard output log from system application and creates below record data if strings “coreapp_startup system” (indicates startup of system application) is contained in the standard output log within target period.

YYYY/MM/DD hh:mm:ss (Timestamp) system ST Started “system”

Moreover, this function can specify multiple string for detection to same application. By clicking “Add Line”, additional string for detection, record type and record content can be specified. (For example, in case of figure3.5, two rules of maintenance event log for router application are specified at line 2 and line 6). A process for creating maintenance event log executes standard error output and save (output) it to external file as maintenance event log.

2) Analyze operation status

i) Analyze operation status

This process refers operation status managed by other applications and check presence of internal status which matches analysis conditions.

As examples of internal status which should be detected are “IP address on LAN interface is not distributed” or ”RSRP (Reference Signal Received Power) on LTE is lower than threshold”.

Example of analyze operation status is shown in **Figure 3.7 Example of Analyzing operation status**. Flow of analysis is shown below.

- [Step 1] Refer operation status from other application

  Refer current value of each operation status defined by analysis condition from other application.

  - In case of **Figure 3.7 Example of Analyzing operation status**, this process refers “LAN IP address” and “RSRP” from router application, refers “number of active connections on TCP” from resource application.
  - Method of referring operation status from other applications is to send GET request to internalio application. This is the same as iopoll application.

- [Step 2] Analyze operation status with the conditions

  - Analyze the operation status whether the conditions are matched or not.
  - As described on Figure 3.7, analysis condition is not only comparison of simple value (absolute comparison) but also increase / decrease amount from previous value (relative comparison) or number of continuous matchings.

    To judge several conditions, “previous value” and “number of continuous matchings” are retained for each analysis condition. Number of continuous matchings is cleared to 0 at condition unmatching.

    - Example of relative comparison:

      Number of connections managed by router application is accumulated value from startup, not number of current connections. If absolute comparison is used for this value, the value exceeds threshold in long running even if it’s running in normal operation. In this case, relative comparison is necessary.

- Example of continuous matchings:
  In an LTE connection, RSRP value temporarily decreases if some obstacles appear between this product and base station. If a detection is applied to this value every time, number of error report increases. In this case, it is better to watch this value for certain of time. So “RSRP value is continuously lower than threshold three times” is proper condition for monitoring.

◆ A condition ID is set for each analysis condition as described on Figure 3.7. If analysis condition is existed, timestamp and condition ID are recorded as an analysis result.

- Description format of analysis result is the same as analyze maintenance event log. However, timestamp is start analyzing time since analyze operation status is analysis for current value.

<Format of analysis result>

```
[
    {timestamp: (start analyzing time), conditionID: (condition ID)},
    {timestamp: (start analyzing time), conditionID: (condition ID)},
    …
]
```

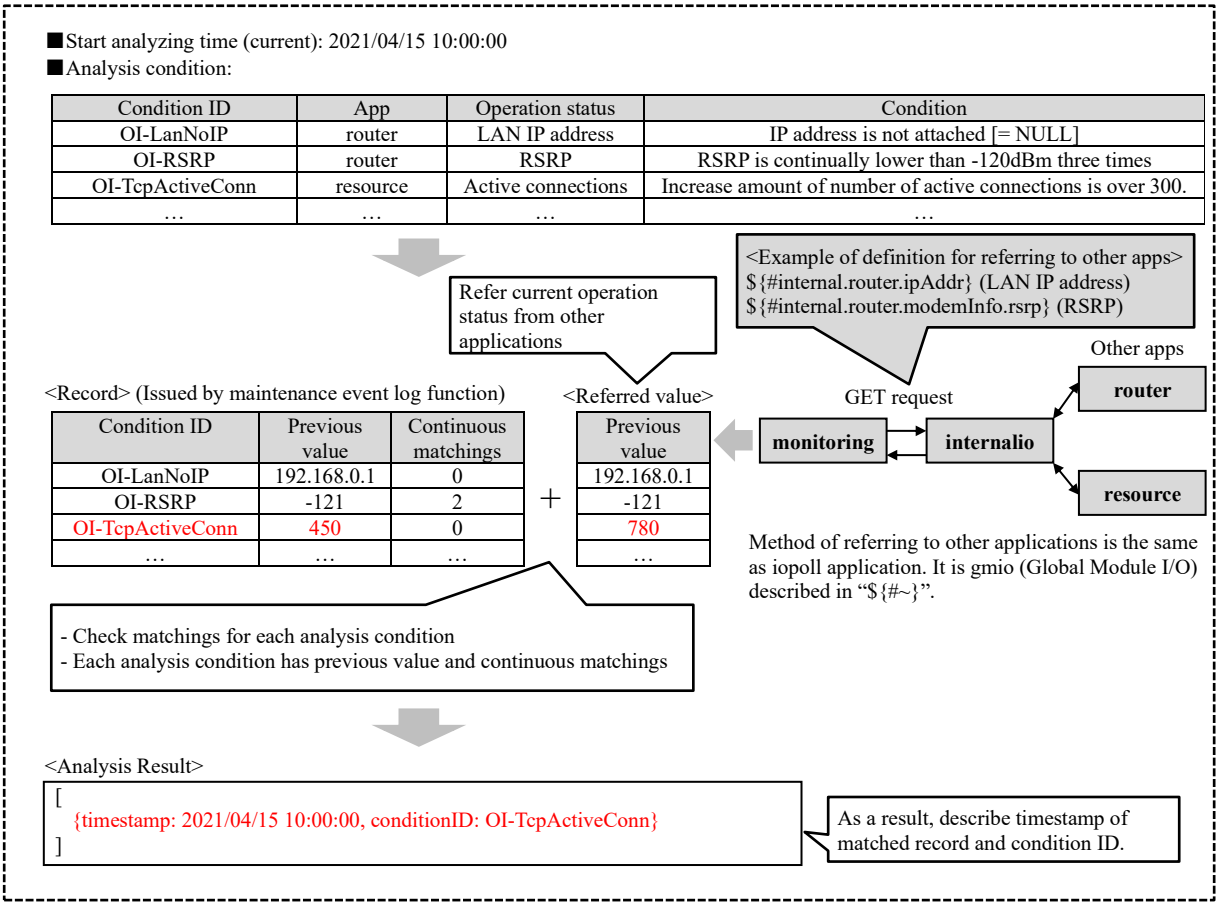



**Figure 3.7 Example of Analyzing operation status**

ii) Define analysis condition for operation status

GUI for analysis operation status is shown on Figure 3.8 **Definition of analysis operation status window** Analysis conditions are specified by setting window. Specified analysis conditions are loaded at startup of this application.

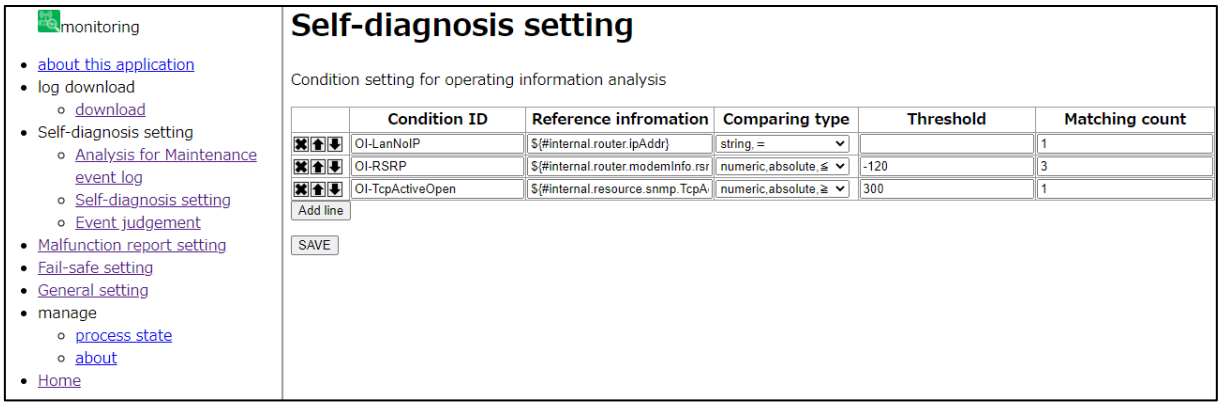



**Figure 3.8 Definition of analysis operation status window**

Each item of setting table is described below.

- *Condition ID*

  An ID information for recognizing an analysis condition. ID can be set unique string but describing OI (Operating Information) to the beginning of ID is recommend.

- *Reference information:*

  Specify operating information from other application. Method of referring to other applications is the same as iopoll application. It is gmio (Global Module I/O) described in "${#~}".

  ${#internal.(application name).(ID described in manifest file)}

- *Type*

  Specify a condition for comparing. Setting items are (a) comparison type, (b) value type and (c) sign of inequality.

  - **(a) Comparison type:** Specify threshold value for comparing as "strings" or "value".
  - **(b) Value type:** Specify threshold value type for comparing as "absolute" or "relative". "Absolute" treats current value without any calculations. On the other hand, "relative" calculates amount of change between current value and previous value. Calculation is "Current – Previous" and calculated value is treated as plus if the amount of change is increased, treated as minus if the amount of change is decreased. "Relative" is available only for "value" comparison.
  - **(c) Sign of inequality:** Specify a condition of comparison in sign of inequality.

  A list of combination of above items is shown below.

**Table 3.116 List of type for analysis condition**

| # | Items | Description |
|---|---|---|
| 1 | numeric, absolute, ＝ | Value is equal to threshold (absolute) |
| 2 | numeric, absolute, ≠ | Value is NOT equal to threshold (absolute) |
| 3 | numeric, absolute, ≧ | Value is threshold or higher (absolute) |
| 4 | numeric, absolute, ≦ | Value is threshold or lower (absolute) |
| 5 | numeric, absolute, > | Value is more than threshold (absolute) |
| 6 | numeric, absolute, < | Value is less than threshold (absolute) |
| 7 | numeric, relative, ＝ | Value is equal to threshold (relative) |
| 8 | numeric, relative, ≠ | Value is NOT equal to threshold (relative) |
| 9 | numeric, relative, ≧ | Value is threshold or higher (relative) |
| 10 | numeric, relative, ≦ | Value is threshold or lower (relative) |
| 11 | numeric, relative, > | Value is more than threshold (relative) |
| 12 | numeric, relative, < | Value is less than threshold (relative) |
| 13 | string, ＝ | Value is equal to threshold (string) |
| 14 | string, ≠ | Value is NOT equal to threshold (string) |

- *Threshold*

Threshold value for comparison against value. If the comparison is numeric, specify numeric value, and specific string if the comparison is string. Comparison is proceeded between value and this threshold according to a condition.
For example, as shown on Figure 3.7 **Example of Analyzing operation status**, if IP address on LAN interface is not allocated, result of referring from router application is null (no value). Therefore, specifying null is available as shown on Figure 3.8 **Definition of analysis operation status window** (column at Condition ID: OI-LanNoIP).

- *Matching count*

  Specify number of continuous matchings of above matching condition. If number of continuous matchings is this value or higher, this analysis condition is satisfied (true).
  For example, if an analysis condition is “RSRP value is continuously lower than -120dBm three times”, specific 3 to this item. In this case, analysis condition is satisfied when it is continuously detected that RSRP value is lower than -120dBm in three times, and analysis condition is not satisfied even if this detection occurs continuously two times.

3) Analyze operation status

In this section, “Event judgement” as shown on Figure 3.4 Flow-chart of monitoring application is described.

[Details of process]

This processes judges whether an event should be issued to “Malfunction report” and “Fail-safe” functions or not, based on analysis results from “Analysis maintenance event log” and “Analysis operating information”. Flow chart of this process is displayed on Figure 3.9 .

- [Step 1] Refer maintenance event log and analysis results

  Refer JSON format of analysis results for maintenance event log and operating information.

  - In case of Figure 3.9 , two condition IDs “EL-WanConnected” and “OI-TcpActiveOpen” are matched.

- [Step 2] Detect events based on analysis conditions

  - As described on Figure 3.9 , two types of event condition are managed, (a) a list of events which should be reported to “Malfunction report” or “Fail-safe”, (b) event trigger for analysis conditions.

    Matching condition IDs can be multiply specified to each event. For example, at column event ID: LackRxCapabiliy on Figure 3.9 , “lack of capability for receiving” on this product is detected if two conditions “rising of CPU load” and “number of drops of receiving packets” are satisfied.
    As above, if multiple conditions are specified, judgment is proceeded by AND condition.

- Detect event conditions based on information from matching condition IDs and above event conditions.
  If an event which satisfies event conditions is exist, issues a combination of timestamp at event detection, and detected event ID, to “Malfunction report” and “Fail-safe” as a judged result in JSON format. Timestamp is used from a timestamp contained in matching condition.
  If an event is detected by multiple condition, latest timestamp is used among matching condition IDs as described on Figure 3.9 .

<Format of judgement result>

```
[
    {timestamp: (event detected time [timestamp of matching condition ID]), eventID: (event ID)},
    {timestamp: (event detected time [timestamp of matching condition ID]), eventID: (event ID)},
    …
 ]
```

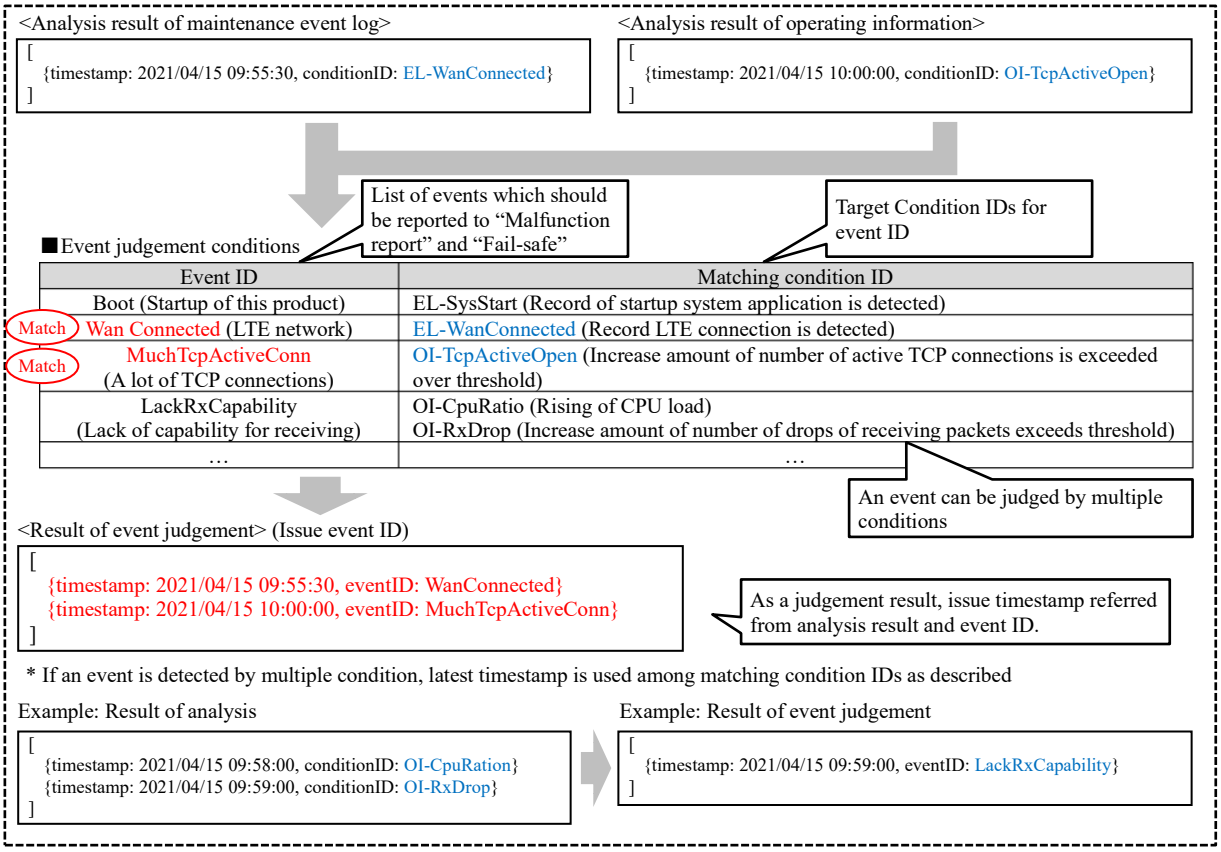



**Figure 3.9 Example of event judgement**

[Setting for event judgement condition]

A GUI window I for setting event judgement condition is shown on Figure 3.10 **Setting for event judgement window**.

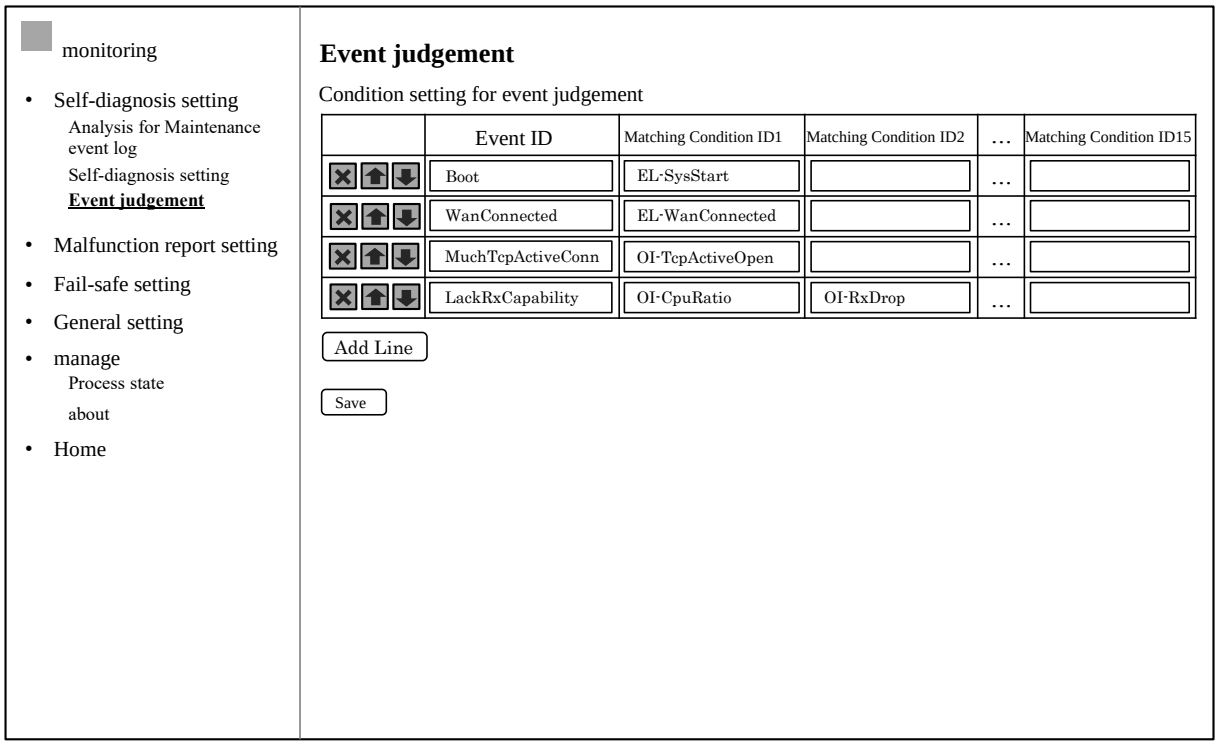



**Figure 3.10 Setting for event judgement window**

Each item settings are described below.

- *Event ID*

  An ID information for recognizing an event condition. ID can be set unique string. Events which are error or needed to report to the management server should be defined in this setting. In case of reporting events to "Malfunction report" or "Fail-safe", it is also necessary to define in this setting.

- *Matching condition ID*

  Specify condition ID for matching to each event defined at event ID setting item. Condition IDs are used from defined IDs which specified at Figure 3.5 Analysis for maintenance event log window or Figure 3.8 **Definition of analysis operation status window**

  Event judgement treats as “true” if all condition IDs are satisfied. If single condition ID is used, specific the condition ID to item “Condition ID 1” and specific null to other

condition ID items. On the other hand, if condition IDs are multiply used, specify condition ID from “Condition ID 2” to onward.

#### 3.2.21.2 Malfunction report

This function is currently not supported.

#### 3.2.21.3 Fail-safe

This function executes reboot to each application or system on this product based on detected event information issued by “Self-diagnosis”.
Detailed specification of this function is explained from next chapter.

#### 3.2.21.4 Appending maintenance event log

This chapter explains a process for appending maintenance event log shown on Figure 3.4 Flow-chart of monitoring application.
[Details of this process]
If reboot action is proceeded without this process, it’s not possible to recognize “reboot due to unexpected behavior” or “reboot by fail-safe function”. To avoid this case, this process appends record which describes “reboot by fail-safe to maintenance event log.
This process has following setting items for self-reboot action.

**Table 3.117 Setting items for fail-safe (self-reboot) function**

| # | Items | Description |
|---|---|---|
| 1 | Event ID | Specify event ID for self-reboot. Event IDs are defined at self-diagnosis function. |
| 2 | Reboot Application ID | Specify whether this function execute reboot or not when event ID is issued. To execute system reboot, specify “system”. |
| 3 | Record contents | Specify record content to indicate that purpose of reboot is fail-safe. This item can be set for each event ID. |
| 4 | Reboot inhibit time(min.) | Specify wait time to start reboot application when above event ID is issued. Purpose of this setting is to avoid unexpected behavior due to immediately reboot at issuing event ID. |

Example of setting is described on Figure 3.11 **Example of fail-safe setting**
This example specifies self-reboot settings for recovering this product when illegal events “a lot of TCP connection occurred” and “IP address on LAN interface is not allocated”. When “a lot of TCP connection occurred” occurs, system reboot is executed because it is not possible to clear this error by reboot of single application. On the other hand, when “IP address on LAN interface is not allocated” occurs, reboot is executed for only router application to re-allocate LAN IP address.
Each record contents are specified to record information of rebooting application and reason of reboot. Record contents can be specified unique string and other items need to be set fixed parameters.

Record format: [Timestamp, application, type, contents]

- *Timestamp*
  Current time information. To recognize a record which is appended after reboot, this process uses timestamp which pasts at least a second or longer from analyzing start time.
- *Application:*
  An application name of reboot target by fail-safe function.
- *Type*
  Specify “FS” for this function. It indicates that this record is related to fail-safe function.

On Figure 3.11 **Example of fail-safe setting**, “event ID: MuchTcpConn” is matched ID which needs a self-reboot function. Therefore, record which should be recorded to maintenance event log is appended based on setting items target application name for self-reboot and record contents.

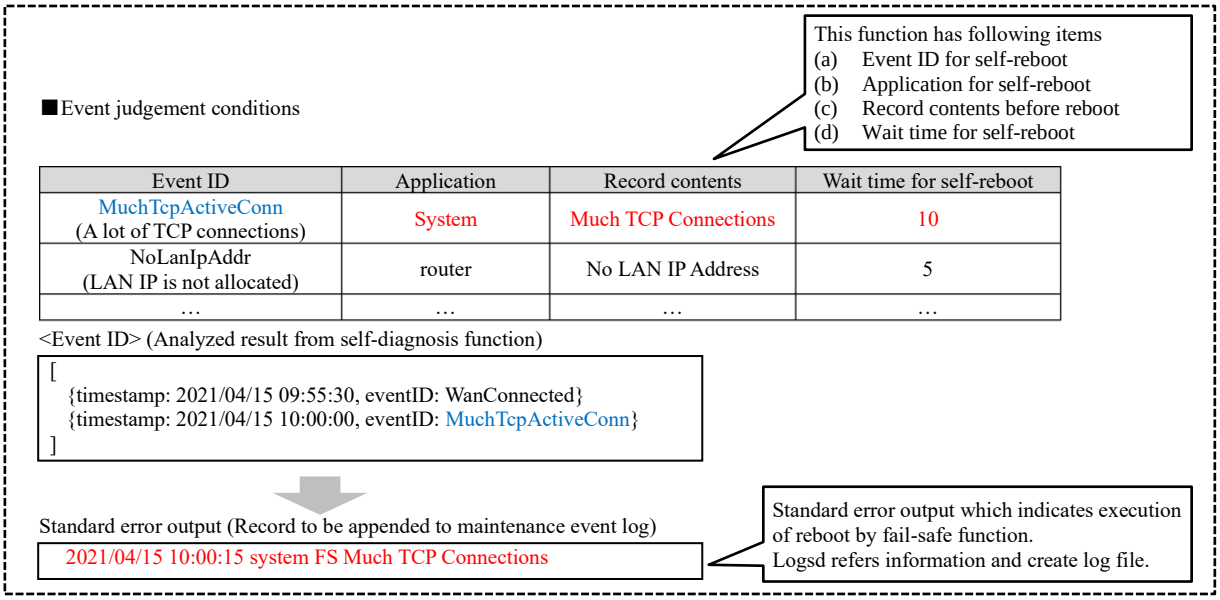



**Figure 3.11 Example of fail-safe setting**

[Setting for self-reboot]

A GUI window for fail-safe setting is shown on Figure 3.12 **Setting for** .

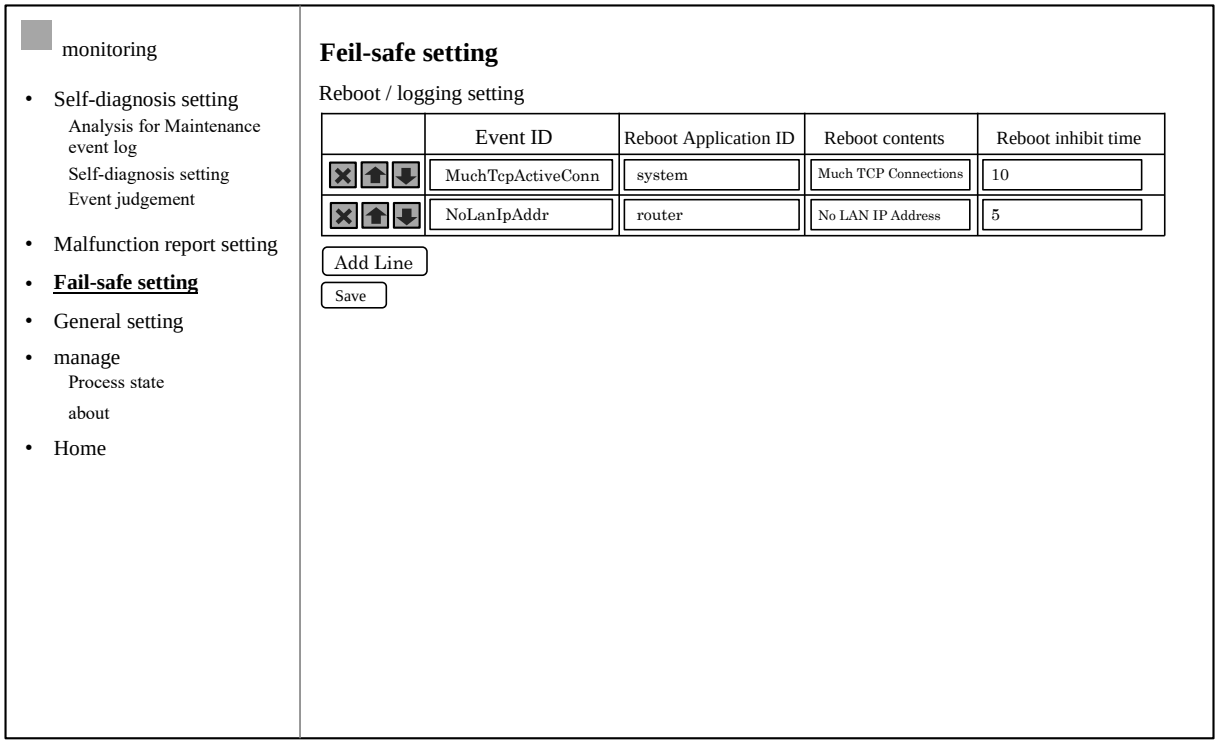



**Figure 3.12 Setting for fail-safe**

Specify items event ID, application name, record contents and reboot inhibit time. A single event ID can reboot one or more applications. By clicking “Add Line”, same event ID and different application can be specified. For the applications which are not necessary to reboot, setting at this window is not necessary.

[Execute application or this product itself]

A process for execution of applications or this product itself is described in below.

[Specification of process]

Reboot process is executed after appending a record which indicates execution of reboot by "appending maintenance event log". Target application name and reboot inhibit time are already defined at Figure 3.12 **Setting for** .

Processes after executing reboot works as following.

- *Event ID is not exist, or execution is successful except system application*

  In this case, this application continues running without reboot itself. Next monitor and analysis process start when certain time has passed as described on Figure 3.4 Flow-chart of monitoring application

- *system application is rebooted*

  In this case, this application is also rebooted. Process starts from the top (load setting files) as displayed on Figure 3.4 Flow-chart of monitoring application

#### 3.2.21.5 Log download function

Log data from this application can be stored to SD card and downloaded it from Web GUI.

**Table 3.118 Supported log types**

| # | Log type | Description |
|---|---|---|
| 1 | Maintenance event log | Log data generated at analysis maintenance event log |
| 2 | Operating information log | Log data generated at analysis operating information log |
| 3 | Application reboot log | Log data generated at reboot request is issued |

(1) Output path

Log data is output to SD card. Path is different from logsd application.

Output path: /media/sdcard/monitor_log/

Output format is described below.

- Format

  [SEQ]-[yymmdd]T[HHMMDD].log

- Description

  [SEQ]:

  Unique number start from 0. Number is incremented for every file created.

  This application refers folder for log data and obtains maximum number of SEQ. Obtained number plus 1 is start SEQ number when this application start running.

  [yymmdd]:

  Date at file generated. yy=year (two digit) mm=month dd=day “T”: fixed character.

  [HHMMSS]:

  Date of time at file generated. HH=hour MM=minute SS=second “.log”: discriminant.

[Caution]

- If this product is not time synchronized, “[yymmdd]T[HHMMDD]” becomes “temp” (fixed characters).
- Time synchronization is judged by following condition.

  System time >= 2000/01/01 0:00:00

(2) Restriction for log output

Log data is not output in following condition.

- SD card cannot be detected at application start running.
- Log output setting is disable.

Log output doesn't start even if SD card is available after application running.

(3) Log rotation and management

Log files are rotated and managed as following rules.

- Setting item "maximum file size per a file" is referred at start application.
- If file size exceeds above setting, new log file is generated.
- Maximum number of log files is depending on file system of SD card. This application doesn't manage number of log files.
- If number of log files exceeds the maximum on SD card, this application doesn't create additional log files.

(4) Download log files

Log files created from this application can be downloaded by Web GUI. A list of log files is shown at windows if "download" is selected on Web GUI. By clicking a log file name, downloading the log file starts.

### 3.2.22 Common function in each application

This product supports following function as common function of each application.

**Table 3.119 Common function of each application**

| # | Function | Description | Remarks |
|---|---|---|---|
| 1 | Status monitor | Monitor operating status of application. | |
| 2 | Log output | Monitor log output of operating application. | |

#### 3.2.22.1 Status monitor

This product supports to output each application status.

Status display items are shown in Table 3.120.

**Table 3.120 Status monitor**

| # | Function | Details | Note |
|---|---|---|---|
| 1 | Application info. | Show version and identification information of each application. | |
| 2 | Operating process | Show status of application process ID and its operating condition. | |
| 3 | Memory information | Show Max memory use, Current memory use, and other memory information. | |
| 4 | CPU Time [Second] | Show CPU operating time of each system. | |

3.2.22.2 Log output

This product has function to output log information of each application. Log can be monitored on each application by WebGUI.
Log output monitor has two log outputs. Log1 (stdout) shows standard outputs and Log2 (stderr) shows standard error outputs. This product firmware supports to show Log2 outputs only.
(Log output details [Log level] can be changed from system log setting as per below.)

Standard output log (stdout):
Show log, message, and output data of each application (Not supported on this firmware)
Standard error log (stderr):

**Table 3.121 System log setting**

| # | Item | Specification | Note |
|---|---|---|---|
| 1 | Log level | Set log output level.<br>Level0: Show only critical error<br>Level1: Show caution notice<br>Level2: Show related information<br>Level3: Show trace information | Contact supplier for details of each log output. |
| 2 | Output | Only from WebGUI monitor | |

## 3.3 Other Functions

### 3.3.1 LED display

This product shows network status etc. on front LED display. LED display details are shown below.

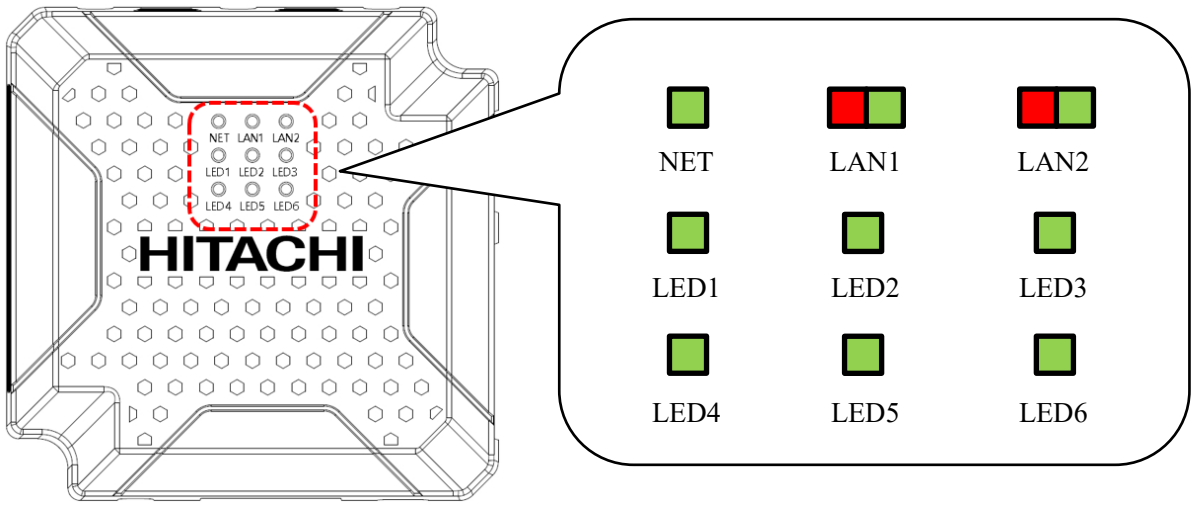



**Figure 3.13 LED display**

Table 3.122 LED display

| # | LED Name | Color showing | Details |
|---|---|---|---|
| 1 | NET | Green | WAN connection status.<br>Offline: light off<br>Connecting: Blinking<br>Online: Green light on |
| 2 | LAN1 | Green – Red | Show LAN1 (Ethernet1) port status.<br>Offline: light off<br>Linkup(100M): Green on (blinking during communication)<br>Linkup(10M): Red on (blinking during communication) |
| 3 | LAN2 | Green – Red | Show LAN2 (Ethernet2) port status.<br>Offline: light off<br>Linkup(100M): Green on (blinking during communication)<br>Linkup(10M): Red on (blinking during communication) |
| 4 | LED1 | Green | LTE signal strength<br>RSSI value < -90dBm [No connection – Weak]: Light off<br>RSSI value >= -90dBm [Acceptable – Strong]: Green light on |
| 5 | LED2 | Green | Power supply and software status.<br>No power: light off<br>Power on and software booting: blinking<br>Unit ready: light on |
| 6 | LED3 | Green | Show wireless LAN module status.<br>Wireless LAN module start up: Light off<br>Wireless LAN module activated: Green light on |
| 7 | LED4 | Green | Communication status on WAN interface<br>No data send: light off<br>Data sending: light on |
| 8 | LED5 | Green | Send status in serial communication<br>No data send: light off<br>Data sending: light on |
| 9 | LED6 | Green | Receive status in serial communication<br>No data receive: light off<br>Data receiving: light on |

1） Normal operation

LED display during normal operation steps is shown as below.

**Table 3.123 LED display (Normal operation)**

| # | LED pattern | | | | | | | | | Description |
|---|---|---|---|---|---|---|---|---|---|---|
| | NET | LAN1 | LAN2 | LED1 | LED2 | LED3 | LED4 | LED5 | LED6 | |
| 1 | OFF | — | — | — | — | — | — | — | — | WAN: Offline (disconnected) |
| 2 | G: Blink 1000ms Cycle | — | — | — | — | — | — | — | — | WAN: Connecting |
| 3 | G: ON | — | — | — | — | — | — | — | — | WAN: Online (Connected) |
| 4 | — | OFF | — | — | — | — | — | — | — | LAN1(Ethernet) Not connected |
| 5 | — | G: ON or blinking | — | — | — | — | — | — | — | LAN1(Ethernet) Link established (100M)<br>Blinking during communication |
| 6 | — | R: ON or blinking | — | — | — | — | — | — | — | LAN1(Ethernet) Link established (10M)<br>Blinking during communication |
| 7 | — | — | OFF | — | — | — | — | — | — | LAN2(Ethernet) Not connected |
| 8 | — | — | G: ON or blinking | — | — | — | — | — | — | LAN2(Ethernet) Link established (100M)<br>Blinking during communication |
| 9 | — | — | R: ON or blinking | — | — | — | — | — | — | LAN2(Ethernet) Link established (10M)<br>Blinking during communication |
| 10 | — | — | — | OFF | — | — | — | — | — | Signal strength: No signal or weak<br>RSSI value < -90dBm] |
| 11 | — | — | — | G: ON | — | — | — | — | — | Signal strength: Strong<br>RSSI value >= -90dBm] |
| 12 | — | — | — | — | OFF | — | — | — | — | No power supply |
| 13 | — | — | — | — | G: Blink 1000ms Cycle | — | — | — | — | From power or launching software (OS) |
| 14 | — | — | — | — | G: ON | — | — | — | — | Software launch has been finished |
| 15 | — | — | — | — | — | OFF | — | — | — | Wireless LAN: Disable |
| 16 | — | — | — | — | — | G: ON | — | — | — | Wireless LAN: Enable |
| 17 | — | — | — | — | — | — | OFF | — | — | No data sending in WAN connection |
| 18 | — | — | — | — | — | — | G: ON | — | — | Data sending in WAN connection |
| 19 | — | — | — | — | — | — | — | OFF | — | No data sending in serial communication |
| 20 | — | — | — | — | — | — | — | G: ON | — | Data sending in serial communication |
| 21 | — | — | — | — | — | — | — | — | OFF | No data receiving in serial communication |
| 22 | — | — | — | — | — | — | — | — | G: ON | Data receiving in serial communication |
| 23 | OFF | — | — | G: Blink 1000ms Cycle | G: Blink 1000ms Cycle | G: Blink 1000ms Cycle | G: Blink 1000ms Cycle | G: Blink 1000ms Cycle | G: Blink 1000ms Cycle | Initializing parameter on this unit (Factory resetting) |

2） Irregular operation

LED display during irregular operation is shown as below.

**Table 3.124 LED Display (Irregular operation)**

| # | LED pattern | | | | | | | | | Description |
|---|---|---|---|---|---|---|---|---|---|---|
| | NET | LAN1 | LAN2 | LED1 | LED2 | LED3 | LED4 | LED5 | LED6 | |
| 1 | — | — | — | — | — | — | G: Blink 1000ms Cycle | — | G: Blink 1000ms Cycle | USIM Error (No SIM, PIN LOCK, PIN BLOCK) |
| 2 | — | — | — | G: Blink 1000ms Cycle | — | — | — | — | — | IP address error (IP address overlapping with this product in same network) |
| 3 | G: Blink 1000ms Cycle | — | — | G: Blink 1000ms Cycle | G: Blink 1000ms Cycle | G: Blink 1000ms Cycle | G: Blink 1000ms Cycle | G: Blink 1000ms Cycle | G: Blink 1000ms Cycle | Communication module error (Communication between Sub-processor and module cannot be detected in certain period) |

### 3.3.2 Watchdog

This product supports Watchdog function which monitor software operation status by itself and in case any irrecoverable error occurs, it reboots automatically. Process is explained as per below.

**Table 3.125 Watchdog function**

| # | Item | Checking operation |
|---|---|---|
| 1 | Monitor on watchdog timer | Monitored system by standard Linux watchdog timer. If watchdog timer is not updated, this unit start reboot process and restart its operation. |

### 3.3.3 Auto registration of connected address

This unit generates connected address setting and registers it automatically. Information for connect address setting is read from USIM.

[Notice]: Connected address setting is generated as per below.

APN and password: User settings will be applied. In case no change, it will use factory initial value.

Username: Automatically generate from USIM information, User setting value will overwrite when this function activates.

[Sample]:

ICCID of USIM = 8981300022643909801

Username of APN setting ＝${mid8,11:${ICCID}}@hitachi-ies.jp

* In case above setting (underline area) is applied, 8th to 18th letter will be used from ICCID.

For above sample, value which is applied on LTE connection shall be 02264390980@hitachi-ies.jp.

### 3.3.4 Communication packet counting

This product provides communication packet counting function, which count receive / sent packet number gone through this product. This product can also monitor each amount. Details of packet counting is shown below.

**Table 3.126 Communication packet counting**

| # | Item | Specification |
|---|---|---|
| 1 | Applicable I/F | GUI (WEB monitor) |
| 2 | Countable network | WAN, LAN(Ethernet) |
| 3 | Counting | Count packet number and data size [byte] of each network for sending (This product ➔ External network) & receiving (External network ➔ This product). |
| 4 | Count start timing | Receive packets from LAN start counting when it is sent out to WAN. Receive packets from WAN is count at the timing of receipt. |
| 5 | Note | Packets count is used as reference value. |

### 3.3.5 Time Synchronization

This product automatically synchronizes clock information within its carrier network.

4. Management port specifications

This product is equipped with a management port as an operation function by the CLI. Because the management port works as a TCP server, it can be connected from a general terminal software. After connecting to the management port, AT commands is available to set the product, acquire information, and control operations.

The management port can be connected from both the LAN side and the WAN side. However, because multiple sessions are not supported, simultaneous connections from both sides are not possible.

*To access from the WAN (LTE network), the router application needs to be configured to allow communication to the management port in the security settings (access control settings).

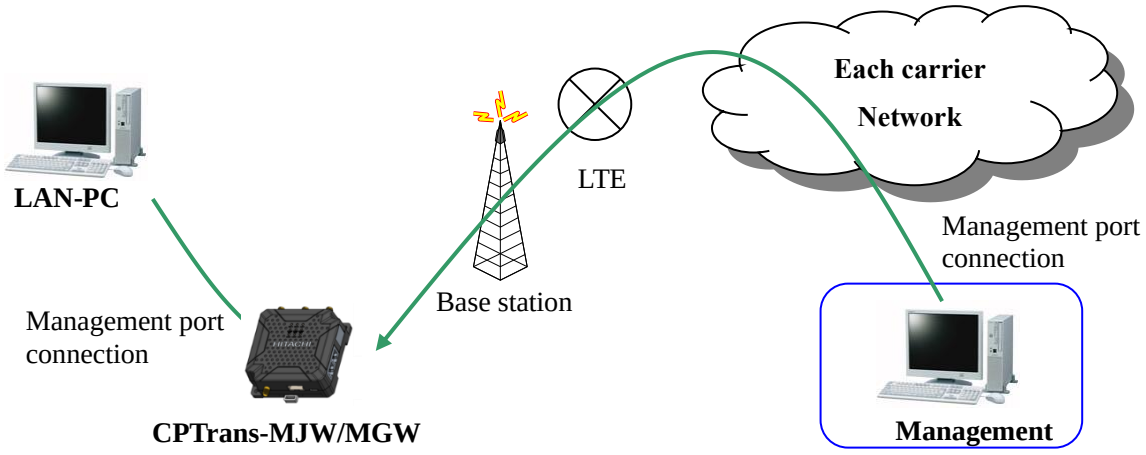



**Figure 4.1 System overview of the management port connection**

The factory default settings for the management port are as follows:

**Table 4.1 The factory default setting for the management port connection**

| Item | Default setting |
|---|---|
| Protocol | TCP |
| LAN side IP address | 192.168.101.1 |
| Port number | 20000 |
| Password Authentication | manager |

*Details of commands are described in a separate document. Refer to the separate "[CPTrans-MJW_MGW] Command Reference manual".

*Please change the password above from the initial value before operating this product.

5. Web server specifications

This product has a Web server function to support operation by GUI. This allows to set various settings, display information, and control operations by a general-purpose web browser.

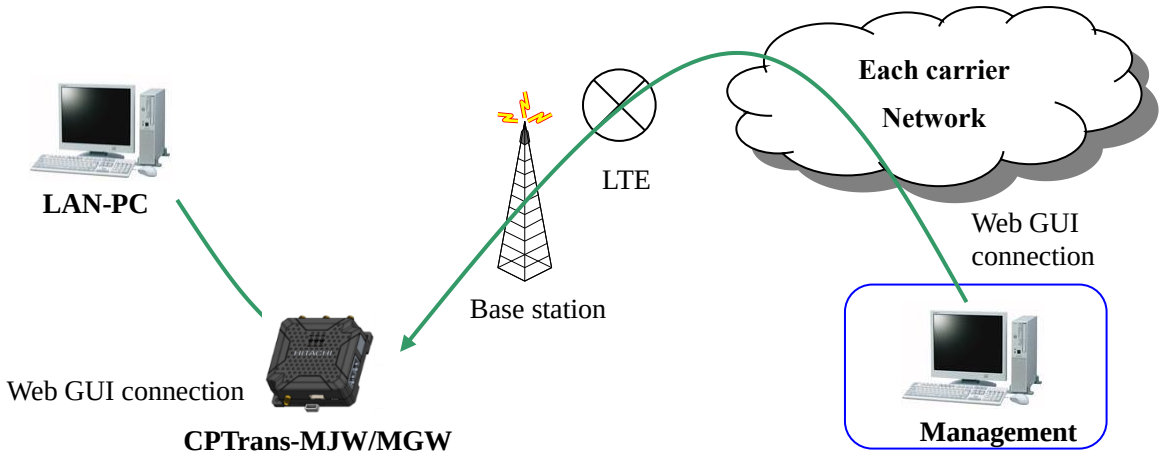



**Figure 5.1 System overview of the Web server connection**

Connections to the Web server can be made from both the LAN side and the WAN side.

*Access from the WAN (LTE network) is secured by the router application. (Access control setting) needs be set to enable communication to Web GUI.

Table 5.1 lists the factory default settings for the Web server.

**Table 5.1 the factory setting of the Web server**

| # | Item | Default setting |
|---|---|---|
| 1 | Protocol | TCPs (acting as HTTP servers) |
| 2 | LAN side IP address | 192.168.101.1 |
| 3 | Port number | 80 |
| 4 | Authentication function | Enabled |
| 5 | Username | admin |
| 6 | Password | manager |

*Please change the above username and password from the initial value before operating this product.

## 5.1 Connecting to the Web Server

① To connect from the LAN, enter the following URL in the URL entry field of the browser of the LAN side PC.

| |
|---|
| http://192.168.101.1/ |

② When a connection to the Web server is established, the user authentication screen is displayed. Enter in half-pitch as shown below.

| |
|---|
| Username: admin<br>Password: manager |

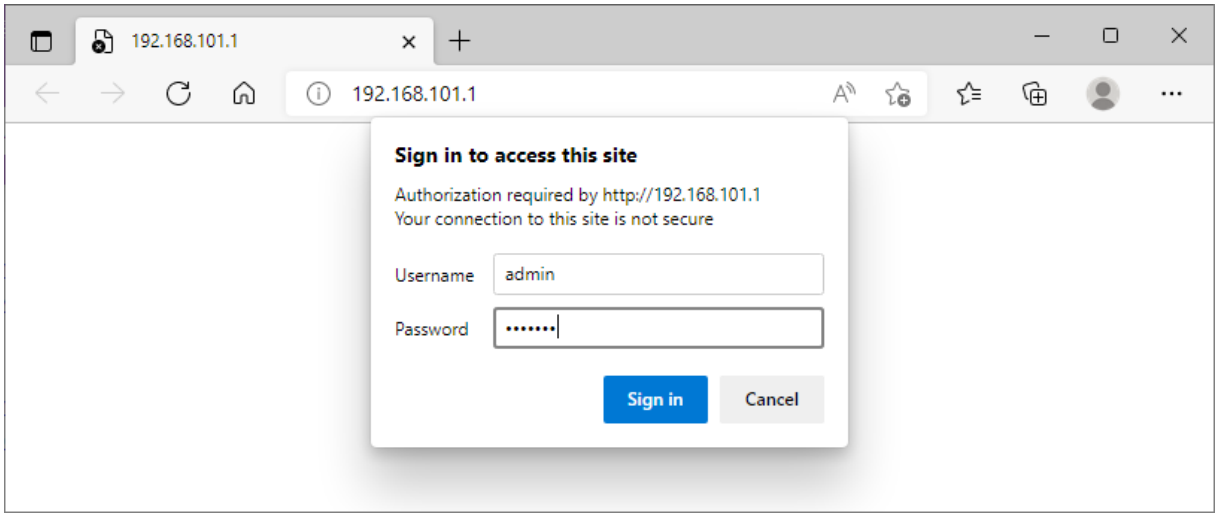



**Figure 5.2 Login window**

[Caution]

Please change the username and password of the Web server from the initial value before using.

③ When authentication is successful, the main window is displayed as shown below.
When connecting from the WAN side, specify the IP address assigned to the WAN side at the time of wireless connection to the IP address of the URL.
If the IP address and port number have been changed from the factory default settings, specify the new IP address and port number.


**Figure 5.3 Main window**

[Notice]

For example, if the LAN IP address is changed from 192.168.101.1 to 172.16.0.1 and the Web server port number is changed from 80 to 8080, enter the following URL in the LAN PC.

| http://172.16.0.1:8080/ |
|---|

## 5.2 Items that can be operated by the web browser

Table 5.2 lists the items that can be operated from a web browser.

**Table 5.2 List of items that can be set with a web browser (1 of 2)**

| Application | Function | | Remarks |
|---|---|---|---|
| System | CLI setting | | |
| | Web GUI Setting | | |
| | SIM pin lock setting | | |
| | Device unique information | | |
| | Misc setting | | |
| Router | LAN Settings | IP address setting | |
| | | DHCP / DNS | |
| | | DHCP server allocation status | |
| | Ether setting | Ether port setting | |
| | | Ether port status | |
| | Wireless LAN setting | Basic setting | |
| | | Setting | |
| | | Access control | |
| | | Connection status | |
| | WAN setting | Basic setting | |
| | | APN | |
| | | Modem status | |
| | Packet forwarding setting | NAT, NAPT, DMZ | |
| | | Ping response setting | |
| | | Static routing settings | |
| | Security settings | Firewall | |
| | | Access control | |
| Scheduled reboot | basic setting | Basic setting | |
| | | Reboot time points setting | |
| | | Status | |
| | | Do not Reboot during APN connection | |
| Update | Manual Update | | |
| | Automatic update | Basic setting | |
| | | Execution | |
| | | Status | |
| SMS | Basic settings (SMS action rules) | | |
| | SMS received log | | |
| Proxy | Basic Settings (Application Proxy Function Enable/Disable) | | |
| NTPd | Basic setting (NTP server function enable/disable) | | |
| DDNS general | Basic setting | | |

Table 5.3 List of items that can be set with a web browser (2 of 2)

| Application | Function | | Remarks |
|---|---|---|---|
| Ping checker | Basic setting | Enable ping checking | |
| | | Ping rules | |
| | Status | Ping results | |
| Location | Basic setting | | |
| Iopoll | Connection config | | |
| Modbusio | MODBUS-RTU(RS485) | | |
| | MODBUS-RTU(RS232) | | |
| | MODBUS-TCP | | |
| | Connection destination device setting | | |
| Mqttio | Retry and backup setting | | |
| | Certificates setting | | |
| | MQTT Settings | | |
| RESTio | Retry and backup setting | | |
| | Certificates setting | | |
| | REST setting | | |
| 232 through | RS232 Setting | | |
| | TCP connection setting | | |
| 485 through | RS485 Setting | | |
| | TCP connection setting | | |
| Datamanager | Basic setting | | |
| | Event Settings | | |
| | Modbus Settings | Modbus Settings | |
| | | Modbus communication status | |
| | Buffer setting | Data buffer setting | |
| | | Buffer state | |
| | Trigger setting | | |
| | Individual data setting | Individual data setting | |
| | | Individual data state | |
| | Payload setting | Payload setting | |
| | | Payload Communication Status | |
| Logsd | Basic setting | | |
| Monitoring | Log download | | |
| | Self-diagnosis setting | | |
| | Malfunction report setting | | |
| | Fail-safe setting | | |
| | General setting | | |

* Item settings can be set by web browser can also be set by management port command (CLI).

## 5.3 system

System applications are described below.

| Icon | Overview |
|---|---|
|  | An application that manages all applications.<br>This is also an application for setting GUI and CLI passwords. |

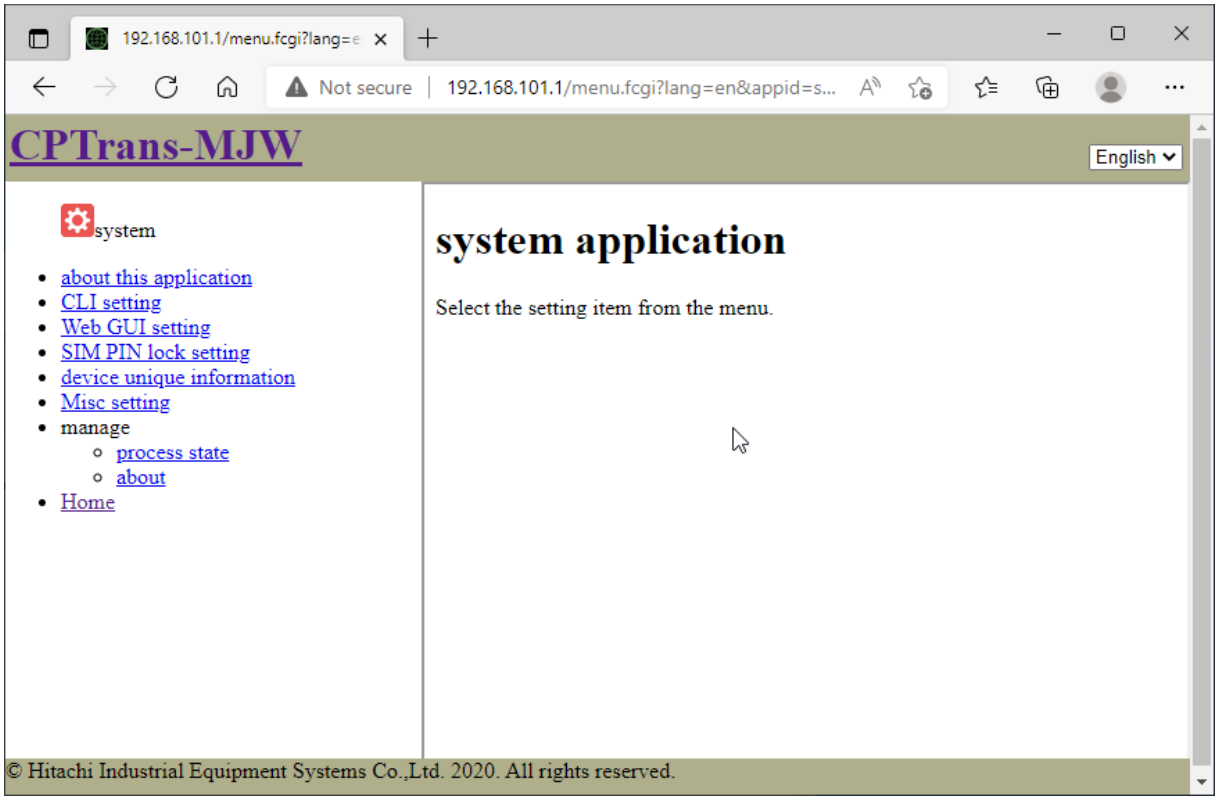



**Figure 5.4 Initial window of system application**

### 5.3.1 CLI Settings

This product can be controlled by command using TP/IP sockets.

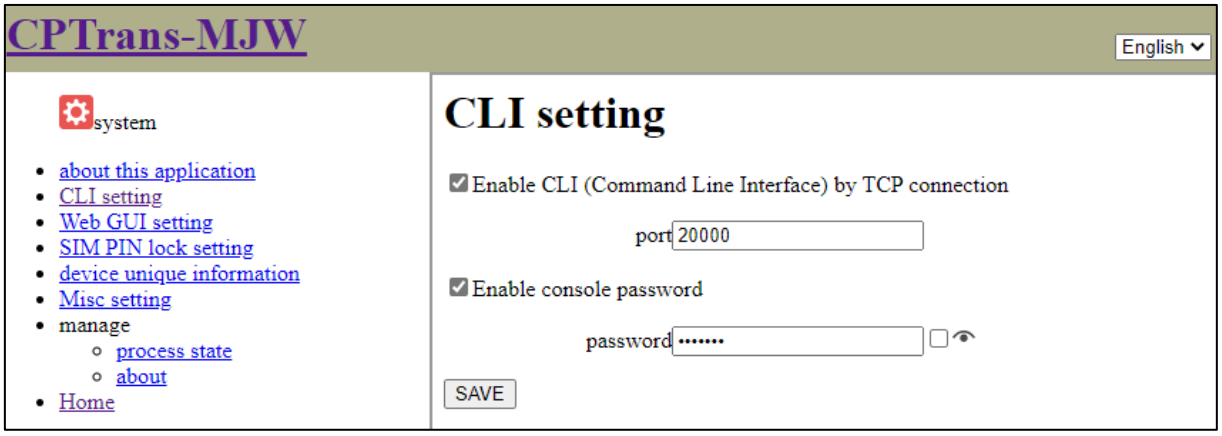



**Figure 5.5 CLI setting window**

The details of the CLI Settings screen are shown below.

(1) Enabling CLI (Command Line Interface) by TCP connection

| Item | Description |
|---|---|
| Enable CLI (Command Line Interface) by TCP connection | Enables or disables the console connection to the CLI (Management Port).<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Port | Sets the port number to be opened for the CLI (management port).<br><br>Setting range :0～65535<br>Remarks : Be careful not to duplicate the port number opened by the packet forwarding function. |

(2) Enable console password

| Item | Description |
|---|---|
| Enable console password | Enables or disables the password for CLI (Management Port) access.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled<br><br>* If disabled, authentication is omitted. (Not recommended) |
| Password | Sets a password for CLI (management port) access.<br><br>Format: Half-width alphanumeric symbols<br>NOTE: Enter a password of at least four characters. |

### 5.3.2 Web GUI Settings

This product can be controlled from Web GUI using general-purpose browsers.

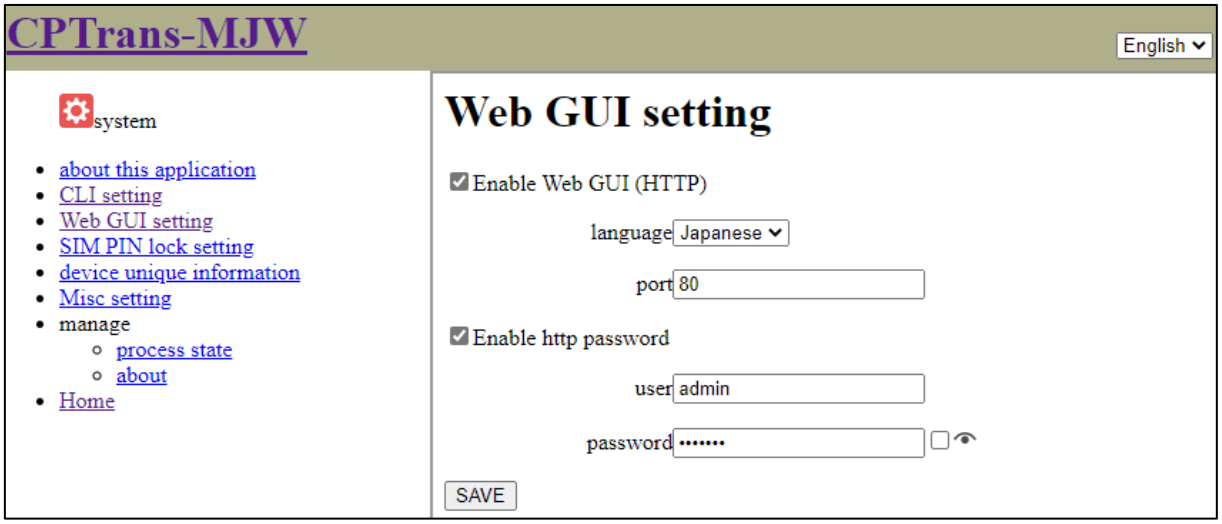



**Figure 5.6 Web GUI setting**

Web GUI Settings window is detailed below.

(1) Enable Web GUI(HTTP)

| Item | Description |
|---|---|
| Enable Web GUI(HTTP) | Specifies whether http connectivity to Web GUI is enabled or disabled.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Language | Sets Web GUI notation language.<br><br>Options:<br>・Japanese<br>・English |
| Port number | Sets the port number to be opened for Web GUI.<br><br>Setting range :1～65535<br>Initial value :80<br>Note:<br>Do not duplicate the port number opened by the packet forwarding function. |

(2) Enable http password

| Item | Description |
|---|---|
| Enable http password | Enables or disables the password for accessing Web GUI.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| User | Specifies the username for accessing Web GUI.<br><br>Format :<br>Half-width alphanumeric characters, up to 32 characters, or empty<br>Initial value : Blank space |
| Password | Specifies the password for accessing Web GUI.<br><br>Format :<br>Half-width alphanumeric characters, 8 or more and 32 characters or less, or empty<br>Initial value : Blank space |

* If both the username and password are set to empty, authentication is omitted.

### 5.3.3 SIM PIN lock setting

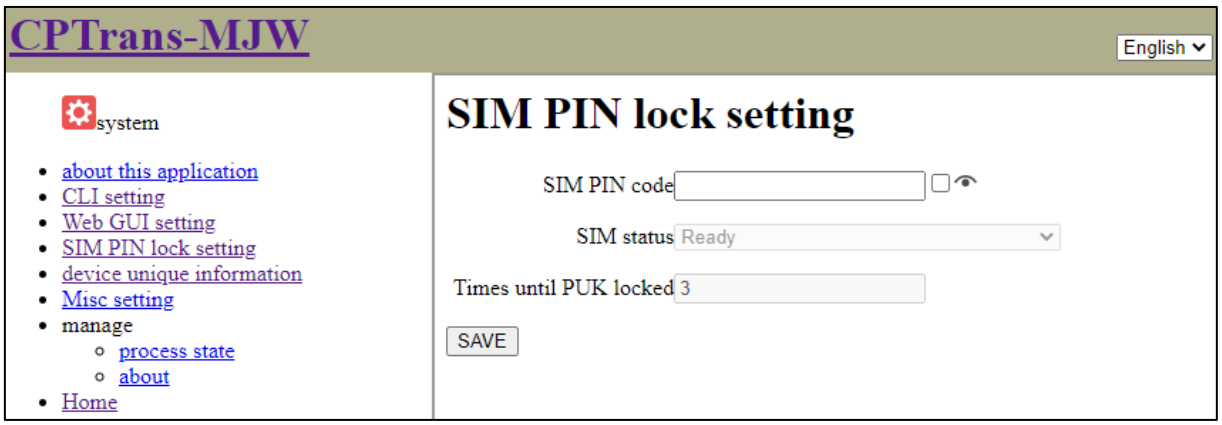



**Figure 5.7 SIM PIN lock setting**

Details of the "SIM pin lock setting" screen are shown below.

(1) SIM PIN lock setting

| Item | Description |
|---|---|
| SIM PIN code | Specify the PIN code of the SIM card.<br><br>Format: Single-byte numbers or blank |
| SIM status | Displays the status of the SIM card.<br><br>Display contents:<br>1: Normal<br>2: Normal, unlocked<br>11: SIM does not exist or cannot be accessed<br>12: Unlock failed (PIN code error)<br>13: PUK lock |
| Number of times to PUK lock | Indicates the number of times the PUK lock is reached. |

5.3.4 Device-specific information


**Figure 5.8 device unique information window**

The details of the "Device Specific Information" screen are shown below.

(1) Device-specific information

| Item | Description |
|---|---|
| Device ID | Unique ID per unit. |
| Project ID | ID used for firmware management, etc. |
| Hardware ID | ID that identifies the hardware. |
| Ether MAC addressing | MAC-address of Ethernet port. |
| WLAN MAC addressing | MAC address of the wireless LAN. |
| IMSI | Displays IMSI (Subscriber Identity Number) of USIM card. |
| ICCID | Displays ICCID (unique number) of USIM. |
| MSISDN | Displays MSISDN (telephone number) corresponding to USIM card.<br>* It is blank depending on the SIM. |
| IMEI | Displays IMEI (terminal ID number) of USIM card. |

### 5.3.5 Misc setting

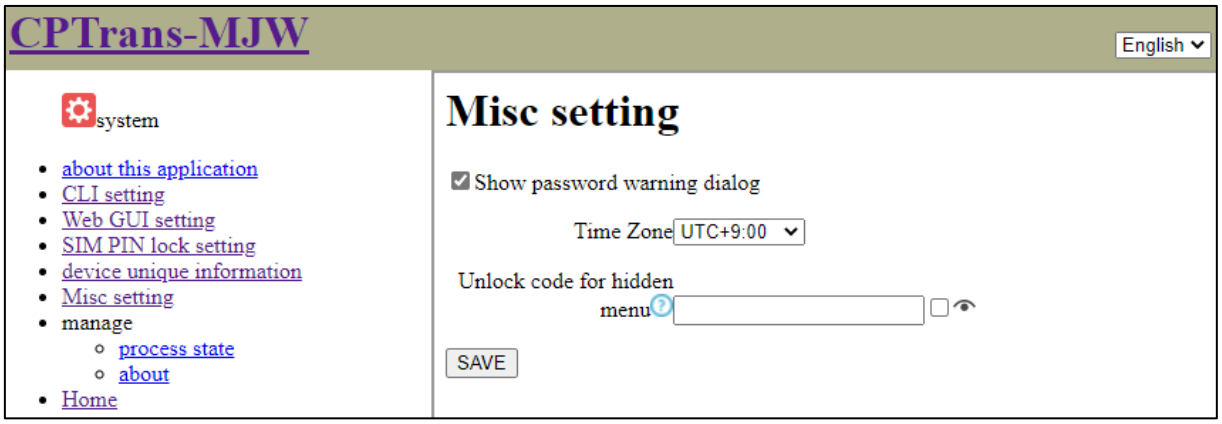



**Figure 5.9 Misc setting window**

Details of the Misc Settings screen are shown below.

(1) Other settings

| Item | Description |
|---|---|
| Show password warning dialog | Specifies whether the CLI or Web GUI displays an alert when no password is set or not.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |

## 5.4 Router

The router application is described below.

| Icon | Overview |
|---|---|
|  | It has the function of the router that relays communication.<br>This is an application for configuring LTE communication, wireless LAN communication, and Ethernet communication. |

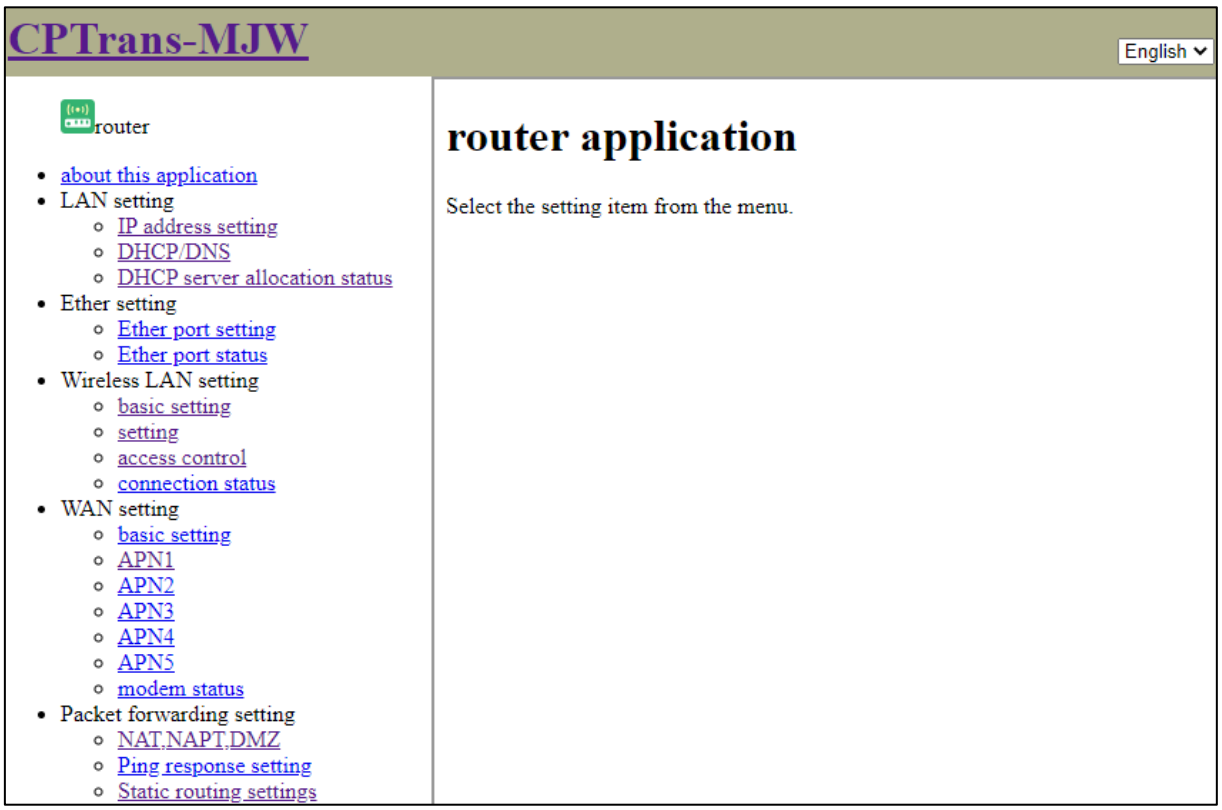



**Figure 5.10 Router application window**

### 5.4.1 LAN Setting

#### 5.4.1.1 IP address setting

LAN side IP address and subnet mask of this product can be set at this window.

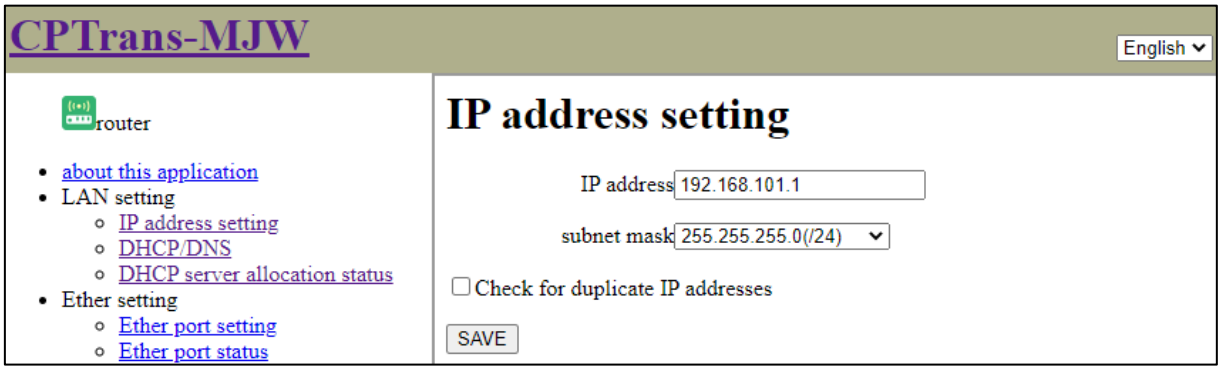



**Figure 5.11 IP address setting window**

The details of the "IP address setting" screen are shown below.

(1) IP address setup

| Item | Description |
|---|---|
| IP address | Specifies the IP address of this product in LAN.<br><br>Format: X.X.X.X<br>(X is a number between 0 and 255.) |
| Subnet Mask | Specifies the subnet mask of the IP address of this product in LAN.<br><br>Setting range:<br>Specify the network address in 0 to 32 digits. |
| Check for duplicate IP addresses | Checks for devices with the same IP address in the LAN.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |

* The IP address and subnet mask are shared by Ethernet and WLAN.

* Gratuitous ARP sending function:

  When checking for duplicate IP addresses, this product sends Gratuitous ARP packets when Ethernet connects (Link UP). If a duplicate IP address is detected as a result, an error is displayed on LED.

5.4.1.2 DHCP・DNS

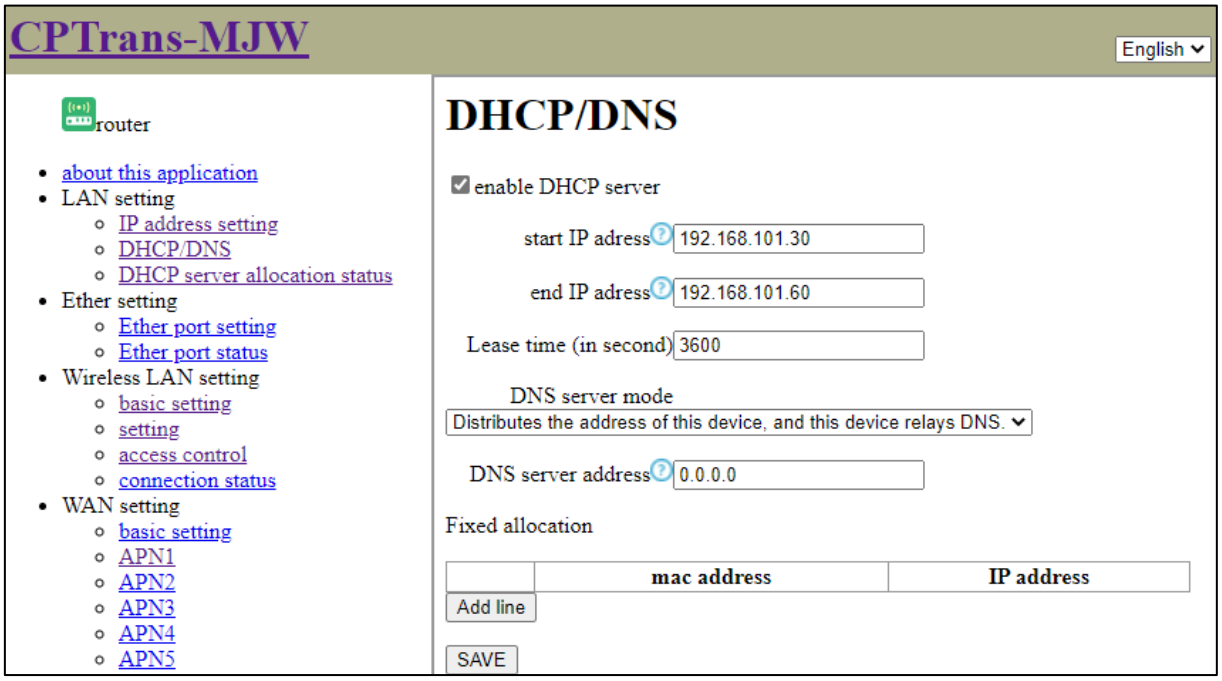



**Figure 5.12 DHCP / DNS setting window**

The detailed description of the "DHCP / DNS" window is shown below.

(1) DHCP Servers Function Setting

| Item | Description |
|---|---|
| Enable DHCP server | Enables or disables DHCP server function.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Start IP address | Specifies the starting address of the serial number assigned from DHCP servers.<br><br>Format: X.X.X.X<br>(X is a number between 0 and 255.) |
| End IP address | Specifies the address of the ending position among the IP addresses of the serial numbers allocated from DHCP servers.<br><br>Format: X.X.X.X<br>(X is a number between 0 and 255.) |
| Lease time | Specify the time from when the IP address is dispensed to when it is released. |
| DNS server mode | Specify the DNS server mode<br><br>Options:<br>・This product performs DNS relay.<br>・Specify the address of the DNS server |

| Item | Description |
|---|---|
| DNS server address | Specifies the address of the DNS server to which to forward.<br><br>Format: X.X.X.X<br>(X is a number between 0 and 255.) |

(2) Fixed allocation

Fixed allocation of DHCP can be specified by clicking Add line.

| Item | Description |
|---|---|
| MAC address | Specifies the MAC address to which a fixed IP address is assigned. |
| IP address | Specifies the static IP address to be assigned.<br><br>Format: X.X.X.X<br>(X is a number between 0 and 255.) |

5.4.1.3 DHCP server allocation status

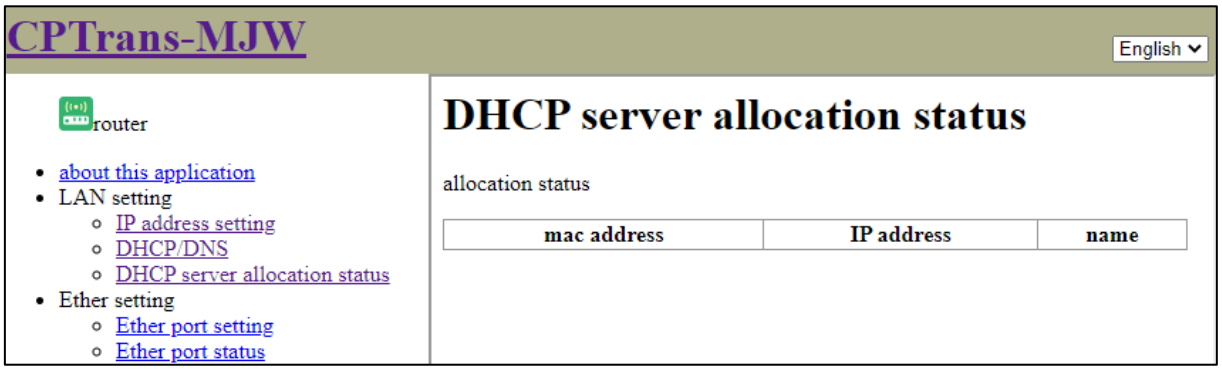



**Figure 5.13 DHCP server allocation status window**

DHCP server's allocation status window is detailed below.

(1) Assignment status

| Item | Description |
|---|---|
| MAC address | Displays the MAC address of the device that has paid out the IP address. |
| IP address | Displays the IP address that has been paid out. |
| Name | Displays the host name of the device whose IP address has been paid out. |

### 5.4.2 Ether setting

#### 5.4.2.1 Ether port setting

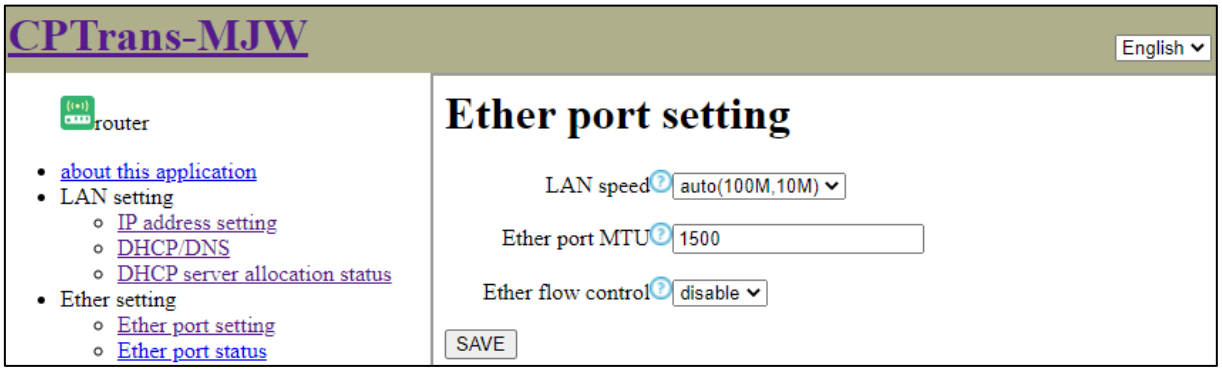



**Figure 5.14 Ether port setting**

Ether port setting window is detailed below.

(1) Ether port setting

| Item | Description |
|---|---|
| LAN speed | Specifies the baud rate of Ether.<br><br>Options:<br>・ 10Mbps / half<br>・ 10Mbps / full<br>・ 100Mbps / half<br>・ 100Mbps / full<br>・ Auto(10Mbps/100Mbps) |
| Ether port MTU | Specifies the MTU of Ether port. The maximum data size to be stored in Ether frame.<br><br>Setting range: 576 to 1500 |
| Ether flow control | Specify ether flow-control settings.<br><br>Options:<br>・Disabled<br>・Reception* This product is enabled only for reception. |

5.4.2.2 Ether port status

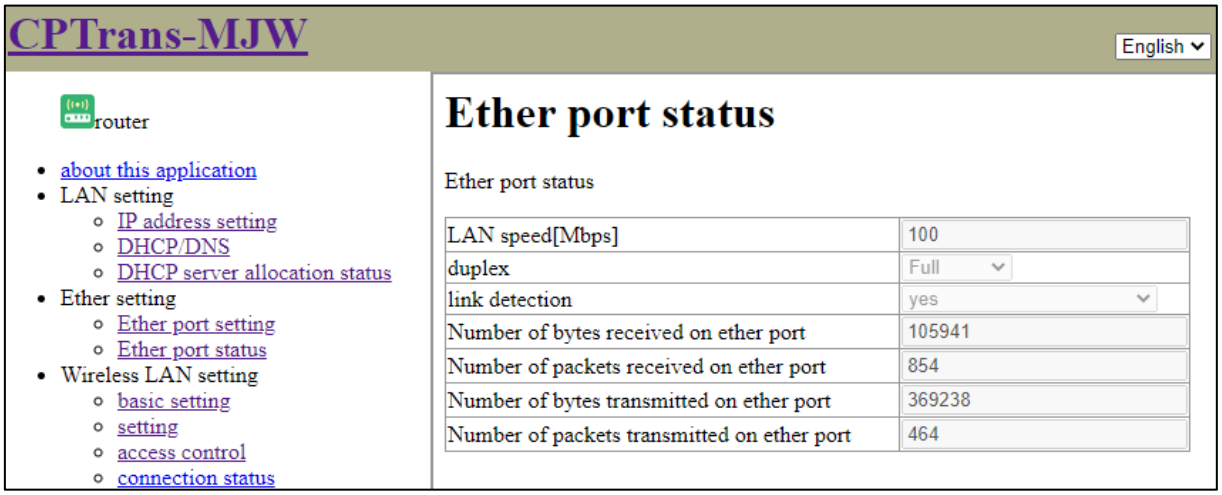



**Figure 5.15 Ether port status window**

Ether port status window is detailed below.

(1) Ether port status

| Item | Description |
|---|---|
| LAN speed [Mbps] | Displays the LAN communication speed setting value. |
| Duplex | Displays duplex (full-duplex/half-duplex) setting of Ether. |
| Link detection | Displays the link-detection status of Ether port. |
| Number of bytes received on ether port | Indicates the number of bytes received on Ether port since this product was started. |
| Number of packets received on ether port | Displays the number of packets received on Ether port since this product was started. |
| Number of bytes transmitted on ether port | Displays the number of bytes sent by Ether port. The number of bytes is displayed after the product is started. |
| Number of packets transmitted on ether port | Displays the number of packets sent on Ether port since this product was started. |

### 5.4.3 Wireless LAN setting

#### 5.4.3.1 Basic setting

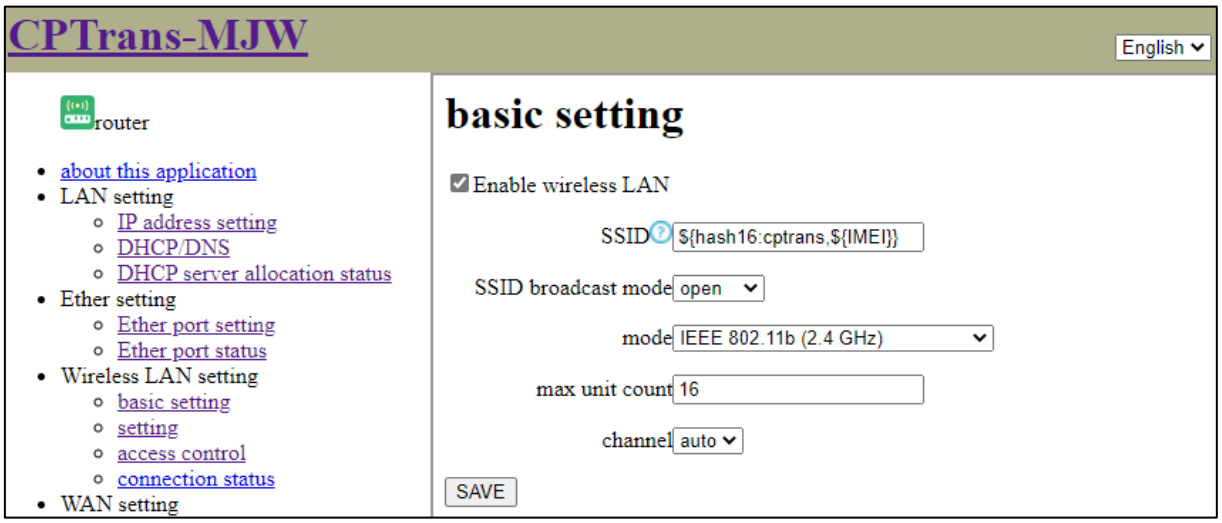



**Figure 5.16 Wireless LAN basic setting**

The basic setting window details are shown below.

(1) Basic Wireless LAN Settings

| Item | Description |
|---|---|
| Enable wireless LAN | Enables or disables the wireless LAN.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| SSID | Specifies SSID of APs.<br><br>Format: Up to 32 one-byte alphanumeric characters |
| SSID broadcast mode | Specify the notification settings for SSID.<br><br>Options:<br>・ open<br>・ hidden<br>・ blank<br><br>* If blank is selected, users cannot connect to the AP unless they also specify a SSID. |

| Item | Description |
|---|---|
| mode | Specify the standards and settings of the wireless LAN to be used.<br><br>Options:<br>・ IEEE 802.11b (2.4GHz)<br>・ IEEE 802.11g (2.4GHz)<br>・ IEEE 802.11a (5GHz)<br>・ IEEE 802.11n (2.4GHz)<br>・ IEEE 802.11n (5GHz)<br>・ IEEE 802.11ac (5GHz)<br>・ IEEE 802.11n (2.4GHz, BW=40M)<br>・ IEEE 802.11ac (5GHz, BW=40M) |
| max unit count | Specify the number of units that can be connected.<br><br>Setting range: 1 to 16 units |
| Channel | Selects the channel of the frequency to be used.<br><br>Options:<br>Automatic、 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 [CH] |

5.4.3.2 Setting

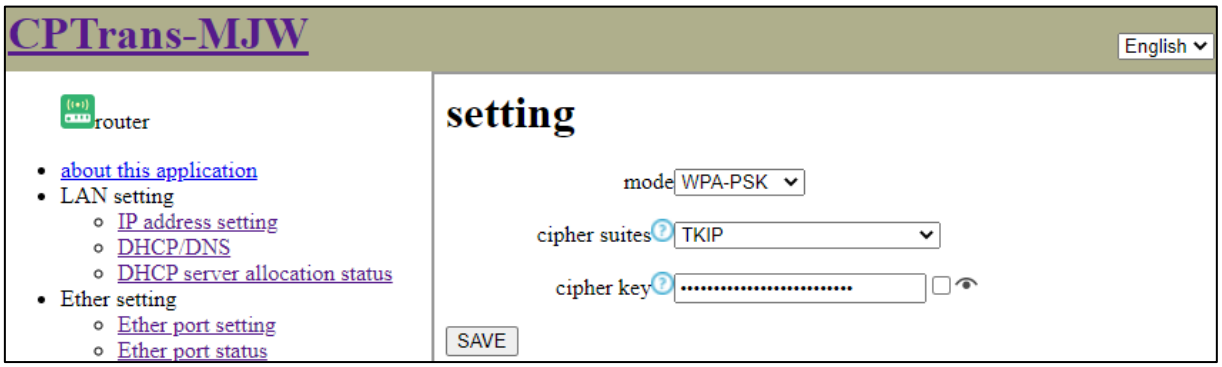



**Figure 5.17 Encryption setting window**

The details of the "Encryption setting" screen are shown below.

(1) Encryption setting

| Item | Description |
|---|---|
| mode | Specifies the encryption standard.<br><br>Options:<br>・ WEP<br>・ WPA-PSK<br>・ WPA2-PSK<br><br>* Use of WEP is not recommended. It is recommended to use WPA2-PSK whenever possible. |
| Cipher suite | Specifies the encryption method.<br><br>Options:<br>・ TKIP<br>・ CCMP/AES-CBC-MAC-128<br>* This setting is invalid for WEP. |
| Cipher key | Specify the password required for the wireless LAN connection.<br>It supports up to 127 characters. |

5.4.3.3 Access control

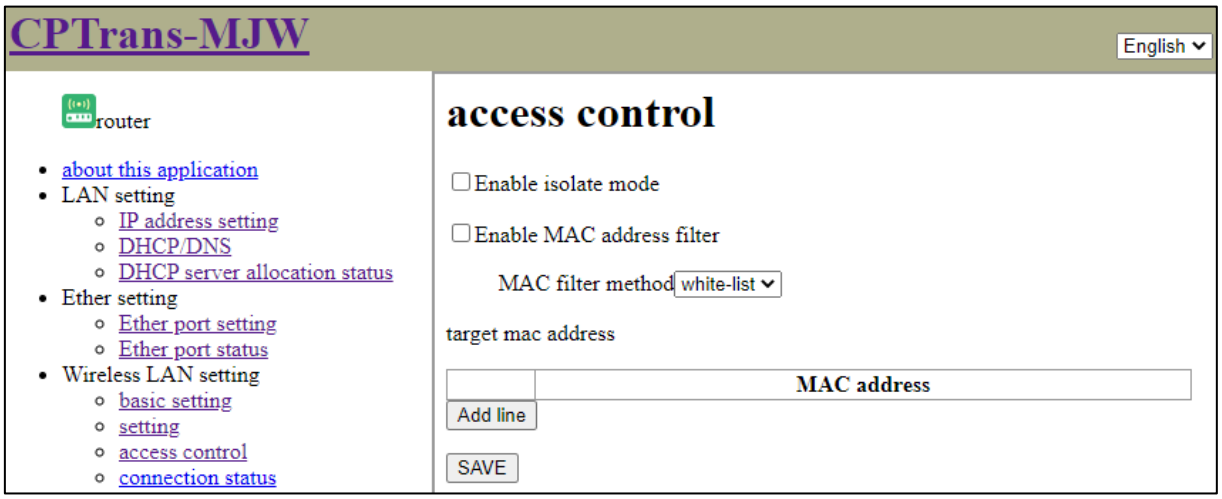



**Figure 5.18 access control setting window**

The details of the Access Control screen are shown below.

(1) Basic setting

| Item | Description |
|---|---|
| Enable isolate mode | Enables or disables the isolation mode, which prohibits access to devices in the LAN through the AP.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Enable MAC address filter | Enables or disables the function that does not allow the specified MAC address to be connected to the AP.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Target MAC address | Specify the filtering method.<br><br>Options:<br>・ Whitelist format<br>・ Only devices added to the target MAC address can be connected.<br>・ Blacklist format<br>・ Block the connection of the device added to the target MAC address. |

(2) Target MAC address

Target MAC address can be added by clicking Add line.

| Item | Description |
|---|---|
| MAC address | Specifies the target MAC address. |

5.4.3.4 Connection status

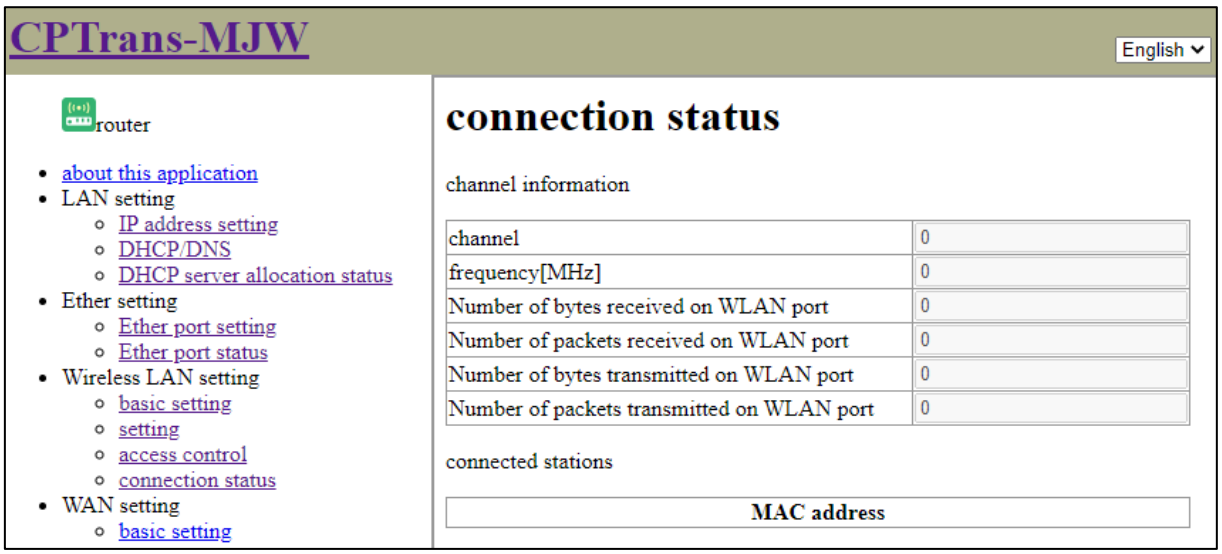



**Figure 5.19 connection status window**

Details of the "Connection status" screen are shown below.

(1) Channel information

| Item | Description |
|---|---|
| Channel | Displays the channel number of the wireless LAN being used. |
| Frequency [MHz] | Displays the frequency of the wireless LAN being used. |
| Number of bytes received on the WLAN port | Displays the number of bytes received via the wireless LAN after the product is started. |
| Number of packets received on the WLAN port | Displays the number of packets received via the wireless LAN after the product is started. |
| Number of bytes transmitted on the WLAN port | Displays the number of bytes sent via the wireless LAN after the product is started. |
| Number of packets sent to the WLAN port | Displays the number of packets sent via the wireless LAN after the product is started. |

(2) Connected station

| Item | Description |
|---|---|
| MAC address | Displays the MAC address of the device connected to the wireless LAN. |

### 5.4.4 WAN Setting

#### 5.4.4.1 Basic setting

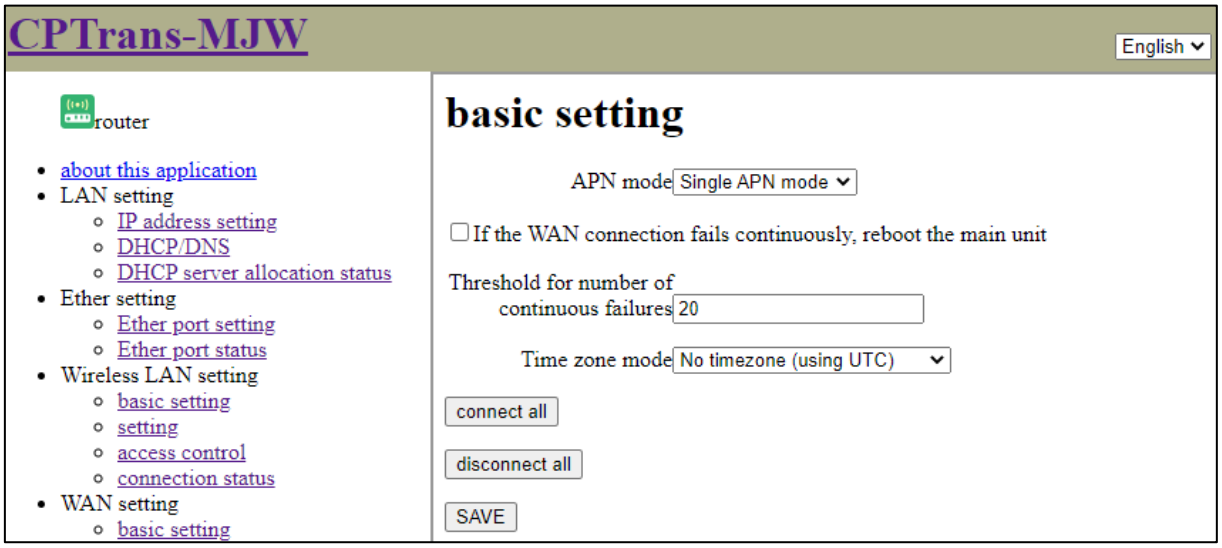



**Figure 5.20 WAN setting, basic setting window**

The basic settings screen details are shown below.

(1) Basic setting

| Item | Description |
|---|---|
| APN mode | Select the APN mode.<br><br>Options:<br>・Single APN mode:<br>Connect to only one APN.<br>・Multi-APN mode:<br>Multiple (up to five) APNs can be connected at the same time.<br><br>※Multi-APN mode is enabled only for supported carriers. |
| If the WAN connection fails continuously, reboot the main unit. | Enables or disables the reboot function when the threshold of the number of failed connections to the WAN is exceeded.<br>Check: The terminal is rebooted when the threshold of the number of connection failures is exceeded.<br>No check: Does not reboot even if the connection fails. |
| Threshold for number of continuous failures | Specifies the threshold for the number of consecutive failures to connect to the WAN.<br><br>Setting range: 5 to 65535 (times) |
| Connect All | Press to connect to APN1 to 5. |
| Disconnect All | Press the button. Cutting is performed for APN1 to 5. |

5.4.4.2 APN1

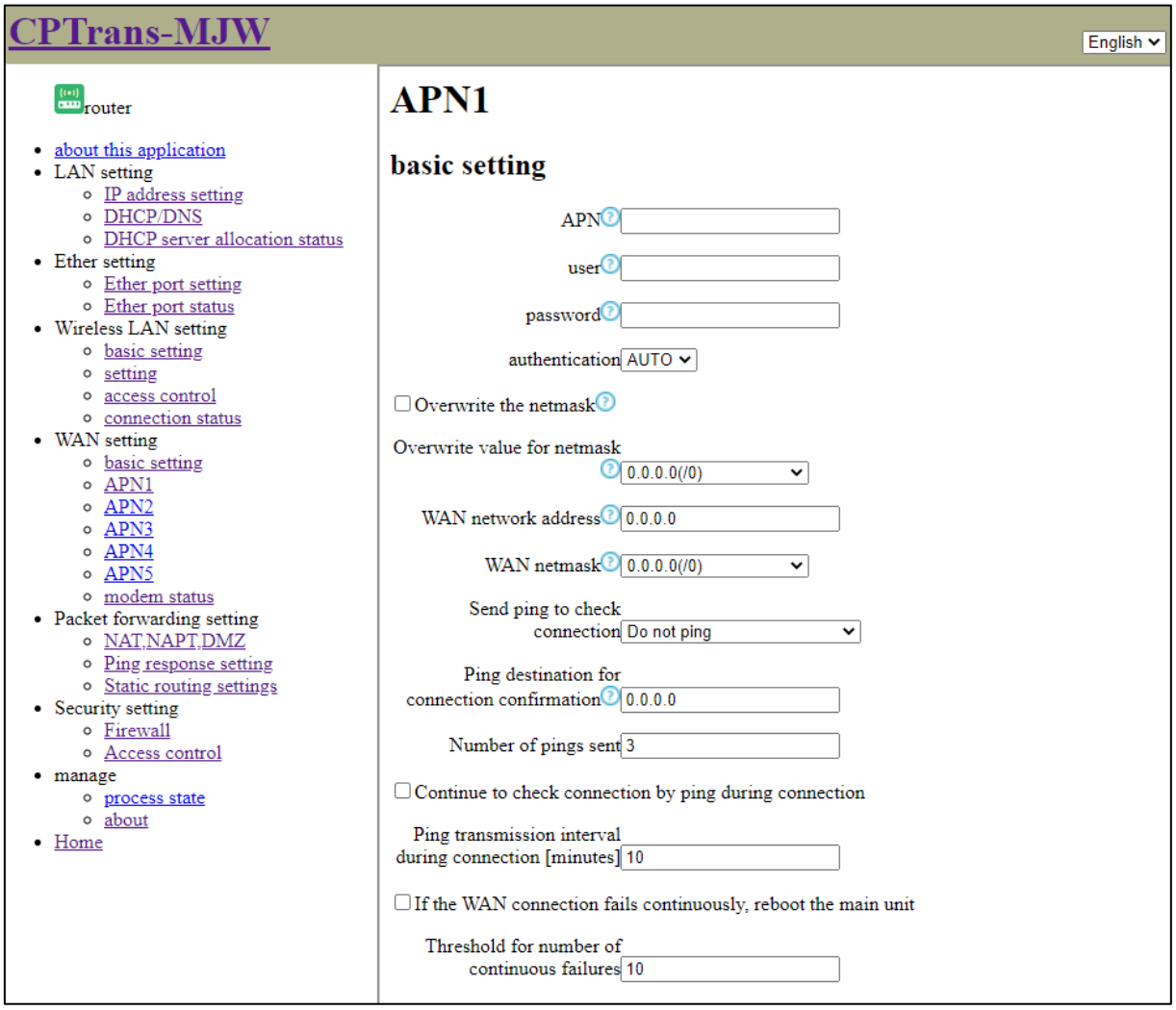



**Figure 5.21 APN setting window (1 of 3)**

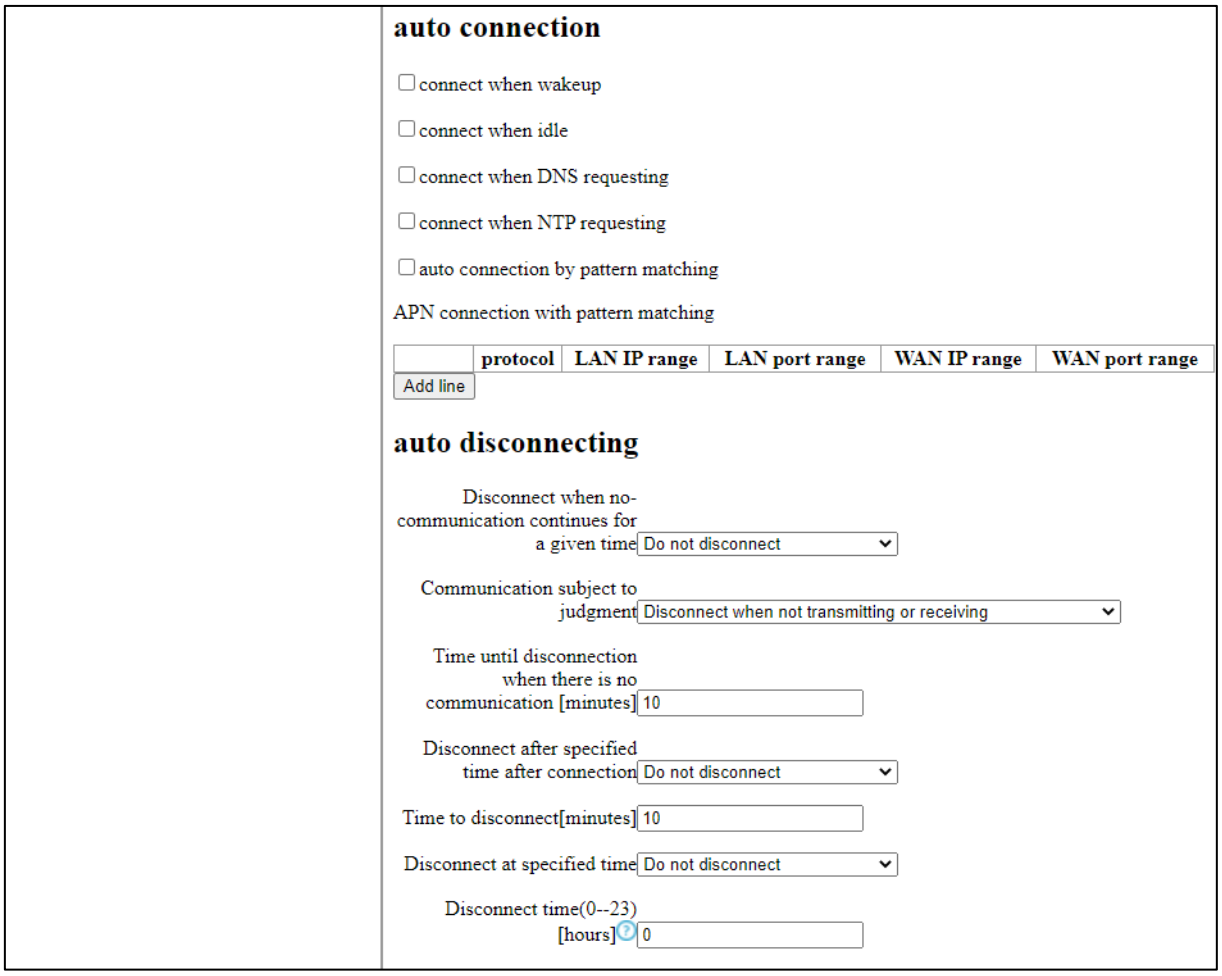



**Figure 5.22 APN setting window (2 of 3)**

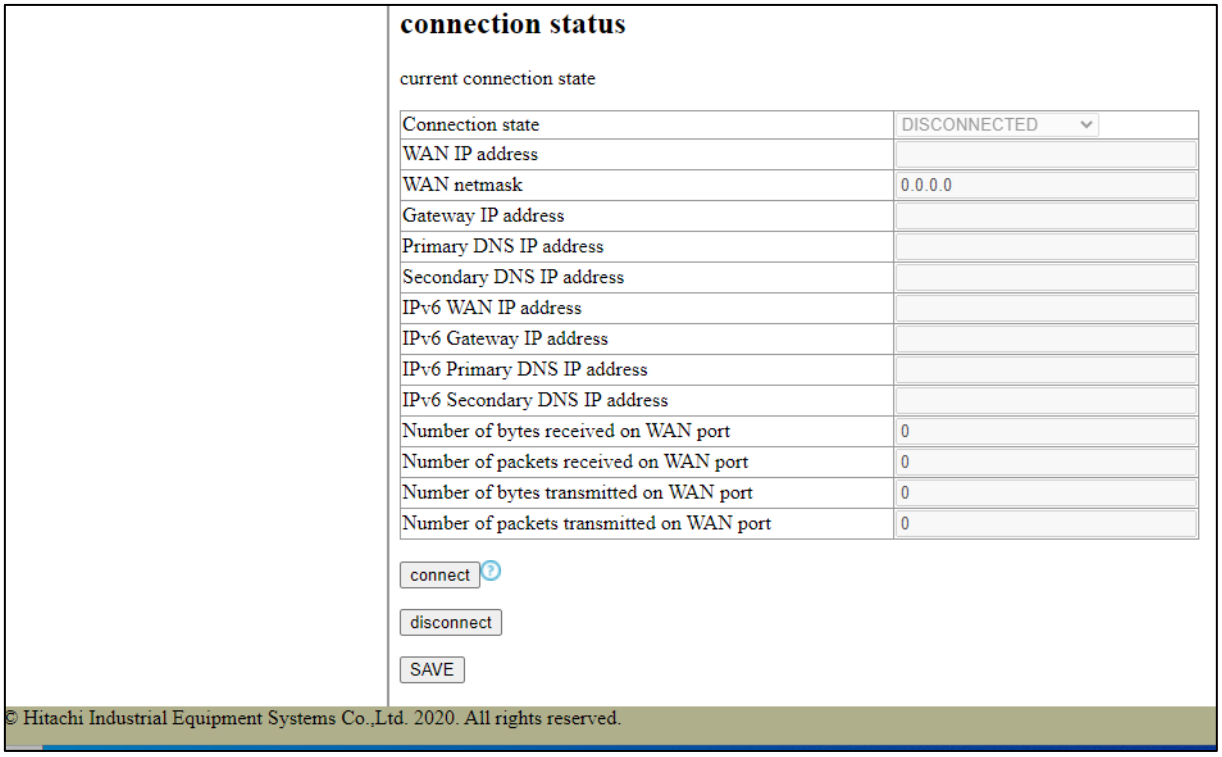



**Figure 5.23 APN setting window (3 of 3)**

APN1 window is detailed below.

(1) Basic setting

| Item | Description |
|---|---|
| APN | Enter the APN name of the access point. |
| User | Enter the user name required for the APN connection. |
| Password | Enter the password required for the APN connection. |
| Authentication | Select the authentication method for APN connection.<br><br>Options:<br>・ PAP<br>・ CHAP<br>・ AUTO (Auto) |
| Overwrite the net mask | Specifies whether to overwrite the netmask acquired during APN connection.<br>Checked: Overwrites the Netmask Overwrite Value.<br>No check: Do not overwrite the netmask. |
| Overwrite value for netmask | Select the netmask overwrite value. |
| WAN network address | Specifies the WAN side network address.<br>※It can be connected even if it is not specified.<br><br>Format: X.X.X.X<br>(X is a number between 0 and 255.) |

| Item | Description |
|---|---|
| WAN netmask | Specifies the WAN netmask.<br><br>Setting range:<br>Specify the network address in 0 to 32 digits. |
| Send ping to check connection | Configure the sending of PING to verify communication to the WANs.<br><br>Options:<br>・ Do not ping<br>・ Ping the gateway address<br>・ Ping the primary DNS server<br>・ Ping the specified address |
| Ping destination for connection confirmation | Set the IP address to check communication with.<br><br>Format: X.X.X.X<br>(X is a number between 0 and 255.) |
| Number of pings sent | Confirmation of communication to the WAN<br>Specify the number.<br><br>Setting range: 1 to 10 [times] |
| Continues to check connection by ping during connection | Enables or disables communication confirmation to the connection destination after the connection is completed for the APN.<br><br>Check ON: Confirmation of communication is performed.<br>No check: Communication confirmation is not performed. |
| Ping transmission interval during connection [minutes] | Specifies the life and death monitoring cycle.<br><br>Setting range: 1 to 60 [min] |
| If the WAN connection fails continuously, reboot the main unit | Threshold for the number of consecutive failures Specify whether to enable or disable the setting to reboot the unit when a WAN connection fails.<br><br>Checked: Performs a reboot with consecutive failures.<br>No check: No reboot is performed. |
| Threshold for number of continuous failures | Specifies the threshold for the number of consecutive WAN connection failures before the body reboots.<br><br>Setting range :5～65535 |

(2) Auto connection

I. Auto connection setting

| Item | Description |
|---|---|
| Connect when wakeup | Enables or disables the setting for APN connection when this product is started.<br><br>Checked: Connected at startup.<br>No check: Do not connect at startup. |
| Connect when idle | Enables or disables the reconnect (always APN connection) setting when LTE is disconnected (idle).<br><br>With check: Connect when idle.<br>No check: Not connected when idle. |
| Connect when DNS requesting | Enables or disables the setting for APN connection when a DNS request is made.<br><br>Checked: Connected when DNS is requested.<br>No check: Do not connect when requesting DNS. |
| Connect when NTP requesting | Enables or disables the setting for APN connection when NTP is requested.<br><br>Checked: Connected when NTP is requested.<br>No check: No connection is made when NTP is requested. |
| Auto connection by pattern matching | Enables or disables the automatic APN connection function by pattern matching.<br><br>With check: Connected at pattern match.<br>No check: Not connected at pattern match.<br><br>The operation condition is that the pattern match rule is added to "APN connection by pattern match". |

II. Auto connection by pattern matching

Rules for pattern-matching APN connections can be added by clicking Add line.

| Item | Description |
|---|---|
| Protocol | Specify the protocol that matches the condition.<br><br>Options:<br>・ ANY<br>・ TCP<br>・ UDP<br>・ ICMP |
| LAN IP range | Specifies LAN IP addressing range.<br><br>Format: X.X.X.X<br>(X is a number between 0 and 255.) |

| Item | Description |
|---|---|
| LAN port range | Specify the LAN port number.<br><br>Setting range :0～65535 |
| WAN IP range | Specifies WAN IP addressing range.<br><br>Format: X.X.X.X<br>(X is a number between 0 and 255.) |
| WAN port range | Specify the WAN port number.<br><br>Setting range :0～65535 |

(3) Auto disconnecting

| Item | Description |
|---|---|
| Disconnect when no-communication continues for a given time | Specify whether to enable or disable the function to disconnect the line when there is no communication for a certain period.<br><br>Options:<br>・ Do not disconnected<br>・ Reconnect after disconnecting<br>・ Do disconnect |
| Communication subject to judgement | Specifies the disconnection condition for the function to disconnect the line when there is no communication for a certain period.<br><br>Options:<br>・ Disconnect if there are no transmissions on the WAN<br>・ Disconnect if there is no receive from the WAN<br>・ Disconnect when there is no transmission or reception.<br>・ Disconnect if there is no transmission or reception. |
| Time until disconnection when there is no communication [minutes] | Specify the time to disconnect [minutes] when "Disconnect line when there is no communication" is enabled for a certain period.<br><br>Setting range: 1 minute or more |
| Disconnect after specified time after connection | Specify whether to enable or disable the function to be disconnected after the specified time has elapsed.<br><br>Options:<br>・ Do not disconnected<br>・ Reconnect after disconnecting<br>・ Do disconnect |

| Item | Description |
|---|---|
| Time to disconnect [minutes] | Specify the time to disconnect [minutes] when "Disconnect after specified time after connection" is enabled.<br>Setting range: 1 minute or more |
| Disconnect at specifies time | Enables or disables the function to disconnect at the specified time.<br><br>Options:<br>・ Do not disconnected<br>・ Reconnect after disconnecting<br>・ Do disconnect |
| Disconnect time (0 to 23) [hour] | When "Disconnect at specified time" is enabled, specify the disconnection time [hour].<br><br>Setting range: 0 to 23 [hour]<br><br>Minutes and seconds of the specified time are determined at random.<br>The disconnection time is specified in UTC. |

(4) Connection status

| Item | Description |
|---|---|
| Connection state | Displays the connection state.<br><br>Display range:<br>1: STARTING<br>2: DISCONNECTED<br>3: CONNECTING<br>4: PRECONNECTED<br>5: CONNECTED<br>6: DISCONNECTING<br>7: PREDISCONNECTED |
| WAN IP address | Displays WAN IP address. |
| Gateway IP address | Displays the gateway IP address. |
| Primary DNS IP address | Displays the primary DNS IP address. |
| Secondary DNS IP Address | Displays the secondary DNS IP address. |
| Number of bytes received on WAN port | Displays the number of bytes received on the WAN port since this product was started. |
| Number of packets received on WAN port | Displays the number of WAN port received packets since this product was started. |
| Number of bytes transmitted on WAN port | Displays the number of bytes sent to the WAN port since this product was started. |
| Number of packets sent to WAN port | Displays the number of packets sent to the WAN port since this product was started. |

#### 5.4.4.3 APN2

The setting window and details are the same as in APN1 5.4.4.2 .

#### 5.4.4.4 APN3

The setting window and details are the same as in APN1 5.4.4.2 .

#### 5.4.4.5 APN4

The setting window and details are the same as in APN1 5.4.4.2 .

#### 5.4.4.6 APN5

The setting window and details are the same as in APN1 5.4.4.2 .

5.4.4.7 Modem status

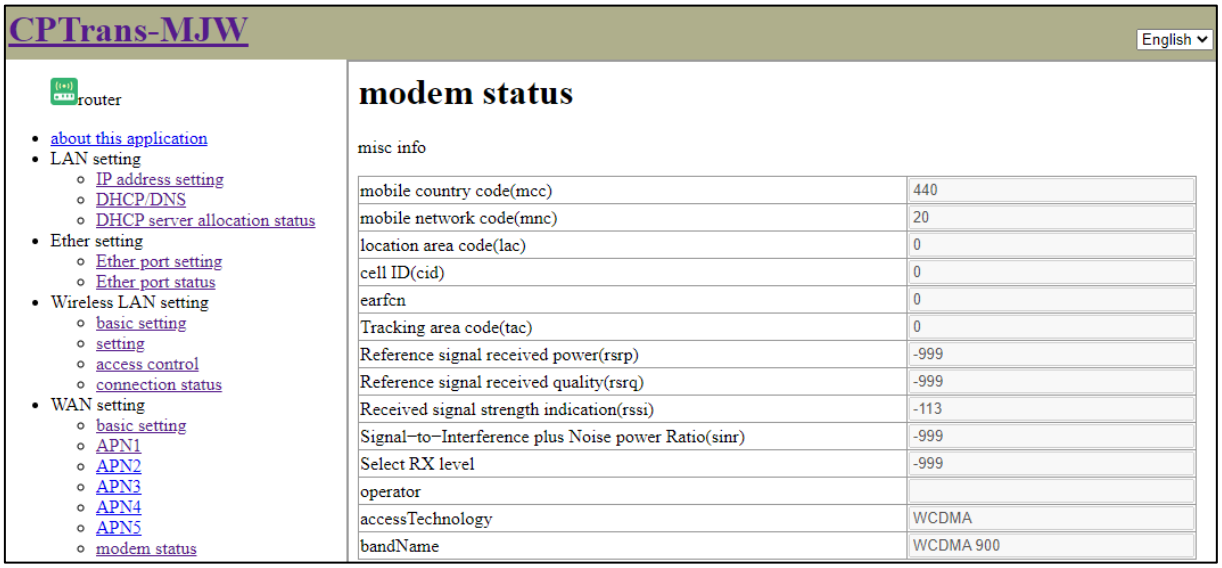



**Figure 5.24 Modem status window**

Details of the Modem Status screen are shown below.

(1) Misc info

| Item | Description |
|---|---|
| Mobile country code(mcc) | Displays MCC (Telecom carrier operation area code). |
| Mobile network code(mnc) | Displays MNC (carrier ID code). |
| Location area code(lac) | Displays the LAC of the base station. |
| Cell ID (cid) | Displays the CID of the base station. |
| Earfcn | Displays the connected frequency band. |
| Tracking area code(tac) | Displays the connected tracking area code (TAC). |
| Reference signal received power(rsrp) | Displays the reference received power (RSRP). |
| Reference signal received quality(rsrq) | Displays the reception qualities (RSRQ). |
| Received signal strength indication(rssi) | Displays the received signal strength (RSSI). |
| Signal to Interference plus Noise power Ratio(sinr) | Displays the signal-to-noise interference ratio (SINR). |
| Select RX level | Displays the radio signal reception level. |
| Operator | Show carrier |
| AccessTechnology | Displays the LTE band type (FDD, TDD, etc.). |
| BandName | Displays the name of the connected band. |

### 5.4.5 Packet forwarding settings

#### 5.4.5.1 NAT・NAPT・DMZ

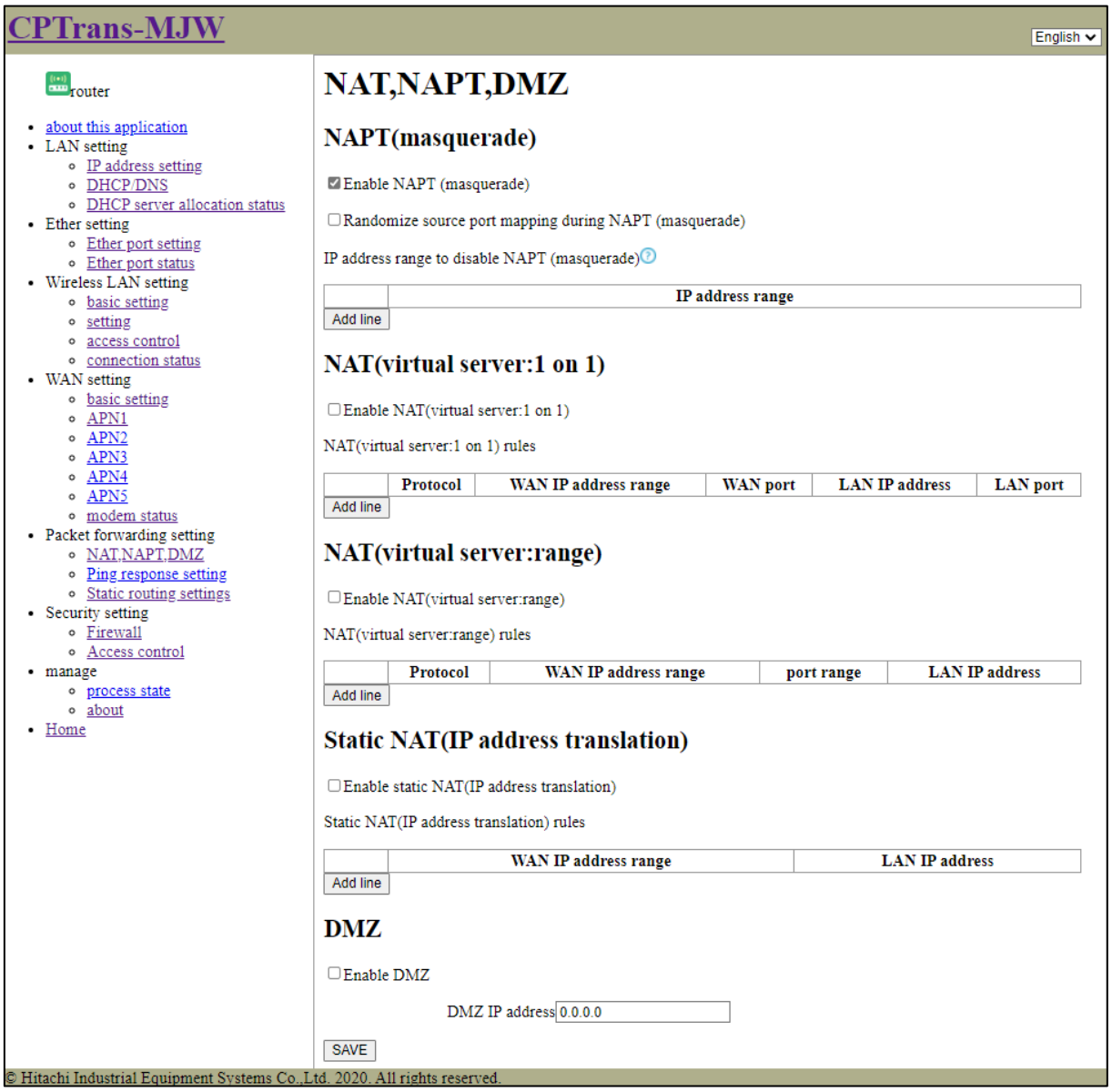



**Figure 5.25 Packet forwarding setting window**

The NAT, NAPT, and DMZ windows are detailed below.

(1) NAPT (masquerade)

I. NAPT setting

| Item | Description |
|---|---|
| Enable NAPT (masquerade) | Enables or disables NAPT (masquerading) function.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Randomize source port mapping during NAPT (masquerade) | The source port is selected randomly.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |

II. IP address range to disable NAPT (masquerade)

Rules for IP address ranges that disable NAPT can be added by clicking Add line.

| Item | Description |
|---|---|
| IP address range | The specified IP address-range disables NAPT (masquerade). |

(2) NAT (Virtual Server)

I. NAT (Virtual Server) Configuration

| Item | Description |
|---|---|
| Enable NAT (Virtual Server) | Enables or disables the NAT (Virtual Server) function.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |

II. NAT (Virtual Server) Rules

NAT (Virtual Server) rules can be added by clicking Add line.

| Item | Description |
|---|---|
| Protocol | Specifies the protocol that is adapted to NAT (virtual server).<br><br>Options:<br>・ TCP<br>・ UDP |
| WAN side IP range | Specifies the WAN IP range. |
| WAN port | Specifies the WAN port number. |
| LAN side IP range | Specify the LAN side IP. |
| LAN port | Specify the LAN port number. |

(3) Static NAT (IP Address Translation)

I. Static NAT (IP Address Translation) Configuration

| Item | Description |
|---|---|
| Enabling Static NAT (IP Address Translation) | Enables or disables the static NAT (IP address translation) function.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |

II. Static NAT (IP Address Translation) Rules

Static NAT (IP Address Translation) rules can be added by clicking Add line.

| Item | Description |
|---|---|
| WAN side IP range | Specifies the WAN IP range. |
| LAN side IP | Specify the LAN side IP. |

(4) DMZ

| Item | Description |
|---|---|
| Enable the DMZ | Enables or disables the DMZ function.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| DMZ IP addressing | Specifies the IP address of the DMZ to be transferred. |

5.4.5.2 Ping response setting

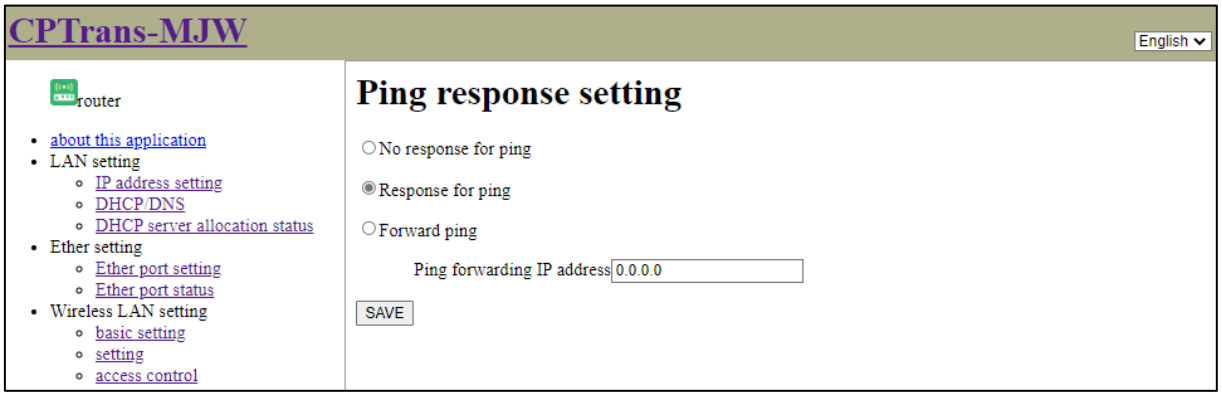



**Figure 5.26 Ping response setting window**

The detailed ping response setting window is shown below.

| Item | Description |
|---|---|
| Not respond for ping | Ping requests from WANs are ignored. |
| Response for ping | Respond to ping requests from WANs. |
| Forward ping | When a ping request is received from the WAN, ping is transferred to the device specified in "ping forwarding IP address".<br>If there is no response, it sends a response packet to the WAN side. |
| Ping forwarding IP address | When "Forward ping" is selected, specify the IP address of the forwarding destination.<br><br>Format: X.X.X.X<br>(X is a number between 0 and 255.) |

### 5.4.5.3 Static routing settings

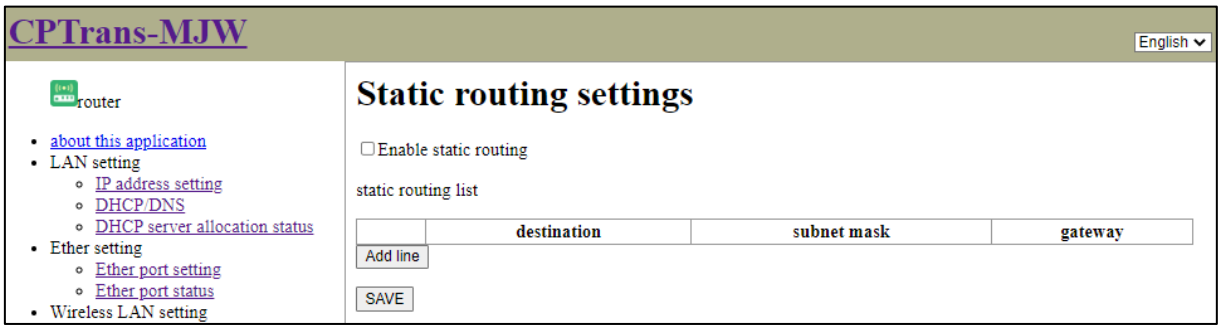



**Figure 5.27 Static routing setting window**

The Static Routing Settings screen details are shown below.

(1) Basic setting

| Item | Description |
|---|---|
| Enable static routing | Enables or disables the static routing function.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |

(2) Static routing list

| Item | Description |
|---|---|
| Destination | Specifies the IP address to which routing is forwarded. |
| Subnet Mask | Specifies the subnet mask of the LAN side network. |
| Gateway | Specify a gateway address other than this product in the network on the LAN side. |

### 5.4.6 Security settings

#### 5.4.6.1 Firewall

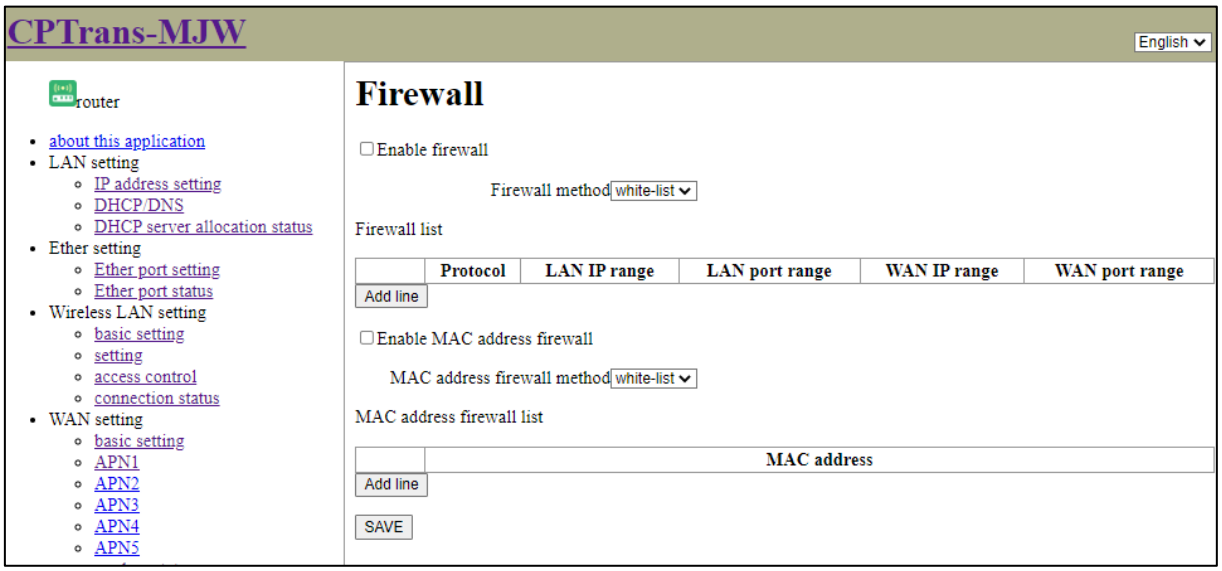



**Figure 5.28 Firewall setting window**

The Firewall setting window details are shown below.

(1) Firewall settings

I. Firewall settings

| Item | Description |
|---|---|
| Enable firewall | Specifies whether the IP firewall is enabled or disabled.<br>When disabled, all packets are treated as "passing".<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Firewall method | Specify the filtering method.<br><br>Options:<br>・ White-list<br>　・ Only records added to the target list can be connected.<br>・ Black-list<br>　・ Block connections for records added to the target list |

II. Firewall list

Rules to the firewall list can be specified by clicking Add line.

| Items | Description |
|---|---|
| Protocol | Specify the target protocol.<br><br>Choices: TCP/UDP/ICMP/ANY |
| LAN IP range | Specify a range of LAN side IP address. |
| LAN port range | Specify a range of LAN port number. |
| WAN IP range | Specifies a range of WAN-side IP address. |
| WAN port range | Specify a range of WAN port number. |

(2) MAC Address Firewall Settings

I. MAC Address Firewall Settings

| Item | Description |
|---|---|
| Enable MAC Address Firewall | Specifies whether the MAC address firewall is enabled or disabled.<br>When disabled, all packets are treated as "passing".<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| MAC address firewall method | Specify the filtering method.<br><br>Options:<br>・ White-list<br>・ Only records added to the target list can be connected.<br>・ Black-list<br>・ Block connections for records added to the target list |

II. MAC Address Firewall List

Rules to the MAC address firewall list can be set by clicking Add line.

| Item | Description |
|---|---|
| MAC address | Specifies the target MAC address. |

5.4.6.2 Access control

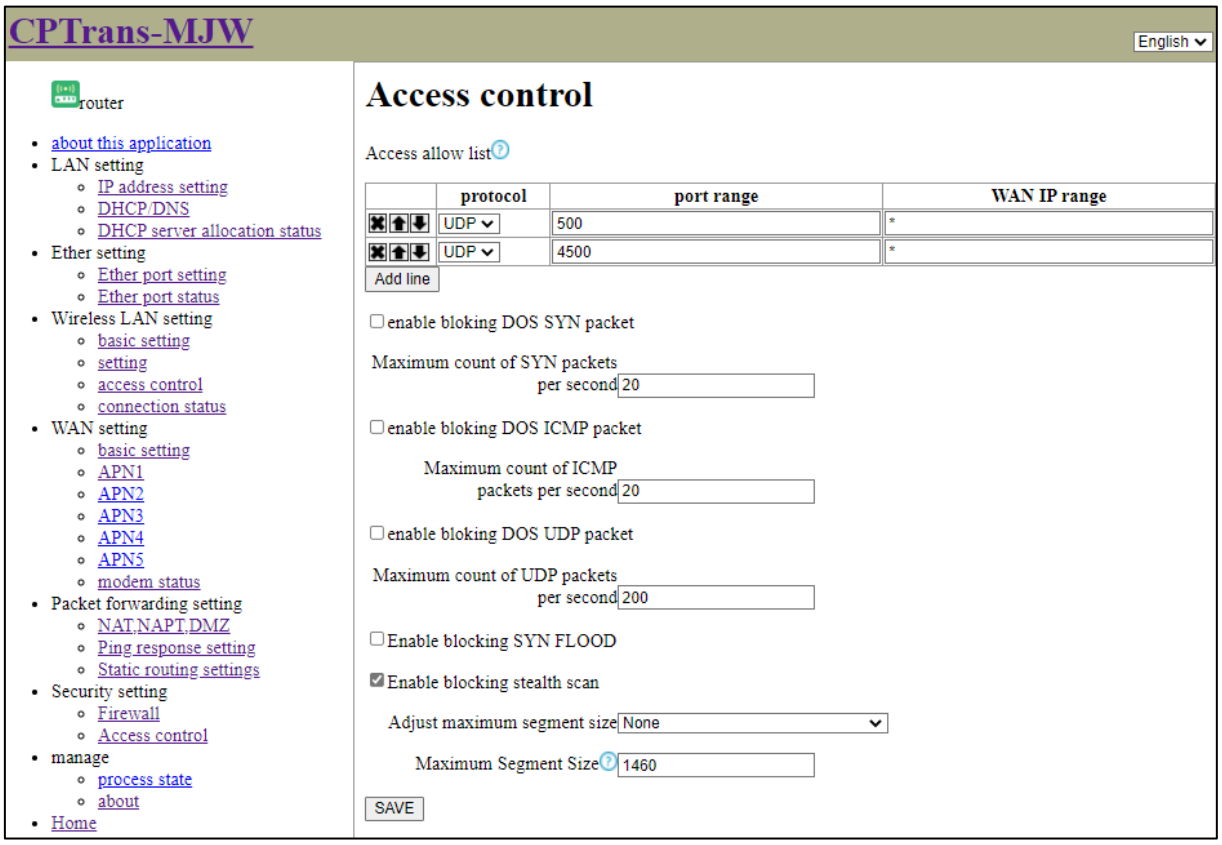



**Figure 5.29 Access control setting**

The details of the Access Control screen are shown below.

(1) Access allow list

A rule to the Access Permissions list can be added by clicking Add line.

| Item | Description |
|---|---|
| Protocol | Specify the protocols that you want to allow access to.<br><br>Options:<br>1: TCP<br>2: UDP |
| Port range | Specifies the port number to which access is permitted. |
| WAN IP range | Specifies the WAN-side IP address to which access is permitted. |

(2) Access Control setting

| Item | Description |
|---|---|
| Enable blocking DOS SYN packet<br>(Not supported) | Specifies whether to enable or disable DoS measures for SYN packets.<br><br>Enabled: DoS measures are taken using SYN packets.<br>Disabled: Do not take measures against DoS. |
| Maximum count of SYN packets per second<br>(Not supported) | Specifies the maximum number of SYN packets to pass per second.<br><br>Set value: 20 (default value)<br>* Setting range: from 10 to 1000 |
| Enable blocking DOS ICMP packet<br>(Not supported) | Enables or disables the denial-of-service protection for ICMP packets.<br><br>Enabled: DoS-based ICMP packets are taken.<br>Disabled: Do not take measures against DoS. |
| Maximum count of ICMP packets per second<br>(Not supported) | Specifies the maximum number of ICMP packets to pass per second.<br><br>Set value: 20 (default value)<br>* Setting range: from 10 to 1000 |
| Enable blocking DOS UDP packet<br>(Not supported) | Enables or disables DoS protection for UDP packets.<br><br>Enabled: DoS countermeasures are taken using UDP packets.<br>Disabled: Do not take measures against DoS. |
| Maximum count of UDP packets per second<br>(Not supported) | Specifies the maximum number of UDP packets to pass per second.<br><br>Set value: 500 (default value)<br>* Setting range: from 10 to 10000 |

| Item | Description |
|---|---|
| Enable blocking SYN FLOOD<br>(Not supported) | Specify whether to enable or disable SYN FLOOD measures.<br>Enabled: Take measure against SYN FLOOD.<br>Disabled: Do not take SYN FLOOD measures. |
| Enable blocking stealth scan | Specifies whether stealth scan protection is enabled or disabled.<br><br>Effective: Take measures against stealth scan.<br>Disabled: Do not take stealth scan measures. |
| Adjust maximum segment Size | Adjust the size that can be transmitted on a single TCP segment.<br><br>Options:<br>・ None<br>・ Calculate automatically from PMTU<br>・ Force to specified value |
| Maximum Segment Size | Valid only when "Force to specified value" is selected in "Adjust Maximum Segment Size".<br><br>Setting range: 128 to 1460 |

## 5.5 Scheduled reboot

The scheduled reboot application is described below.

| Icon | Overview |
|---|---|
|  | This product can be rebooted at a specific time and time.<br>It is also possible to specify the time that has elapsed since startup, a specific time and day of the week, and a combination |

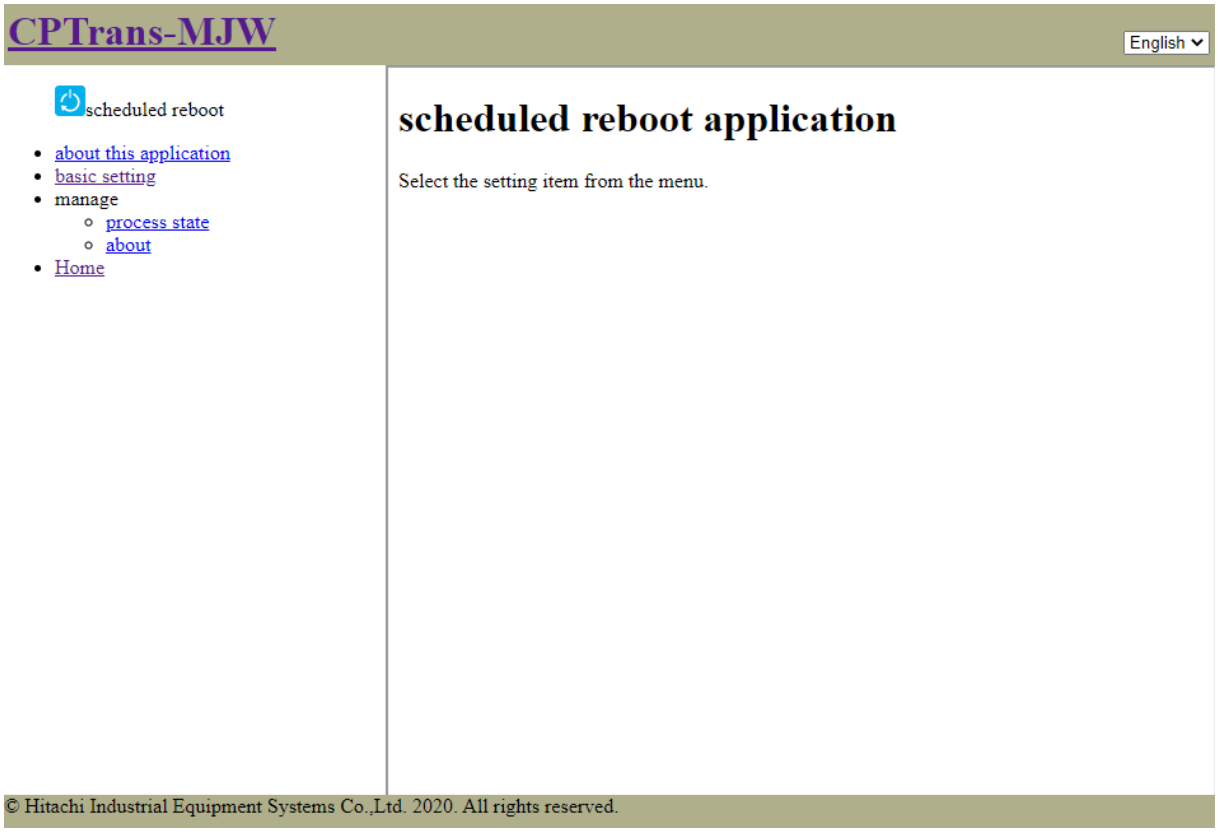



**Figure 5.30 Initial window for scheduled reboot application**

### 5.5.1 Basic setting

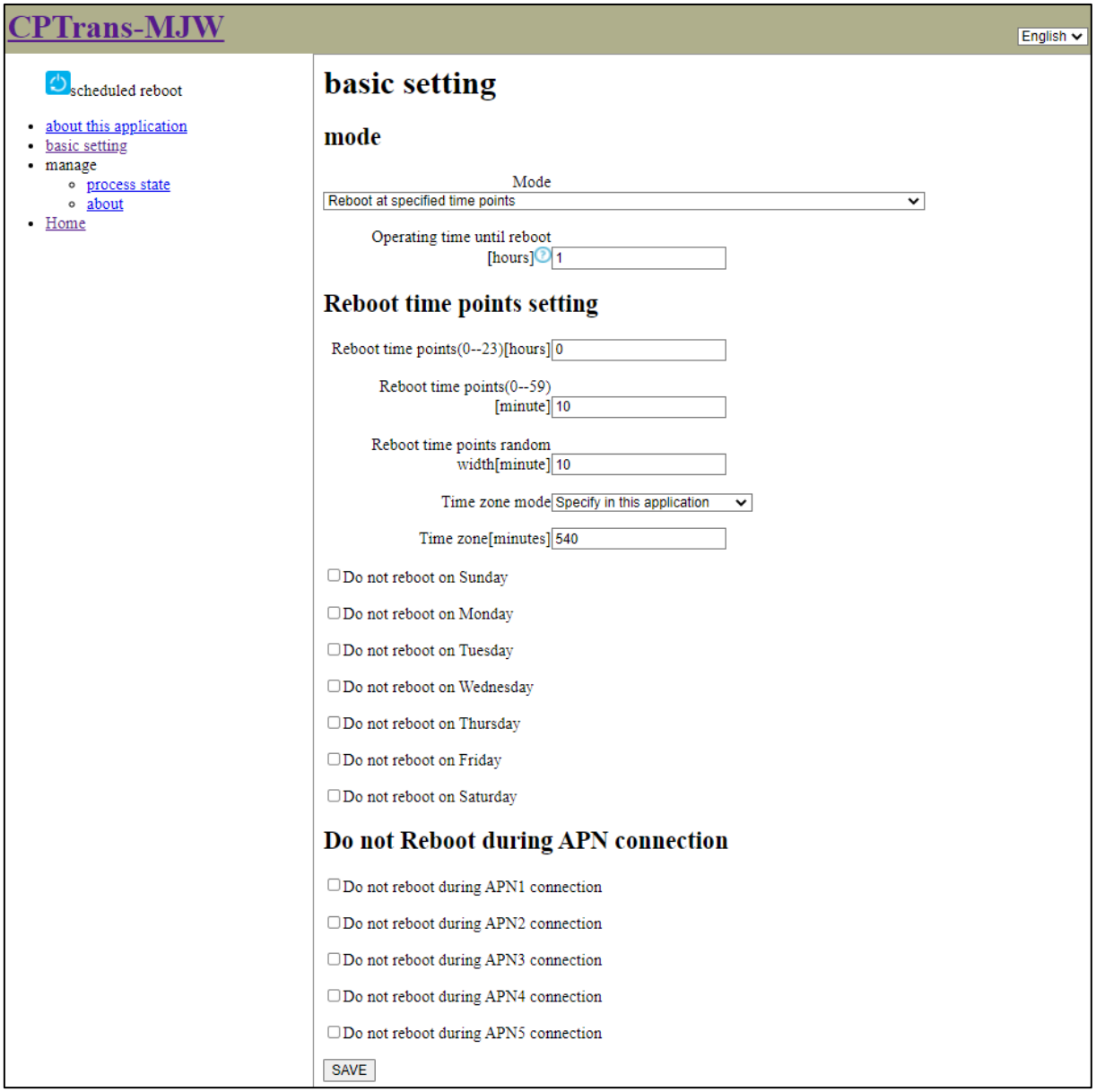



**Figure 5.31 Scheduled reboot basic setting window**

The basic settings screen details are shown below.

(1) Operation mode

| Item | Setting range |
|---|---|
| Mode | Do not perform a scheduled reboot |
| | Reboot at the specified time points |
| | Reboot when the specified operating time is exceeded |
| | When the specified operating time is exceeded, reboot is performed at the specified time points |

(2) Reboot time setting

| Item | Description |
|---|---|
| Reboot time points (0 to 23) [hour] | Specifies the time to reboot (time in 24-hour format).<br><br>Setting range: 0 to 23 [hour] |
| Reboot time points (0 to 59) [minute] | Specifies the time to reboot (time in 24-hour format).<br><br>Setting range: 0 to 59 [min] |
| Reboot time points random width [minute] | Specifies the random amplitude around the set reboot time.<br><br>Setting range: 10 to 1440 [min]<br>Note: It is determined by random in seconds. |
| Time zone [min] | Sets the time zone (in UTC) of the set reboot time.<br><br>Setting range :-1440～1440<br><br>Example: 540 (min.) for Japan Time (JST) |
| Do not reboot on Sunday | Checked: Do not reboot on Sunday |
| Do not reboot on Monday | Checked: Do not reboot on Monday |
| Do not reboot on Tuesday | Checked: Do not reboot on Tuesday |
| Do not reboot on Wednesday | Checked: Do not reboot on Wed |
| Do not reboot on Thursday | Checked: Do not reboot on Thursday |
| Do not reboot on Friday | Checked: Do not reboot on Friday |
| Do not reboot on Saturday | Checked: Do not reboot on Saturday |

(3) Reboot time setting

| Item | Description |
|---|---|
| Operating time until reboot [time] | Sets the operating time to reboot.<br>(1 to 720 hours) |

(4) Do not Reboot during APN connection

Restricts the automatic restart function when the APN is connected.

Example: If APN1 limit is enabled and APN1 is connected, the reboot doesn't occur after the specified time, day of the week, or uptime has elapsed. If the connection is broken, a reboot is performed immediately.

| Setting item | Description |
|---|---|
| Do not reboot while APN1 is connected | Checked: Do not reboot while APN1 is connected. |
| Do not reboot while APN2 is connected | Checked: Do not reboot while APN2 is connected. |
| Do not reboot while APN3 is connected | Checked: Do not reboot while APN3 is connected. |
| Do not reboot while APN4 is connected | Checked: Do not reboot while APN4 is connected. |
| Do not reboot while APN5 is connected | Checked: Do not reboot while APN5 is connected. |

## 5.6 Update

The update application is described below.

| Icon | Overview |
|---|---|
|  | This app accesses the server that manages the terminal, obtains the update file, and performs the update process. |

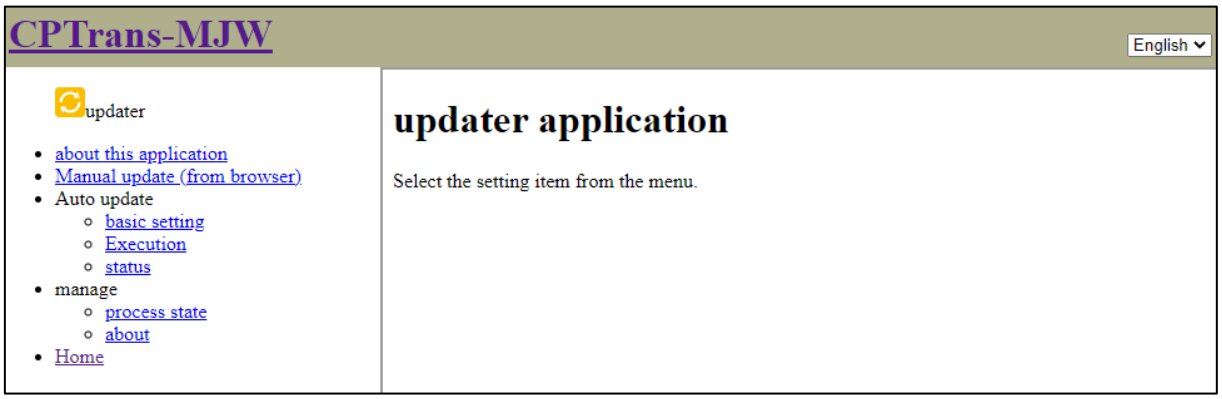



**Figure 5.32 Initial window of updater application**

### 5.6.1 Manual Update (from Browser)

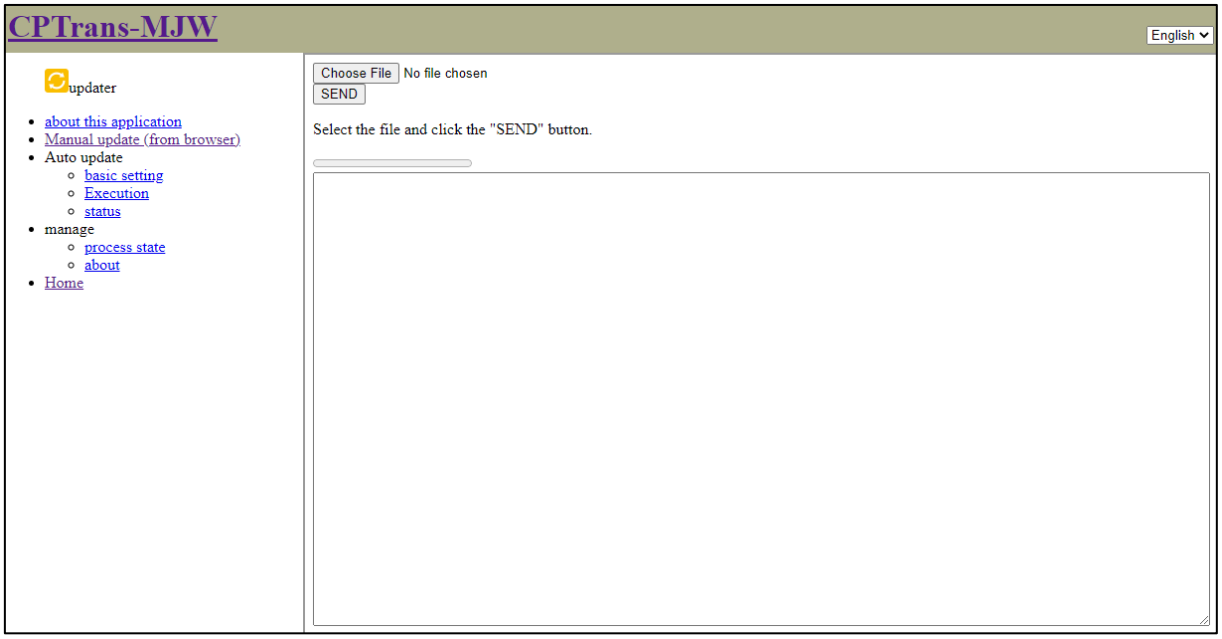



**Figure 5.33 Manual update**

The manual update procedure is shown below.

Manual Update Procedure

① [Choose file] Press the button.

② Select the firmware image file to download to the product.

③ [Send] Press the button.

④ The image file selected in step ② is downloaded.

⑤ After the download is complete, the image file is extracted.

※After the firmware upload is complete (after the image file is unpacked),

This product is set so that it will not be restarted automatically (the firmware will not be updated).

To apply the uploaded firmware, you must restart this product.

### 5.6.2 Auto update

#### 5.6.2.1 Basic setting

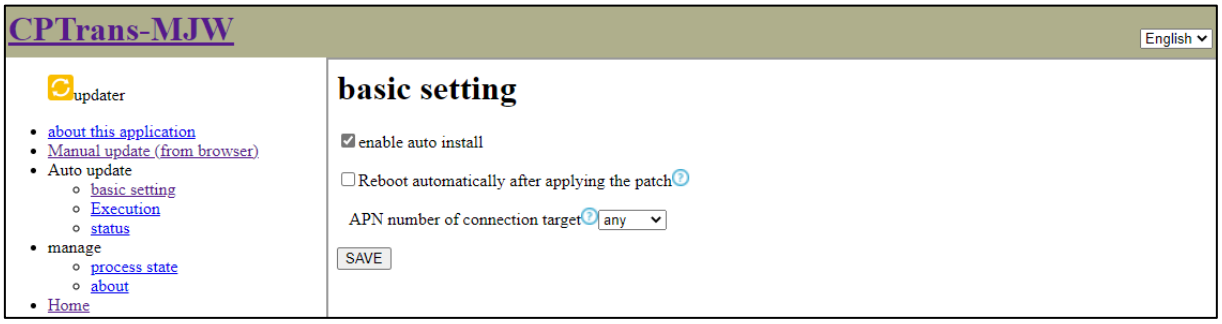



**Figure 5.34 Auto update basic setting**

The basic settings screen details are shown below.

(1) Basic setting

| Item | Description |
|---|---|
| Enable auto install | Enables or disables automatic installation.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Automatically reboot after patching | Specifies whether to automatically reboot after patching. |
| APN number to be connected | Specifies the APN number to be connected.<br><br>Setting range:<br>Optional, APN1～APN5 |

5.6.2.2 Execution

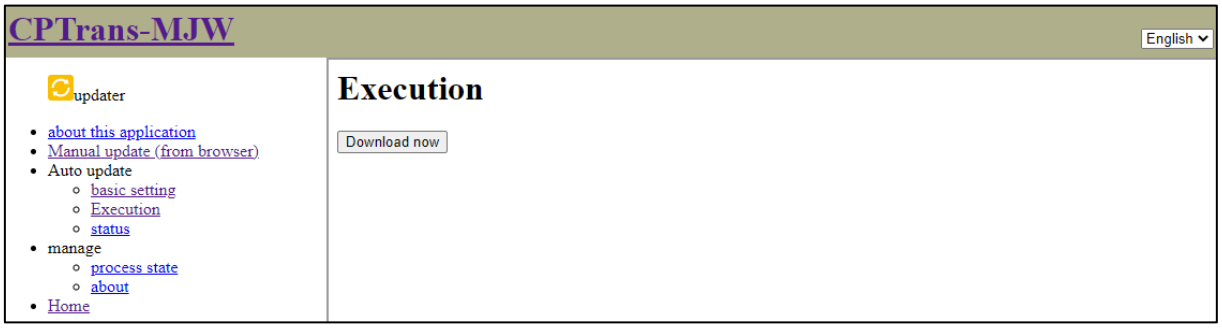



**Figure 5.35 Execution window**

5.6.2.3 Status

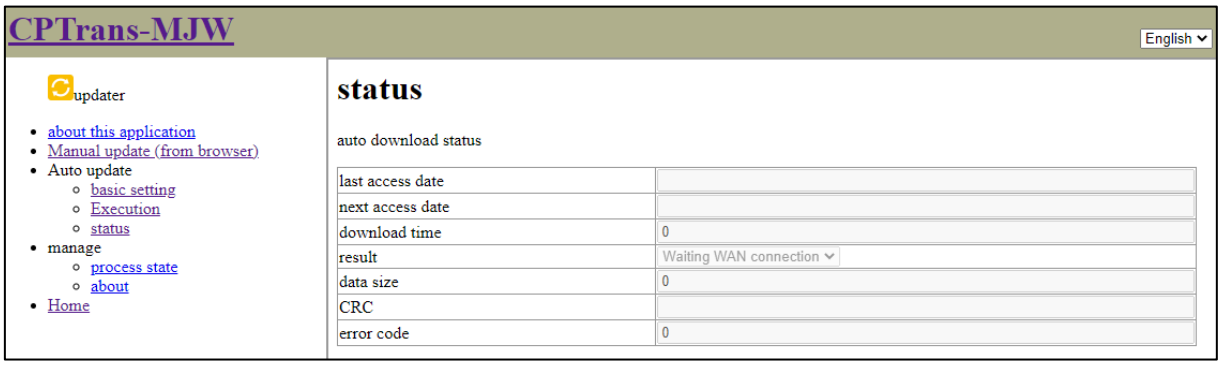



**Figure 5.36 Status window**

Details of the Status screen are shown below.

(1) Auto Download Status

| Item | Description |
|---|---|
| Last access date[sec] | The elapsed time since the last automatic update. |
| Next access date[sec] | Time remaining until the next automatic update. |
| Download time | Displays the time taken for downloading. |
| Result | Displays the results of the last automatic update.<br><br>Display contents:<br>0: None<br>1: No schedule<br>2: Running<br>3: Success (no data<br>4: Success (with data)<br>5: Interruption<br>6: Download failed<br>7: Deployment failure<br>8: Busy |
| Data size | Displays the downloaded data size. |
| CRC | Displays the CRC of the downloaded data. |
| Error code | If the status is invalid, an error code is displayed. |

## 5.7 SMS

The SMS application is described below.

| Icon | Overview |
|---|---|
|  | Receive SMS and leave it in the log. In addition, the application restarts or starts LTE communication when receiving. |

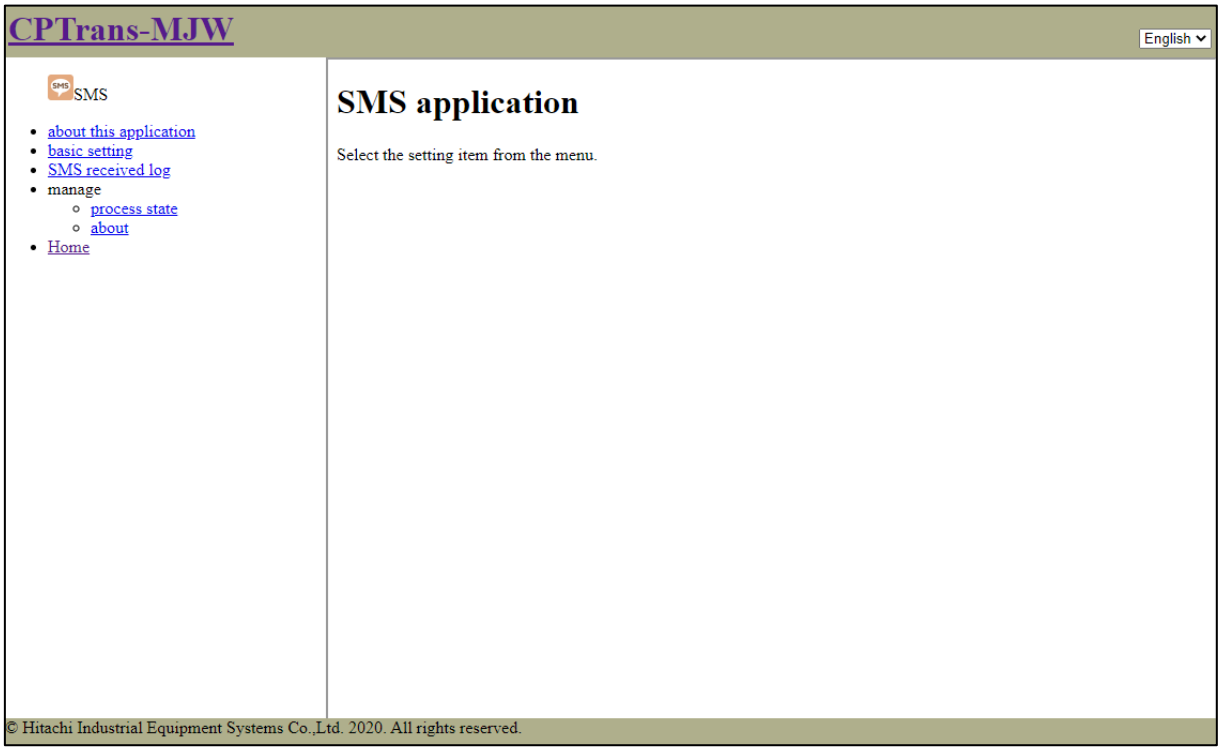



**Figure 5.37 Initial window of SMS application**

### 5.7.1 Basic setting

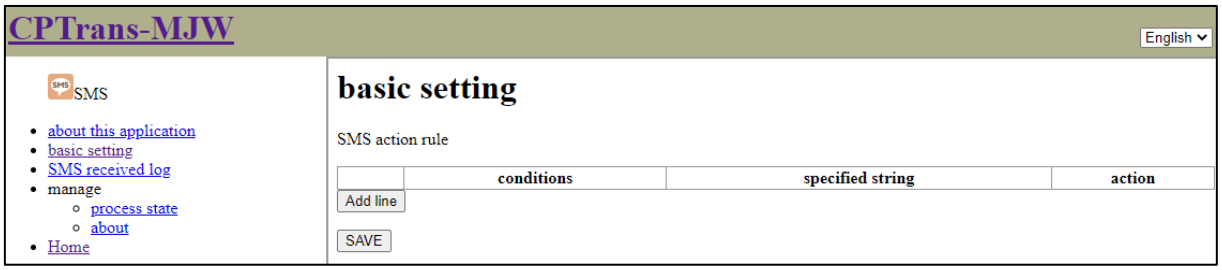



**Figure 5.38 SMS basic setting**

The basic settings screen details are shown below.

(1) SMS action rules

A rule for SMS action can be set by clicking Add line.

| Item | Description |
|---|---|
| Conditions | Specify the condition that triggers the action when receiving SMS.<br><br>Options:<br>・Disabled<br>・Match the specified string<br>・Contain the specified string |
| Specified string | Specifies the character string to be the action trigger. |
| Action | Specifies the action to take if the conditions are met.<br><br>Options:<br>0: Do nothing<br>1: Connect to APN1<br>2: Connect to APN2<br>3: Connect to APN3<br>4: Connect to APN4<br>5: Connect to APN5<br>101: Rebooted |

### 5.7.2 SMS received log

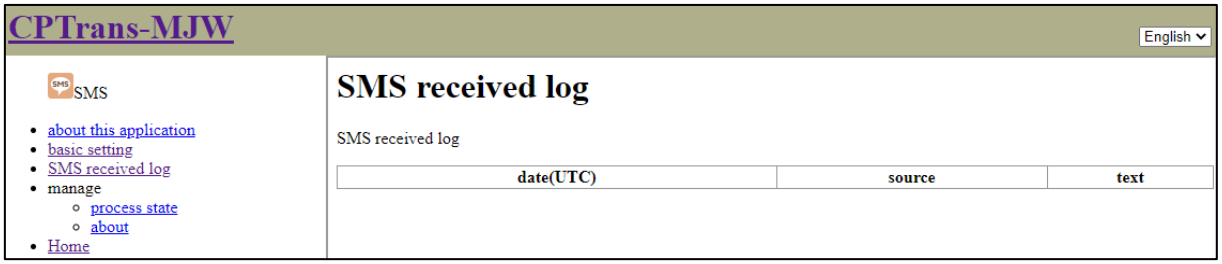



**Figure 5.39 SMS received log window**

The details of the "SMS reception log" screen are shown below.

(1) SMS received log

| Item | Description |
|---|---|
| Date (UTC) | The date and time when the SMS are received. |
| Source | The source of the SMS. |
| Text | The contents (text) of received SMS. |

## 5.8 Proxy

The proxy application is described below.

| Icon | Overview |
|---|---|
|  | Provides the ability to act as a proxy and respond on behalf.<br>This is an application that relays communications via this product and serves as a proxy for communications. |

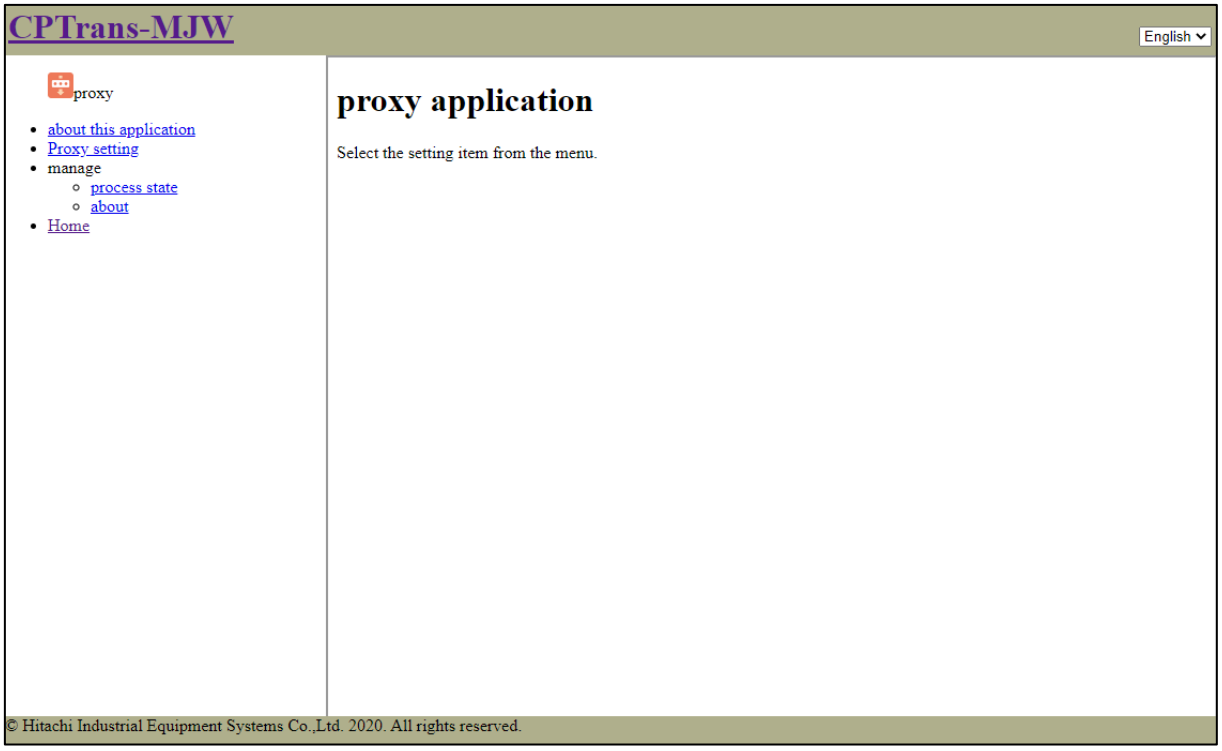



**Figure 5.40 Initial window of proxy application**

### 5.8.1 Proxy Settings

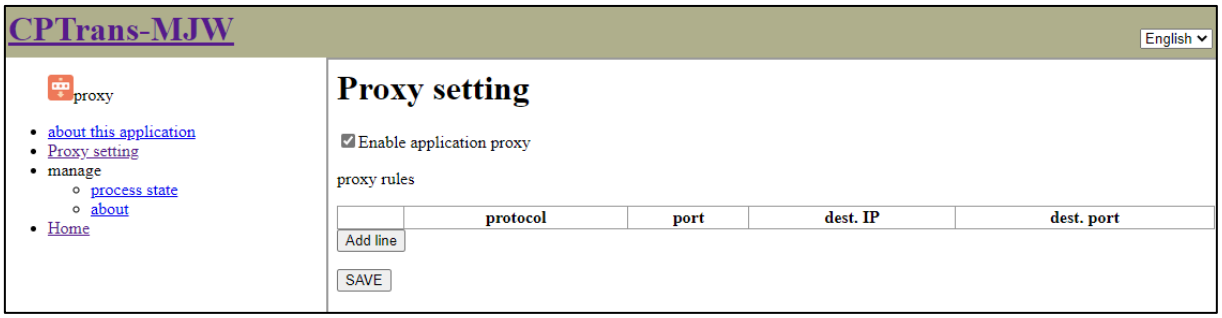



**Figure 5.41 Proxy setting window**

The details of the "Proxy setting" screen are shown below.

(1) Enable application proxy.

| Item | Description |
|---|---|
| Enable application Proxy | Enables or disables the proxy function.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |

(2) Proxy Rules

A proxy rule can be added by clicking Add line.

| Item | Description |
|---|---|
| Protocol | Specifies the protocol for which the proxy is to be enabled.<br><br>Options:<br>・TCP<br>・UDP<br><br>Remark: No matter the LAN or WAN.<br>* To access from the WAN, you must configure the port settings in Router > Access Control Settings. |
| Port | Specifies the source port on which to enable the proxy. |
| Dest. IP | Specifies the destination IP for which the proxy is to be enabled. |
| Dest. port | Specify the destination port on which to enable the proxy. |

## 5.9 NTPd

NTPd application is described below.

| Icon | Overview |
|---|---|
|  | Provides functions as an NTP (time synchronization) server.<br>When this function is enabled, it is an app that distributes its own time to the time request from the subordinate device. |


**Figure 5.42 Initial window of NTPd application**

### 5.9.1 Basic setting

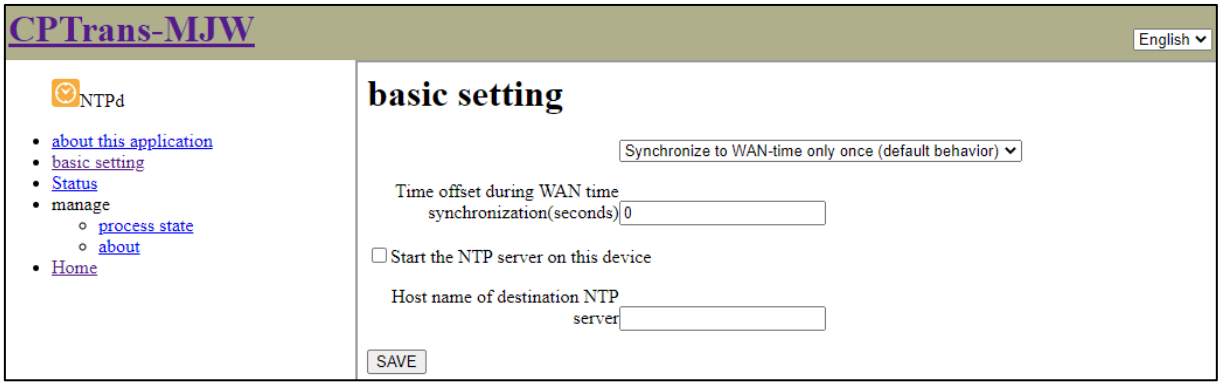



**Figure 5.43 NTPd basic setting**

The basic settings screen details are shown below.

(1) Basic setting

| Name | Description |
|---|---|
| Mode | Specify method for time synchronization. |
| Time offset during WAN time synchronization [sec] | Specify time offset when WAN time is synchronized. |
| Start the NTP server on this device | Enables or disables the NTPd function.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Host name of destination NTP server | Specify host name of destination NTP server |

### 5.9.2 Status

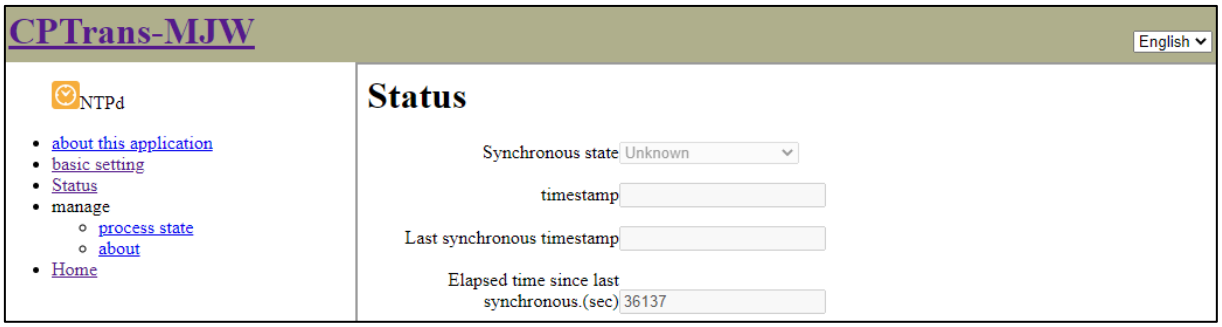



**Figure 5.44 NTPd status window**

The status screen details are shown below.

| Item | Description |
|---|---|
| Synchronous state | Display synchronous state |
| Timestamp | Display current timestamp |
| Last synchronous timestamp | Display last synchronized timestamp |
| Elapsed time since last synchronous [sec] | Display elapsed time since last synchronous |

## 5.10 DDNS general purpose

DDNS application is described below.

| Icon | Overview |
|---|---|
|  | Corresponds to DDNS of registering the IP address of the terminal and the domain name that uniquely corresponds when connecting to the Internet.<br>This is an application that requests updating to DDNS servers. |

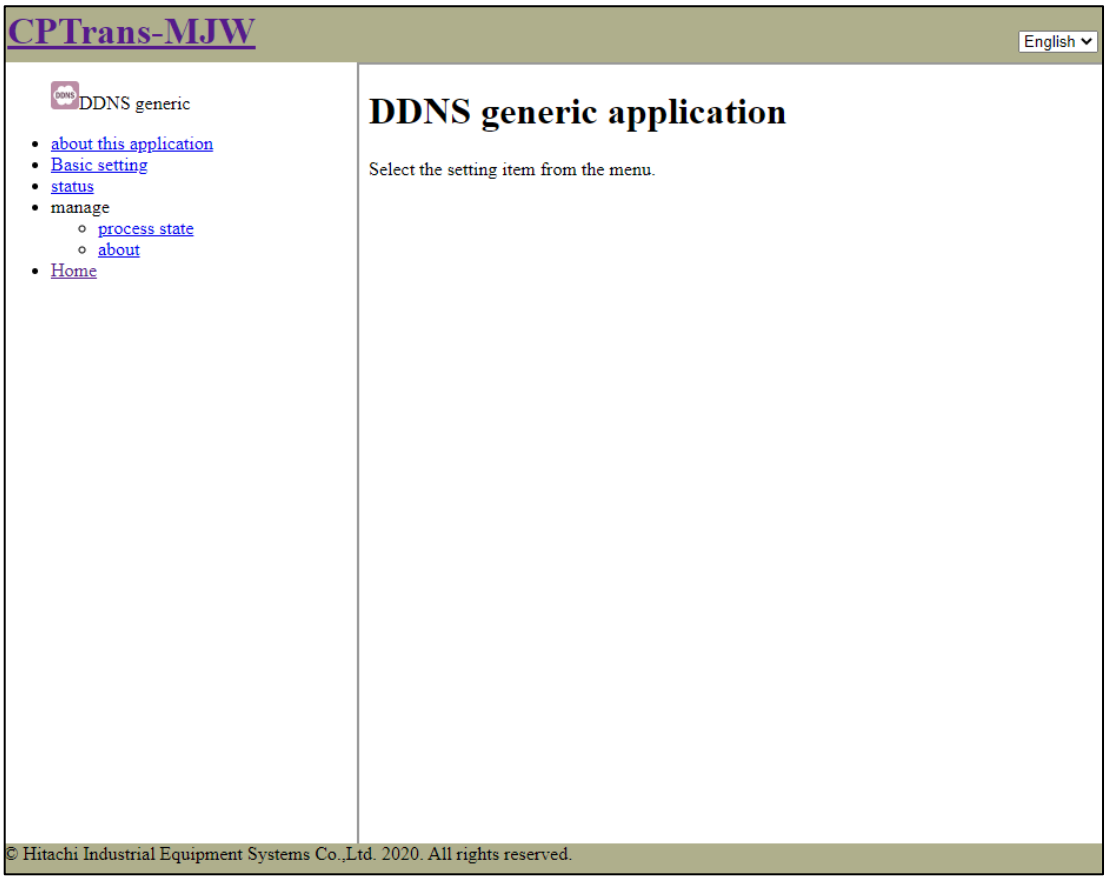



**Figure 5.45 Initial window of DDNS application**

### 5.10.1 Basic setting


**Figure 5.46 Basic setting window**

The basic setting items are shown below.

| Item | Description | Note |
|---|---|---|
| APN number of target | Specifies the APN number for DDNS function.<br>0: None<br>1 to 5: APN1 to APN5 | |
| Select a DDNS service | Specify DDNS service to be used.<br>0: customized<br>1: ieserver.net<br>2: mydns<br>3: no-ip | "ieserver.net" is not supported. |
| Account | Enter the account name (username or master ID) for accessing DDNS service. | When DDNS service="Customized" is selected, this value is ignored. |
| Password | Enter the security code (password) for accessing DDNS service. | When DDNS service="Customized" is selected, this value is ignored. |
| Hostname of DDNS service | Enter the hostname (or domain name) of the application to be registered with DDNS service. | When DDNS service="Customized" or "mydns" is selected, this value is ignored. |
| URL | Enter the requesting URLs for DDNS servers when “customized” is selected. | Configure the settings according to the specifications of your DDNS service. |

5.10.2 Status

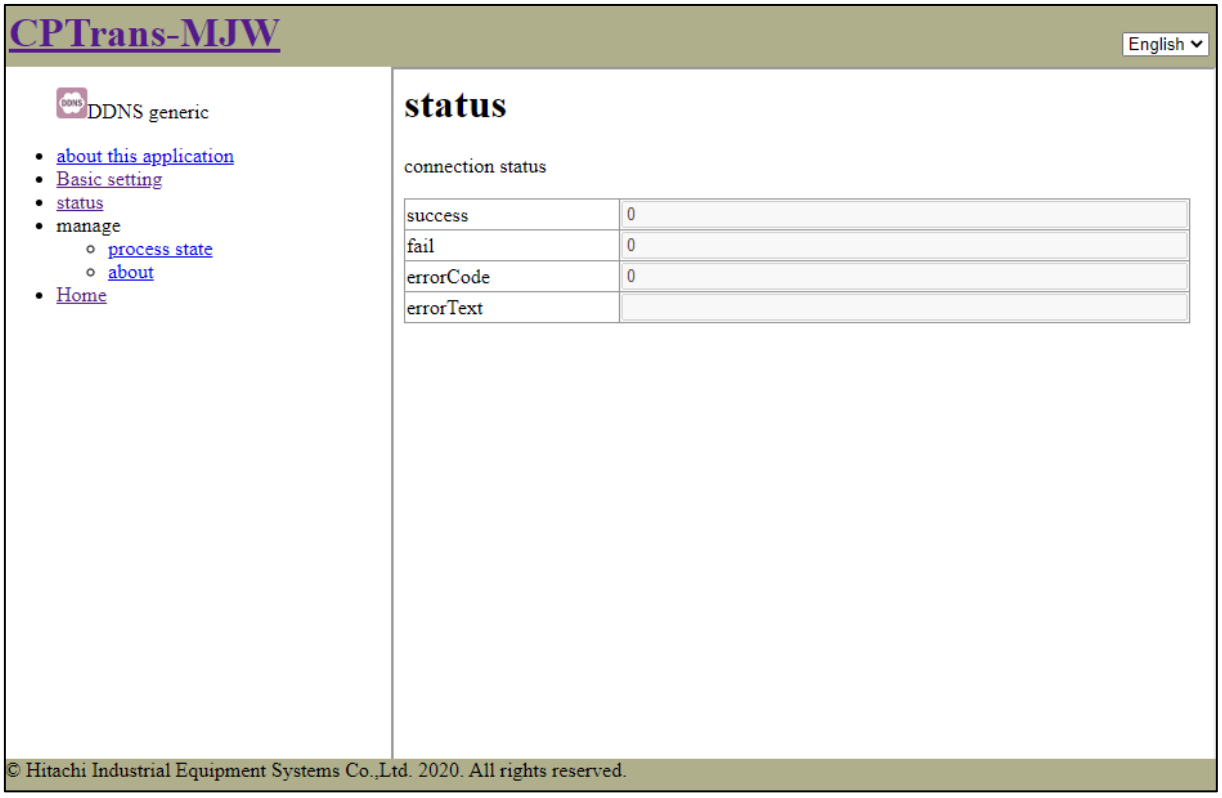



**Figure 5.47 Status window**

The status screen items are shown below.

| Item | Description |
|---|---|
| Success | Displays the number of times successfully updated to DDNS servers. |
| Fail | Displays the number of failed attempts to refresh DDNS servers. |
| ErrorCode | Displays the error code of the last error that occurred. |
| ErrorText | Displays the error message of the last error that occurred. |

## 5.11 Ping checker

Ping checker application is described below.

| Icon | Overview |
|---|---|
|  | A ping (communication confirmation packet) is sent to any IP address, and the result is acquired and displayed. Several ping can be set, and the fail-safe function is an application that can reboot according to the set number of ping calls. |

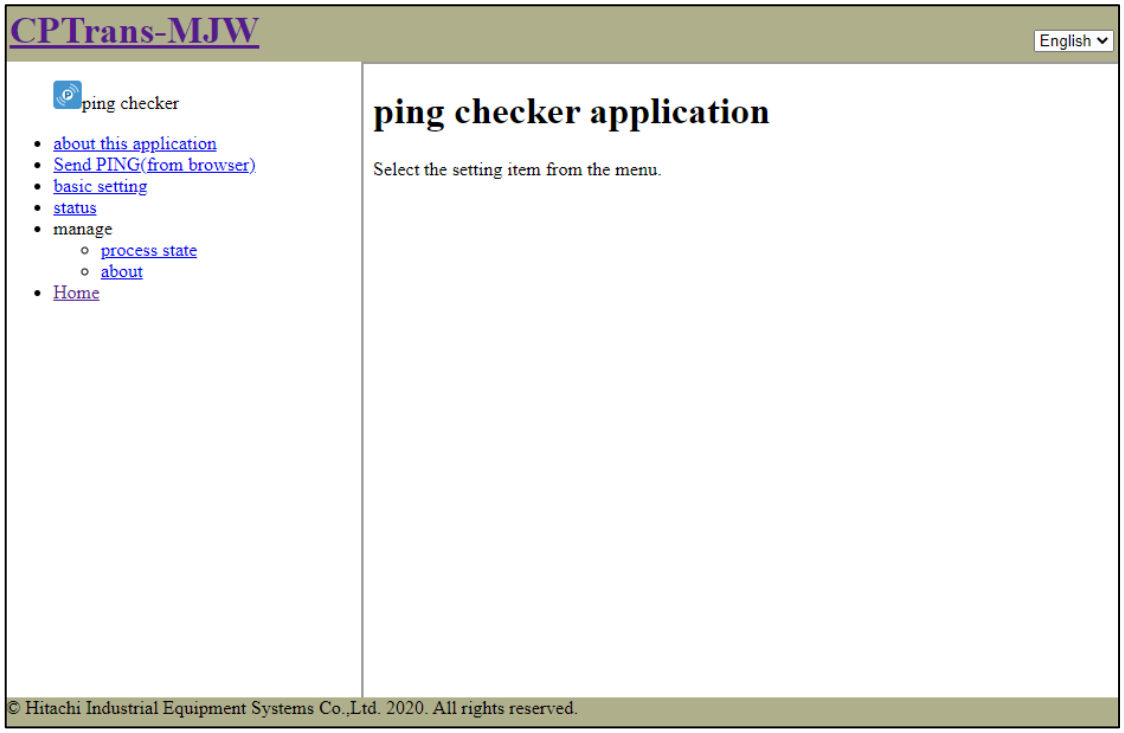



**Figure 5.48 Initial window of ping checker application**

### 5.11.1 Basic setting

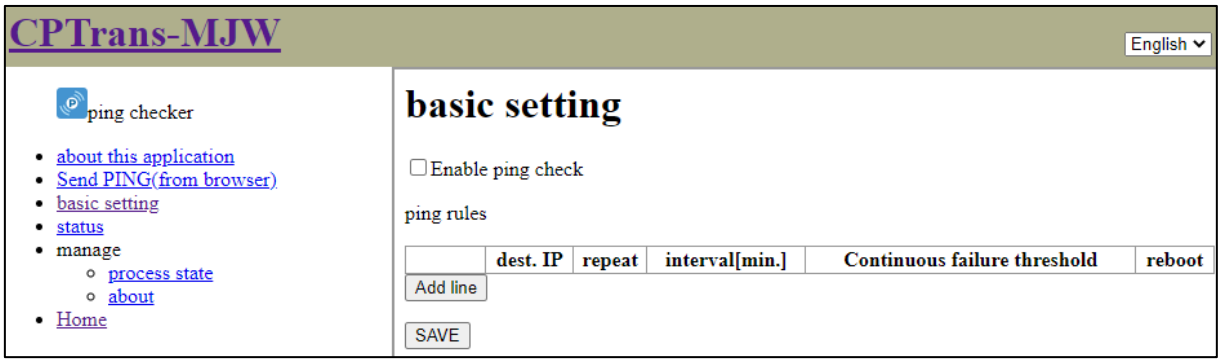



**Figure 5.49 Basic setting**

The basic settings screen details are shown below.

(1) Enable ping check

| Item | Description |
|---|---|
| Enable ping checking. | Enables or disables periodic sending of ping set by ping.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |

(2) Ping rules

| Item | Description |
|---|---|
| Dest. IP | Sets ping destination. |
| Repeat | Sets the number of times ping is sent. |
| Interval [min] | Set ping send interval [min]. |
| Continuous failure Threshold | Sets the threshold for consecutive failed ping transmissions required when Reboot is enabled. |
| Reboot | Specifies whether rebooting is enabled or disabled when ping reply fails "Continuous Failure Threshold".<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |

5.11.2 Status

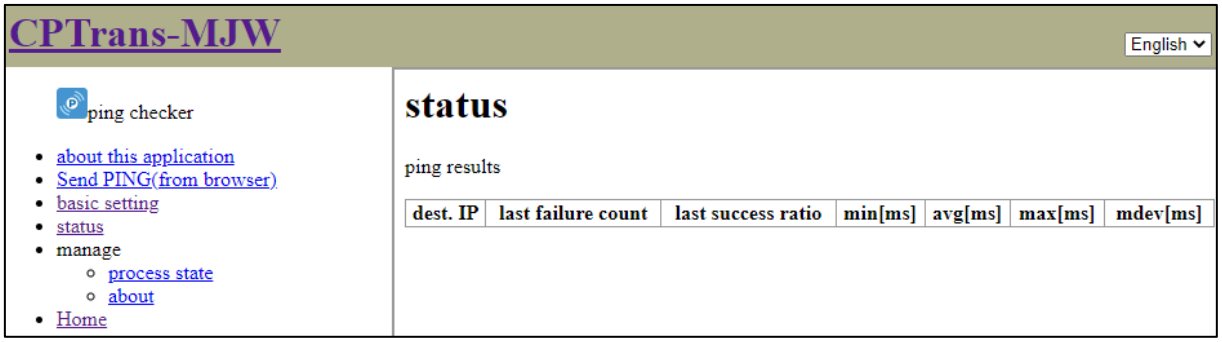



**Figure 5.50 Status window**

Details of the Status screen are shown below.

(1) Ping executions

| Item | Description |
|---|---|
| Dest. IP | Displays ping destination. |
| Last failure count | Number of consecutive failures of ping transmissions just before |
| Last success ratio | Success rate at the last ping transmission<br><br>Example :0→0%、1→100% |
| Min [ms] | The smallest ping turnaround [ms] during the last ping transmit is displayed. |
| Avg [ms] | The averaged ping turnaround during the last ping transmit [ms] is displayed. |
| Max [ms] | The highest ping turnaround [ms] during the last ping transmit is displayed. |
| mdev [ms] | The standard-deviation [ms] of ping turnaround during the last ping transmit is displayed. |

## 5.12 Location

Location applications are described below.

| Icon | Overview |
|---|---|
|  | The current location of this product can be displayed. |

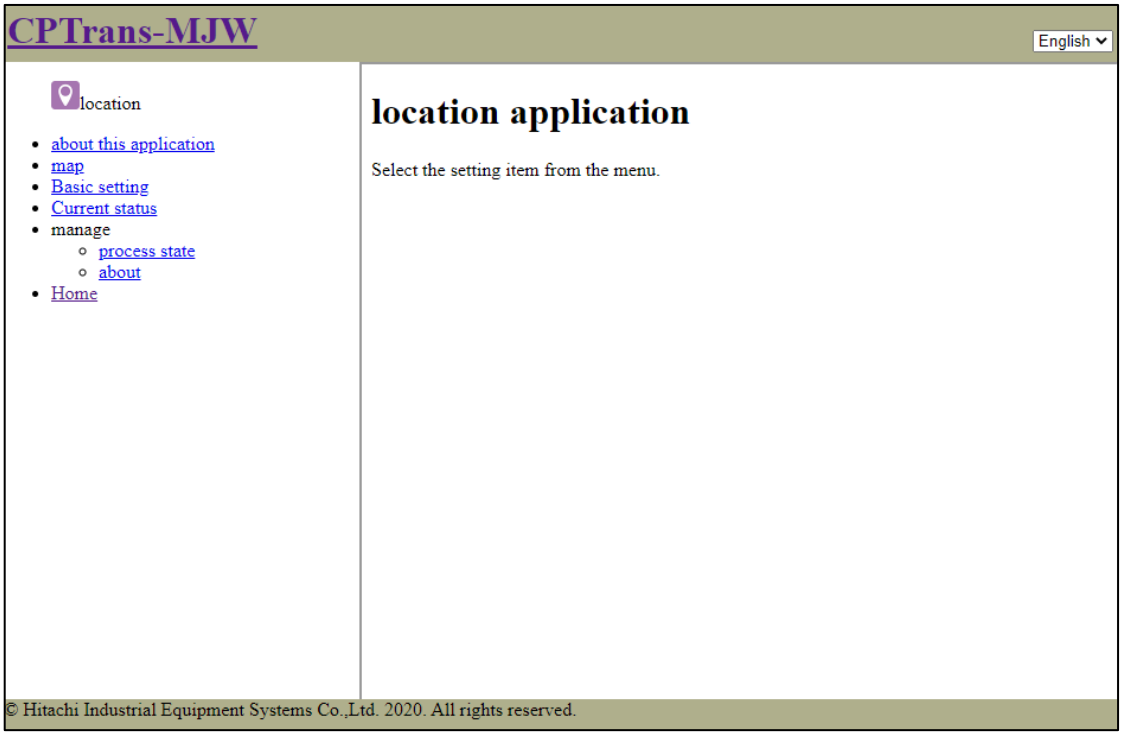



**Figure 5.51 Initial window of location application**

### 5.12.1 Map display

A map based on the location information data is displayed.

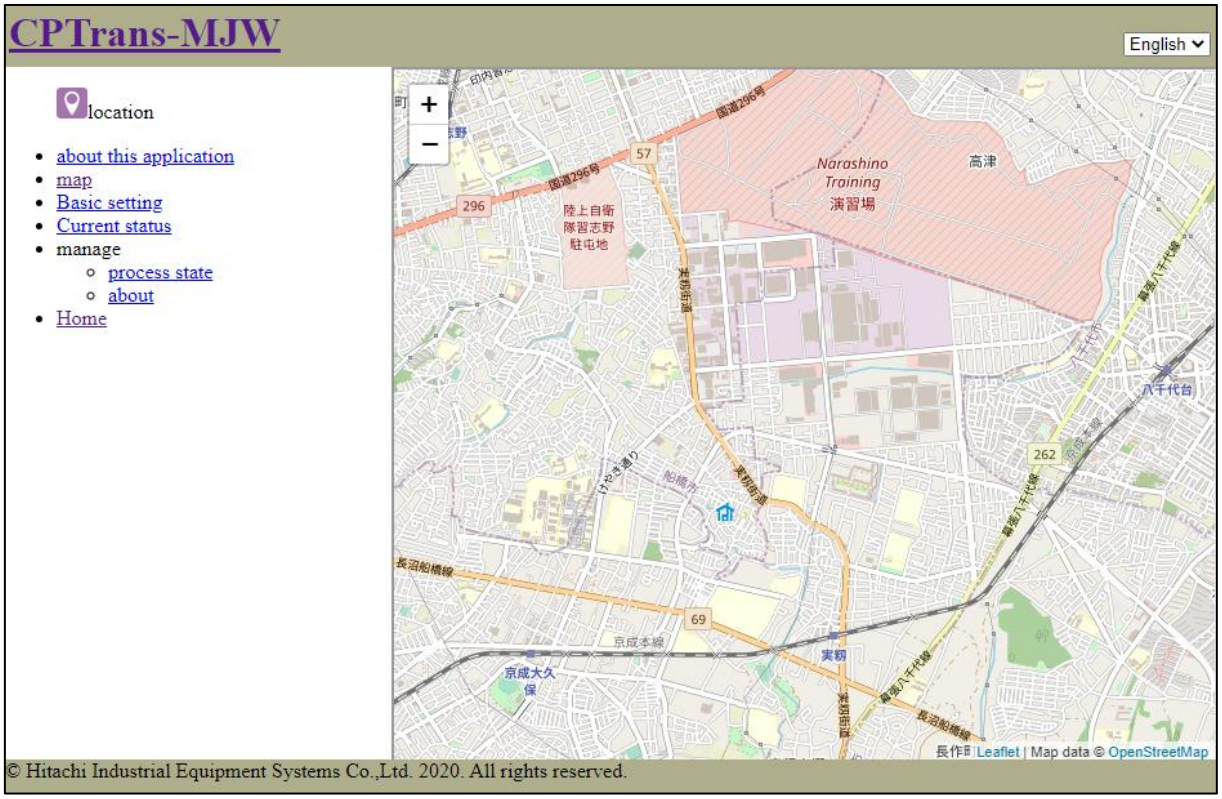



**Figure 5.52 Map window**

5.12.2 Basic setting

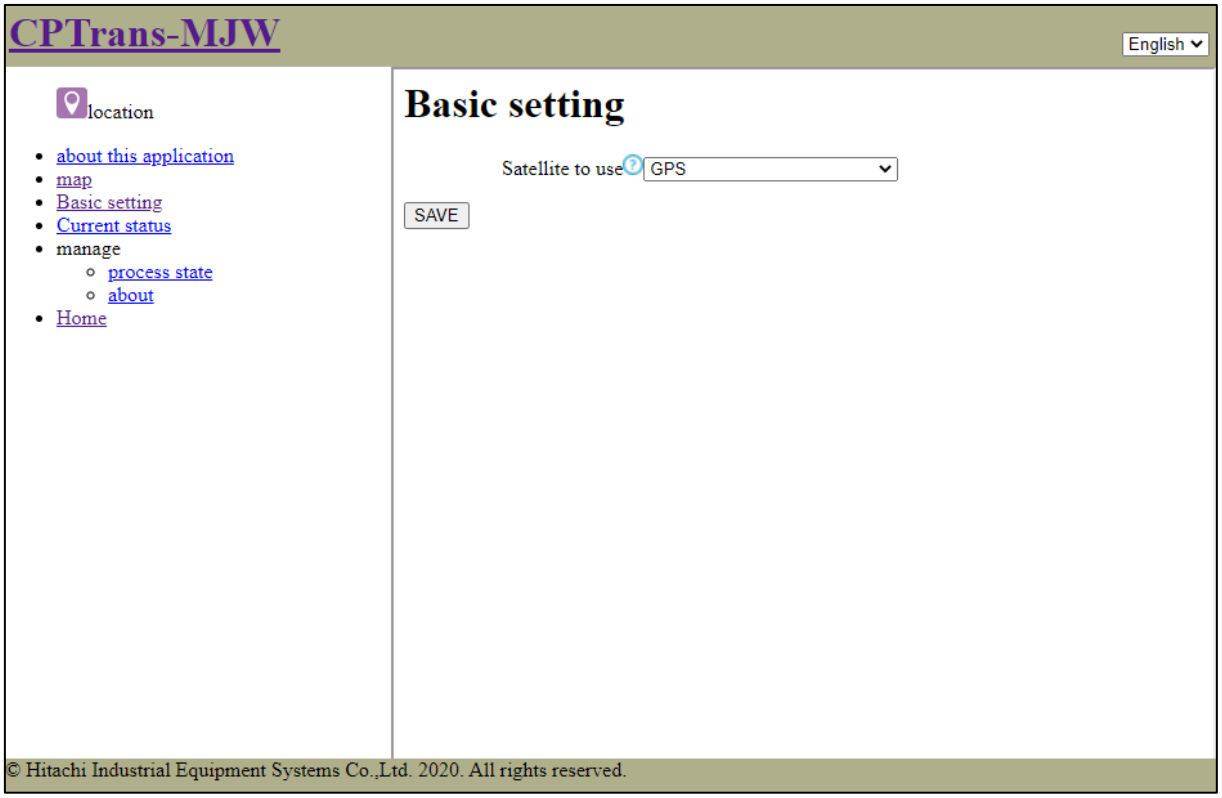



**Figure 5.53 Basic setting**

The basic settings screen details are shown below.

(1) Current status

| Name | Description |
|---|---|
| Satellites used | Select the satellite to be used.<br><br>・GPS* default value<br>・GPS,Glonass,BeiDou,Galileo<br>・GPS,Glonass,BeiDou<br>・GPS,Glonass,Galileo<br>・GPS,Glonass<br>・GPS,BeiDou,Galileo<br>・GPS,Galileo |

5.12.3 Current status

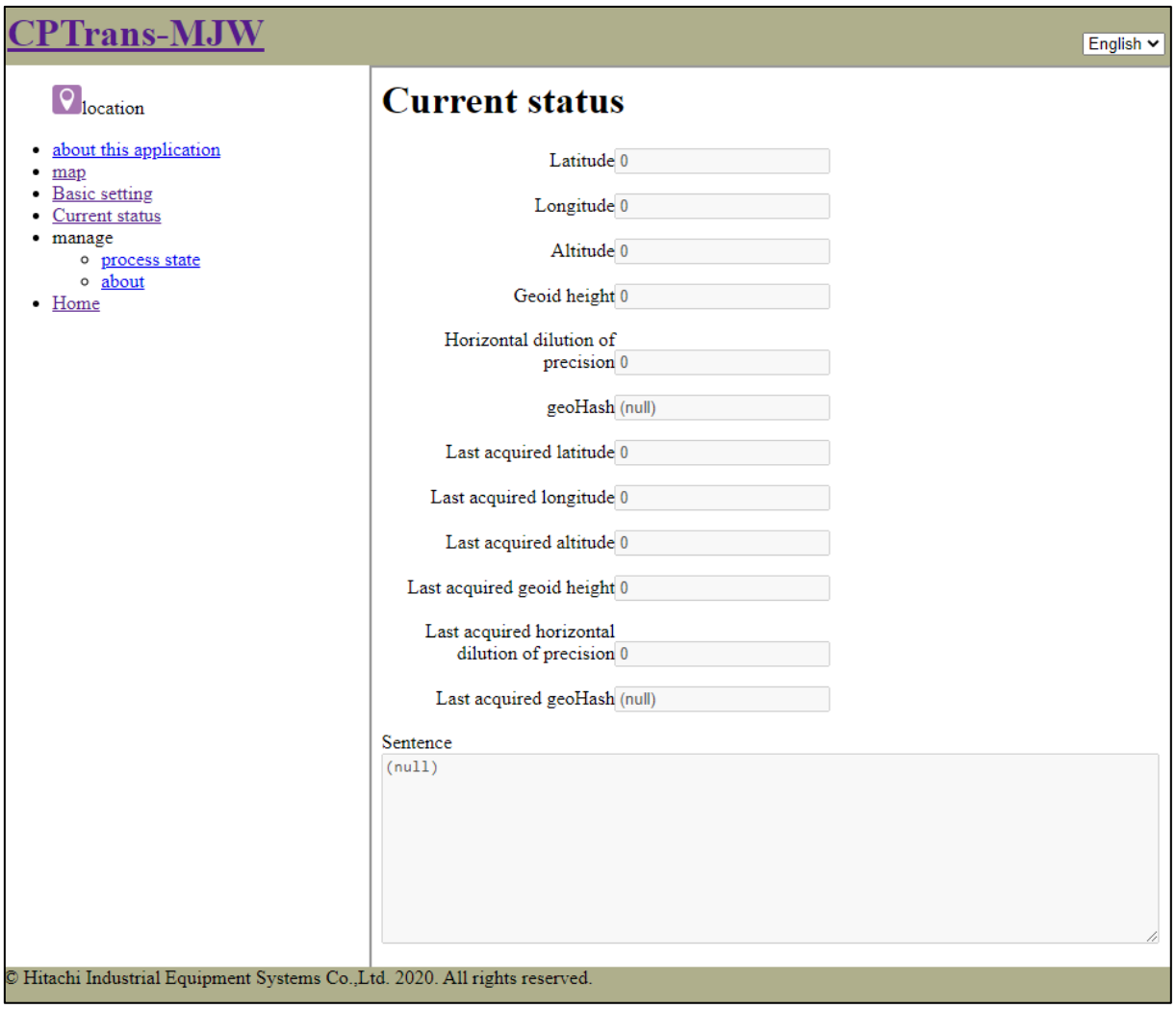



**Figure 5.54 Current status**

Details of the Current Status screen are shown below.

(2) Current status

| Item | Description |
|---|---|
| Latitude | Latitude [degree] is displayed. |
| Longitude | Longitude [degree] is displayed. |
| Altitude | Altitude [m] is displayed. |
| Geoid height | The geoid height [m] is displayed. |
| Horizontal accuracy drop rate | Horizontal accuracy reduction rate is displayed. |
| GeoHash | GeoHash is displayed in 12-digit format.<br>If GNSS is difficult to receive, it will be empty. |
| Last Latitude Acquired | Lastly acquired latitude [degree] is displayed. |
| Last Acquired Longitude | The longitude [degree] obtained last is displayed. |
| Last acquired altitude | The altitude [m] obtained last is displayed. |
| Last acquired geoid height | The last acquired geoid height [m] is displayed. |
| Last Horizontal Accuracy Loss Rate Acquired | The last obtained horizontal accuracy reduction rate is displayed. |
| Last geoHash retrieved | The last acquired geoHash is displayed in 12-digit format.<br>If GNSS is difficult to receive, it will be empty. |
| Sentence | The acquired GNSS data (sentences) are displayed. |

## 5.13 Iopoll

Iopoll application is described below.

| Icon | Overview |
|---|---|
|  | Modbus application sends an informational requisition,<br>Send a request to MQTT, REST application to send the collected data.<br>The connection settings for each protocol are made by the application dedicated to each protocol. |

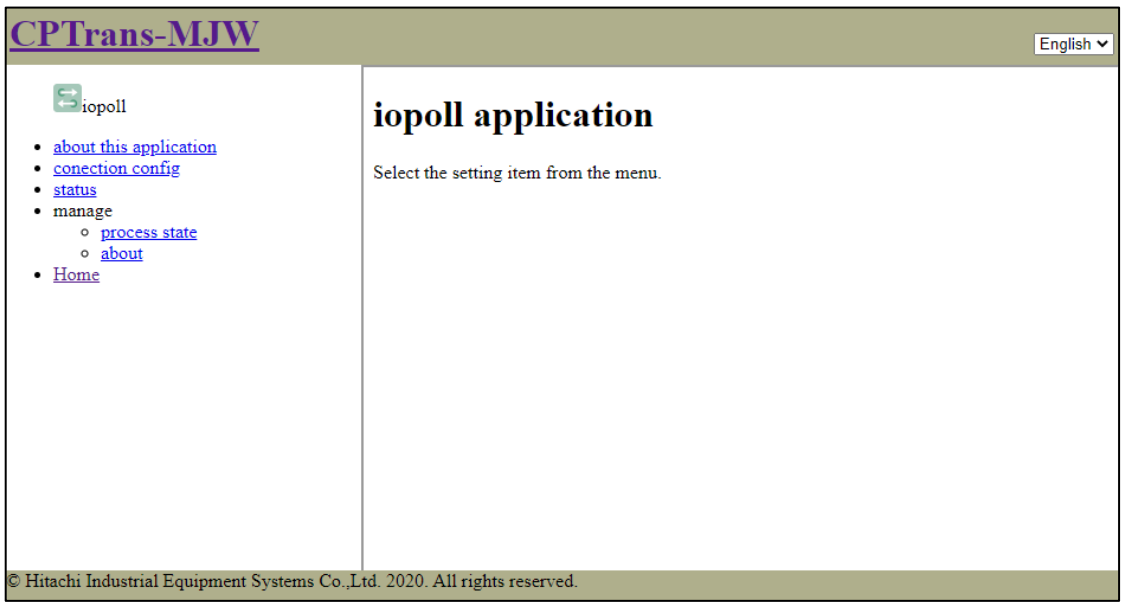



**Figure 5.55 Initial window of iopoll application**

### 5.13.1 Connection setting

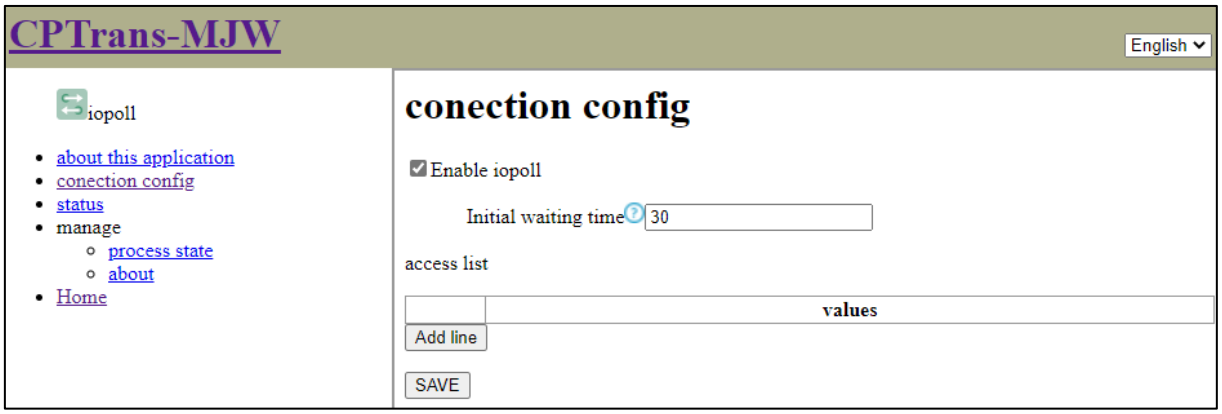



**Figure 5.56 Connection config**

Details of the "Connection config" screen are shown below.

(1) Access list

| Item | Description |
|---|---|
| Dest. | Specifies the destination application (MQTT or REST).<br><br>For MQTT: mqtt.[key]<br>For REST: rest.[key]<br>※[key] is an arbitrary key value. Used for processing sorting in the destination application |
| Text | Specifies the text that composes the transmitted data.<br><br>Setting range: Up to 20000 half-width characters ($ number of characters before replacement) |
| Input timeout (ms) | Specifies the time-out period when collecting data from Modbus app (on entry).<br><br>Setting range: 1 to 10000ms |
| Output Timeout (ms) | Specifies the time-out period when sending a request to MQTT or REST (when outputting).<br><br>Setting range: 1 to 10000ms |
| Interval (sec.) | Specify the time interval at which to retrieve information and notify other applications of text.<br><br>Setting range: 1 s or more |

### 5.13.2 Status

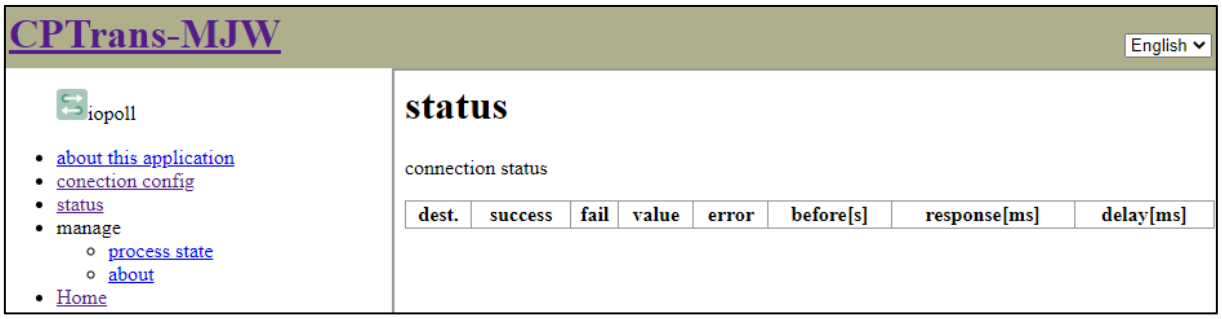



**Figure 5.57 Status**

Details of the Status screen are shown below.

(1) Connection Status

| Item | Description |
|---|---|
| Dest. | Displays the destination application. |
| Success | The number of times a request was sent to the destination application. |
| Fail | The number of times a request could not be sent to the destination application. |
| Value | Content of the most recently sent text (value after conversion). |
| Error | Error information from the previous request. |
| Before [sec] | Elapsed time from the last request transmission [s]. |
| Response [ms] | Response time until the text value is retrieved during the previous request. |
| Delay [ms] | The delay time in the last request. |

## 5.14 Modbusio

Modbusio application is described below.

| Icon | Overview |
|---|---|
|  | It becomes Modbus master and supports the function to acquire and change registers of slave devices. |

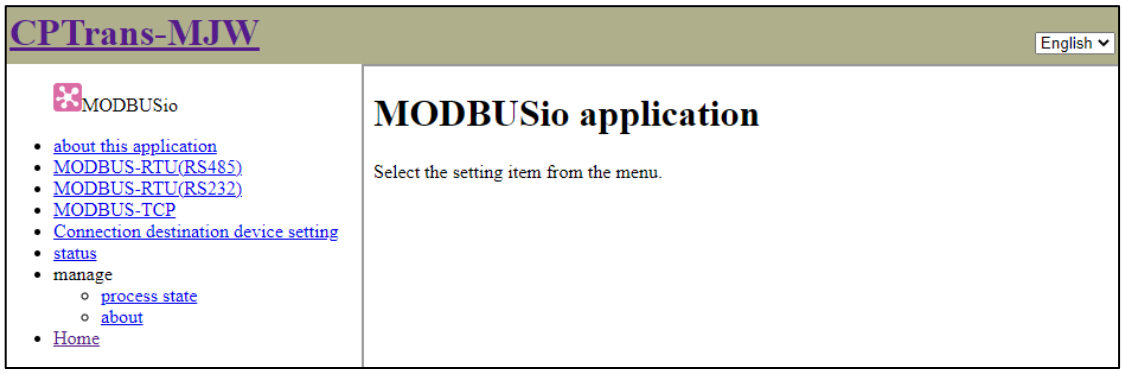



**Figure 5.58 Initial window of MODBUSio application**

### 5.14.1 MODBUS-RTU(RS485)

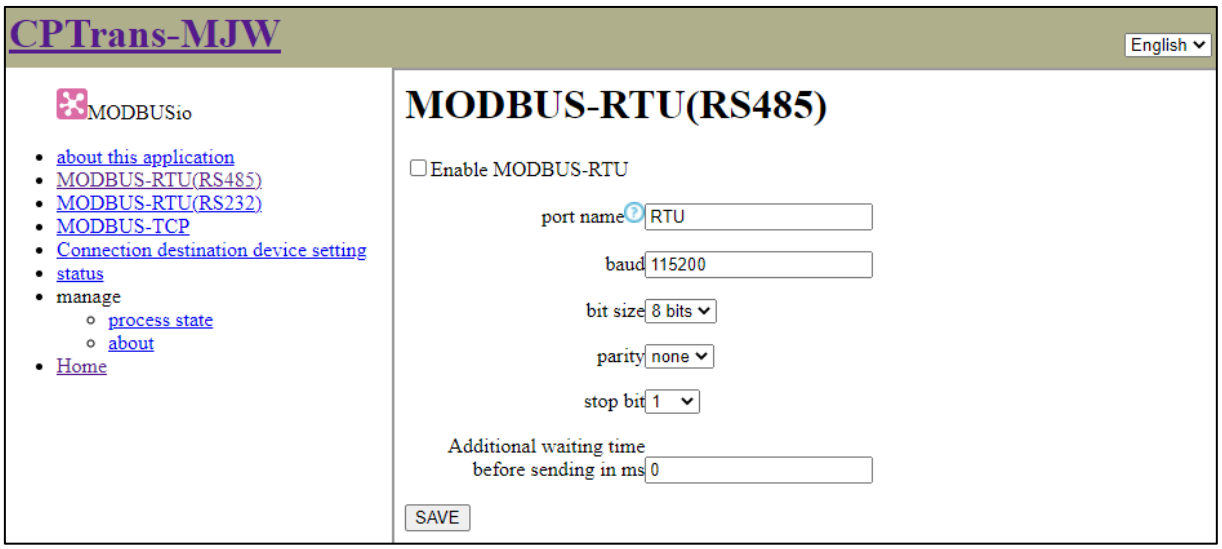



**Figure 5.59 MODBUS-RTU (RS485)**

MODBUS-RTU(RS485) window is detailed below.

(1) MODBUS-RTU(RS485) Setting

| Item | Description |
|---|---|
| Enable MODBUS-RTU | Enables or disables MODBUS-RTU function.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Port name | Specify the port name described in the connection destination device setting. |
| Baud rate | Specify the baud rate.<br>Setting range: Within 1000000<br>(Within 250000 for RS232) |
| Size | Specifies the size of the data bit.<br>Options:<br>7: 7 bits<br>8: 8 bits |
| Parity | These bits specify the parity bit setting.<br>Options:<br>0: None 1: Even 2: Odd |
| Stop bit | Specify the stop bit setting.<br>Options:<br>0: 1 bit<br>1: 1.5 bits<br>2: 2 bits |
| Wait time before sending [ms] | Specifies the wait time to be set before sending.<br>Setting range: Within 1000 ms |

### 5.14.2 MODBUS-RTU(RS232)

The setting display and details are the same as those in 5.13.1 MODBUS-RTU(RS485).

### 5.14.3 MODBUS-TCP

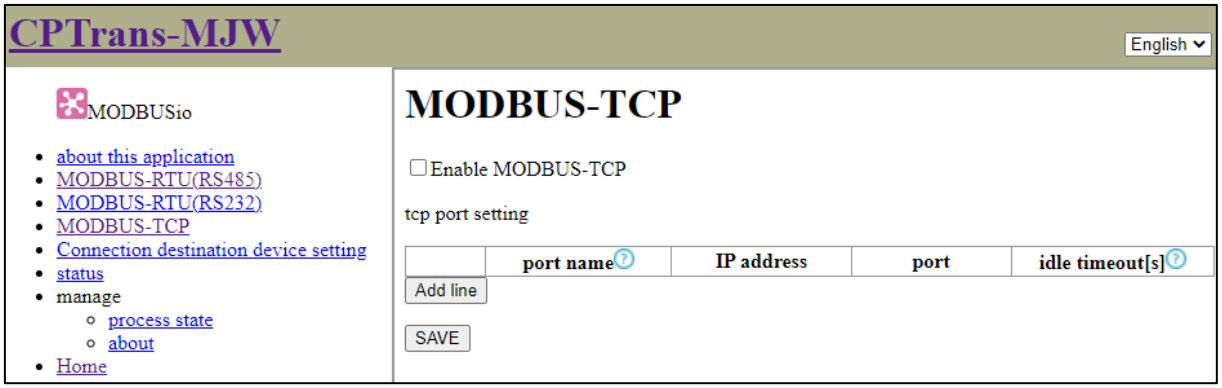



**Figure 5.60 MODBUS-TCP**

MODBUS-TCP window is detailed below.

(1) MODBUS-TCP setting

| Item | Description |
|---|---|
| Enable MODBUS-TCP | Enables or disables MODBUS-TCP function.<br>(Items added to TCP port settings)<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |

(2) TCP port settings

| Item | Description |
|---|---|
| Port name | Specify the port name described in the connection destination device setting. |
| IP address | Specifies the IP address of the TCP connection destination. |
| Port | Specifies the port number of the TCP connection destination.<br><br>Setting range: 0 to 65535 |
| Idle Timeout (seconds) | TCP is disconnected when communication is interrupted for a specified period.<br>If it is 0, its connection is not cut.<br><br>Setting range :0～65535 |

5.14.4 Connection destination device setting

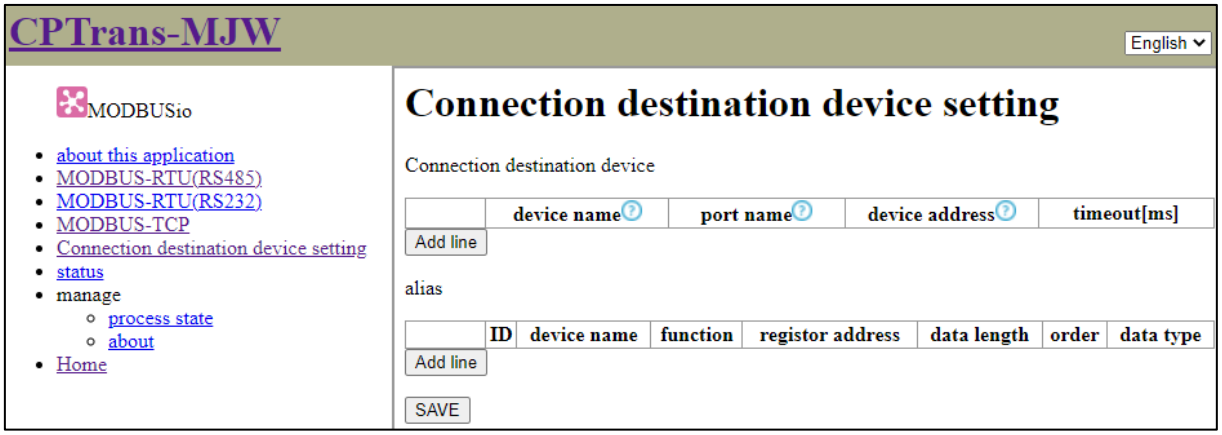



**Figure 5.61 Connection destination device setting**

The details of the "Connection destination device setting" screen are shown below.

(1) Destination device

| Item | Description |
|---|---|
| Device name | Set any device-name specified in iopoll application.<br>Format: 1 or more characters |
| Port name | Describes the port name specified in Modbus-RTU and TCP settings to distinguish the RTU and TCP ports.<br>Format: 1 or more characters |
| Device advice | Indicates the slave address (unit identification) of Modbus. |
| Timeout | Specify the timeout period. |

(2) Alias

| Item | Description |
|---|---|
| ID | Defines an alias for the key name. |
| Device name | Set any device-name specified in iopoll application.<br>Format: 1 or more characters |
| Function | Specify the function code.<br><br>Setting range: 0 to 3<br>0: coil<br>1: input register<br>2: holding register<br>3: discrete |
| Register address | Specifies the address of the register. |
| Data length | Specify the number of registers to be acquired consecutively. |
| Order | Specify the order of the data to be read.<br>Setting range: 0 to 1<br>0: H-L order<br>1: L-H order |

| Item | Description |
|---|---|
| Data type | Specifies the data type.<br>Setting range: 0 to 3<br>0: Unsigned<br>1: Signed<br>2: BCD<br>3: Binary |

### 5.14.5 Status

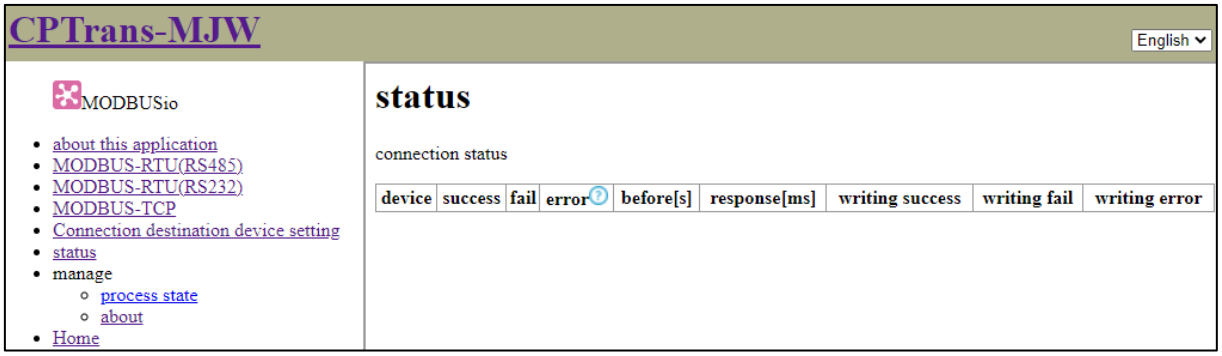



**Figure 5.62 Status**

Details of the Status screen are shown below.

(1) Connection status

| Item | Description |
|---|---|
| Device | The device name of the connection destination. |
| Success | This is the number of times register value acquisition was successful. |
| Fail | Number of times register value acquisition failed. |
| Error | Error code of the last acquisition. |
| Before [sec] | Elapsed time from the last acquired time [sec] |
| Response [ms] | The last response time [milliseconds]. |
| Writing Success | This is the number of times the register value was written successfully. |
| Writing fail | This is the number of register value write failures. |
| Writing error | Error code from previous write. |

## 5.15 mqttio

Mqttio application is described below.

| Icon | Overview |
|---|---|
|  | It supports the ability to upload various types of data using MQTT protocols. |

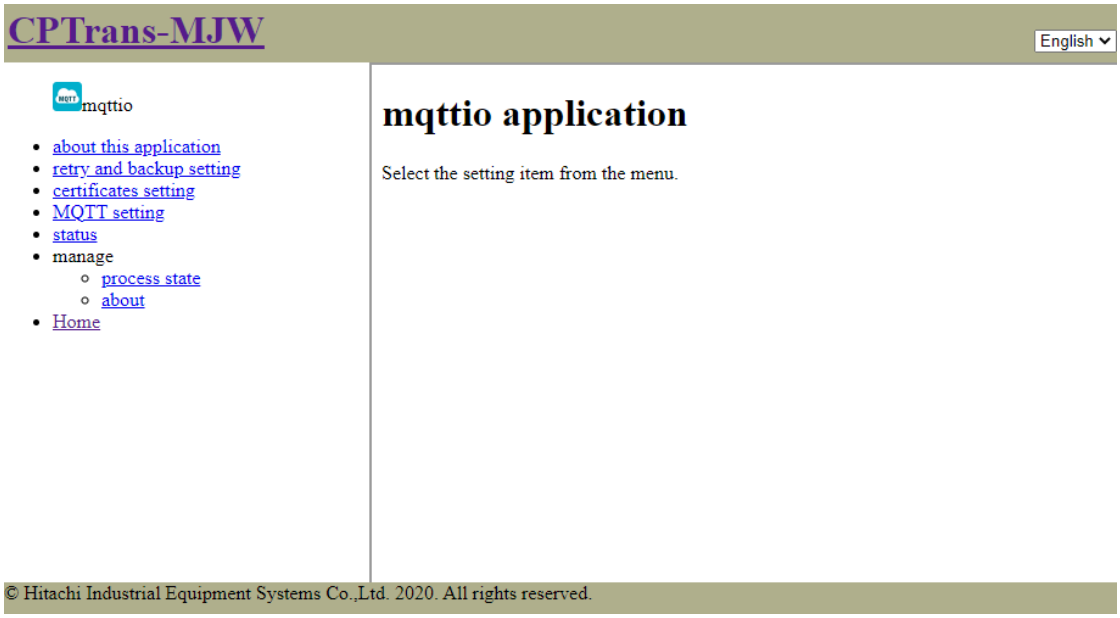



**Figure 5.63 Initial window of mqttio application**

### 5.15.1 Retry and backup setting

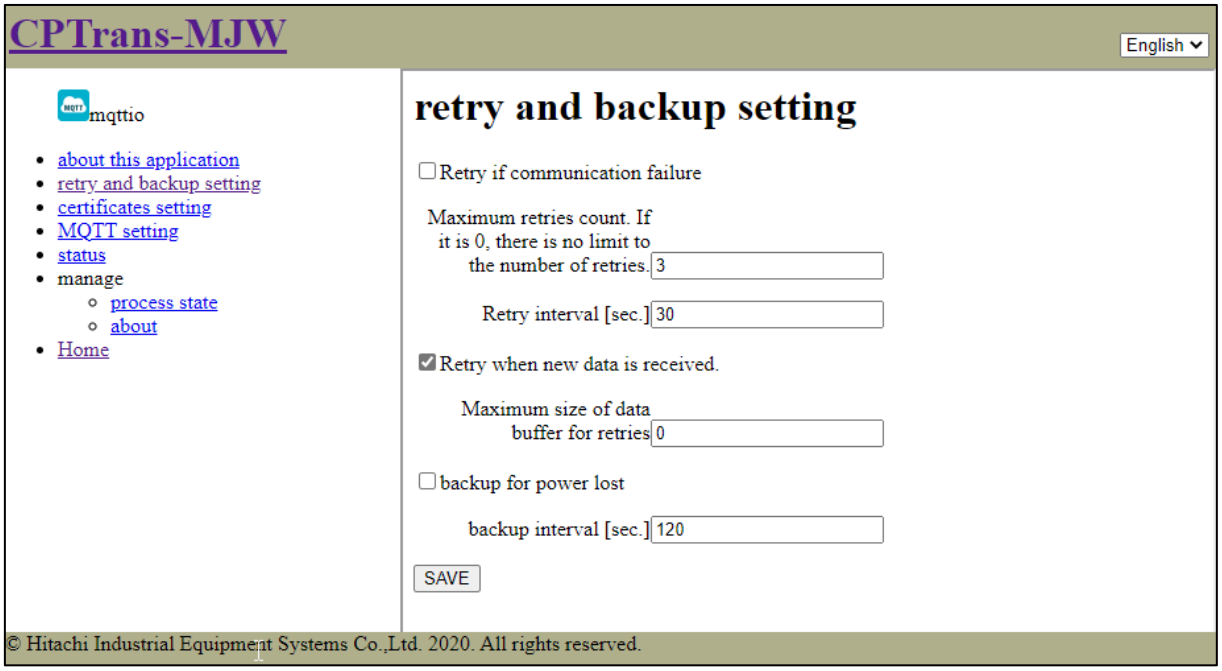



**Figure 5.64 Retry and backup setting**

The details of the "Retry and backup setting" screen are shown below.

(1) Perform retry due to communication failure

| Item | Description |
|---|---|
| Retry if communication failure | Specifies whether the retransmission function is enabled or disabled.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Maximum retries count. If it is 0, there is no limit to the number of retries. | Specifies the number of retransmissions when communication fails. |
| Retry interval [sec] | Specify the time interval between retransmissions when communication fails. |
| Retry when new data is received | Specifies whether the retransmission function starts when new data is received.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Maximum size of data buffer for retries | Specify the maximum data size to be saved when communication fails.<br>Setting range: Up to 1000000 |

(2) Perform backup against power interruption

| Item | Description |
|---|---|
| Backup for power lost | Enables or disables the function to save the transmitted data to the backup file in case of power off.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Backup interval [sec.] | Specify the time interval for saving the transmitted data to the backup file in case of power off. |

5.15.2 Certificates setting

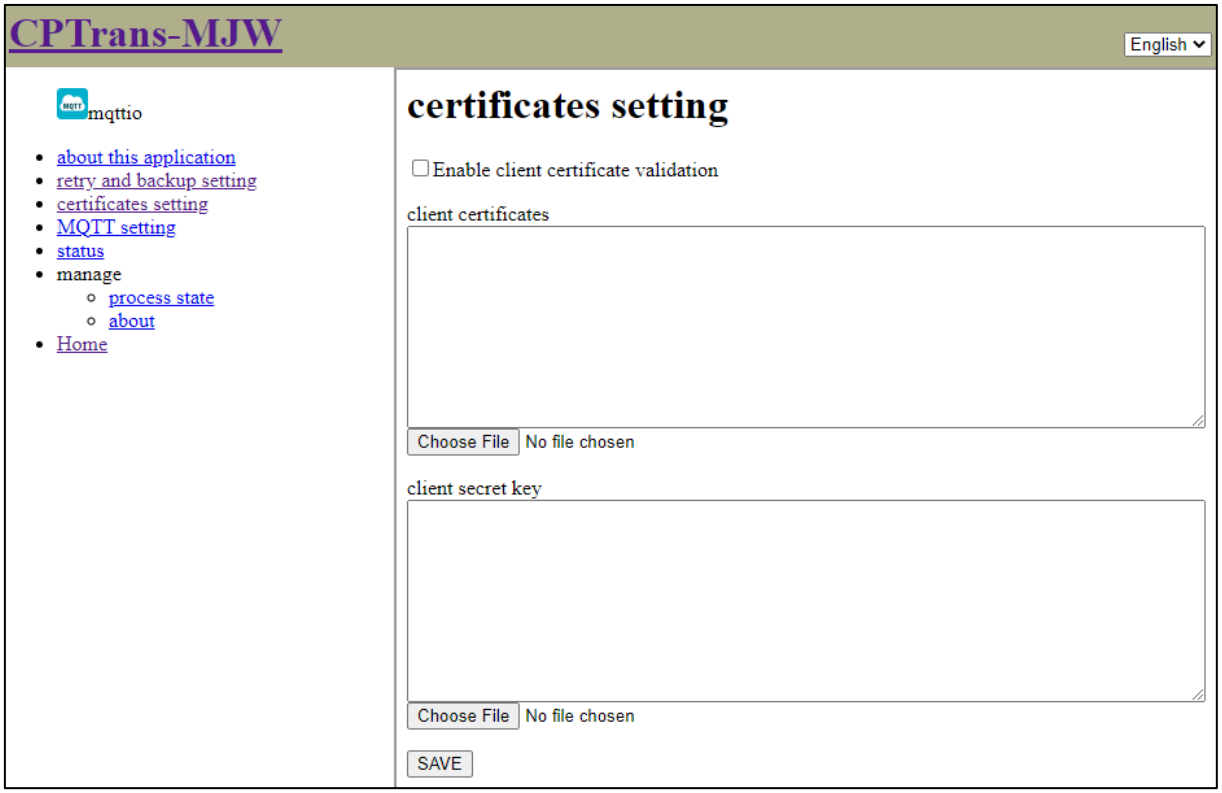



**Figure 5.65 Certificates setting**

The details of the "Certificate Setting" screen are shown below.

(1) Client certificate

| Item | Description |
|---|---|
| Enable client certificates validation | Enables or disables the client certificate function using the client certificate.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Client certificate | Register the client certificate.<br>Select directly or select a file to register. |

(2) Client secret key

| Name | Description |
|---|---|
| Client secret key | Register the client secret key.<br>Select directly or select a file to register. |

### 5.15.3 MQTT Settings

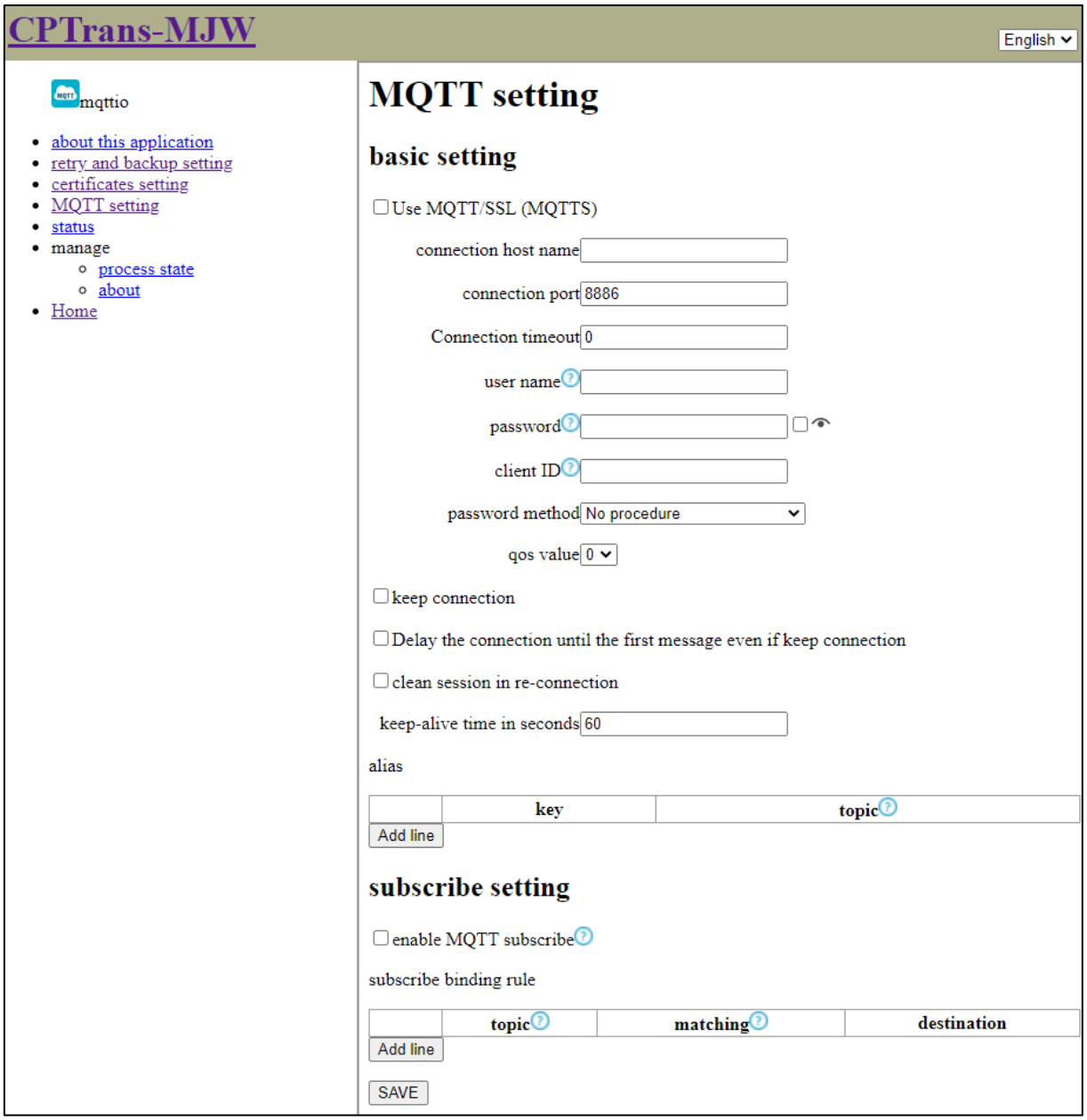



**Figure 5.66 MQTT setting**

MQTT Settings window is detailed below.

(1) Basic setting

| Item | Description |
|---|---|
| Use MQTT/SSL (MQTTS) | Enables or disables MQTTS (encrypted MQTT) communication.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| connection host name | Specifies the host name to connect to. |
| connection port | Specifies the TCP port to connect to. |
| User name | Specifies the user name for authentication. |
| Password | Specify the password for authentication. |
| Client ID | Specifies the client ID for session identification.<br><br>※Because MQTT servers identify communication sessions by client IDs, clientID must be unique.<br>※If this setting is blank, the session is discarded regardless of whether the setting is enabled or disabled. |
| Password method | Choose a password policy that depends on the cloud service.<br><br>Options:<br>0: No procedure<br>1: Calculate SAS automatically |
| QOS value | Selects MQTT QOS-value.<br><br>Options:<br>0: 0 (without retransmission)<br>1: 1 (Always reach at least once)<br>2: 2 (Always arrive once) |
| Keep connection | Specifies whether MQTT remains connected.<br><br>Setting range:<br>Check ON: Keeps the connection status.<br>No check: Do not maintain connection status |
| Clean session in re-connection | Specifies whether to discard the previous session when reconnecting.<br><br>Setting range:<br>Checked: Discard the session<br>No check: Do not discard session |

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Keep-alive time in seconds</td><td>Specifies the interval for sending keep-alive messages. This setting is mandatory if the connection status is to be maintained.<br><br>Setting range: 10 [sec] or more<br>※Keep-alive messages are messages that inform the server of connection status.</td></tr>
<tr><td>Alias</td><td>You can register topic names for each key value contained in the destination information in iopoll.<br>Create the key value and topic name in association with each other.<br><br><table><tr><th>Item</th><th>Description</th></tr><tr><td>Key</td><td>The key-value part of iopoll that follows mqtt with a "." as the destination.</td></tr><tr><td>Topic</td><td>The actual topic-name of MQTT to be sent.</td></tr></table></td></tr>
</table>

(2) Subscribe setting

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td>Enable MQTT Subscribe</td><td>Enables or disables MQTTS subscribing feature.<br><br>Setting range:<br>Checked: valid, unchecked: invalid</td></tr>
<tr><td>Binding rule</td><td>When a message with the topic name registered in this rule is received, the message can be transferred to Modbus app, etc.<br><br><table><tr><th>Item</th><th>Description</th></tr><tr><td>Topic</td><td>Specifies the topic name to subscribe to.</td></tr><tr><td>Matching</td><td>Specifies a matching rule for the received topic. You can use glob command-syntax.</td></tr><tr><td>Destination</td><td>Specify the destination application.</td></tr></table></td></tr>
</table>

### 5.15.4 Status

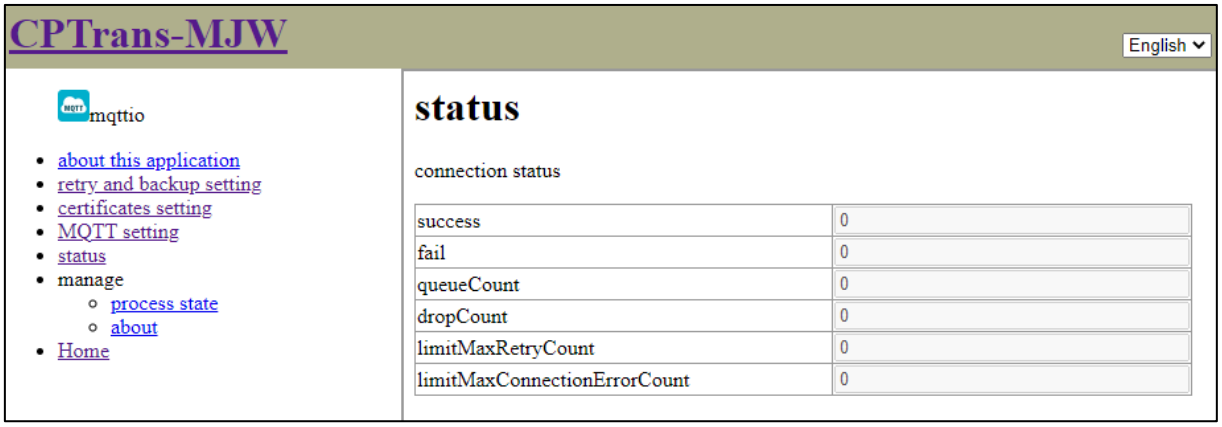



**Figure 5.67 Status**

Details of the Status screen are shown below.

(1) Connection Status

| Name | Description |
|---|---|
| Success | This is the number of successful MQTT communications. |
| Fail | This is the number of failed MQTT communications. |
| QueueCount | Number of unsent data. |
| DropCount | Number of data discarded due to communication failure. |

## 5.16 RESTio

RESTio application is described below.

| Icon | Overview |
|---|---|
|  | Supports the ability to upload various types of data by REST API using HTTP protocols. |

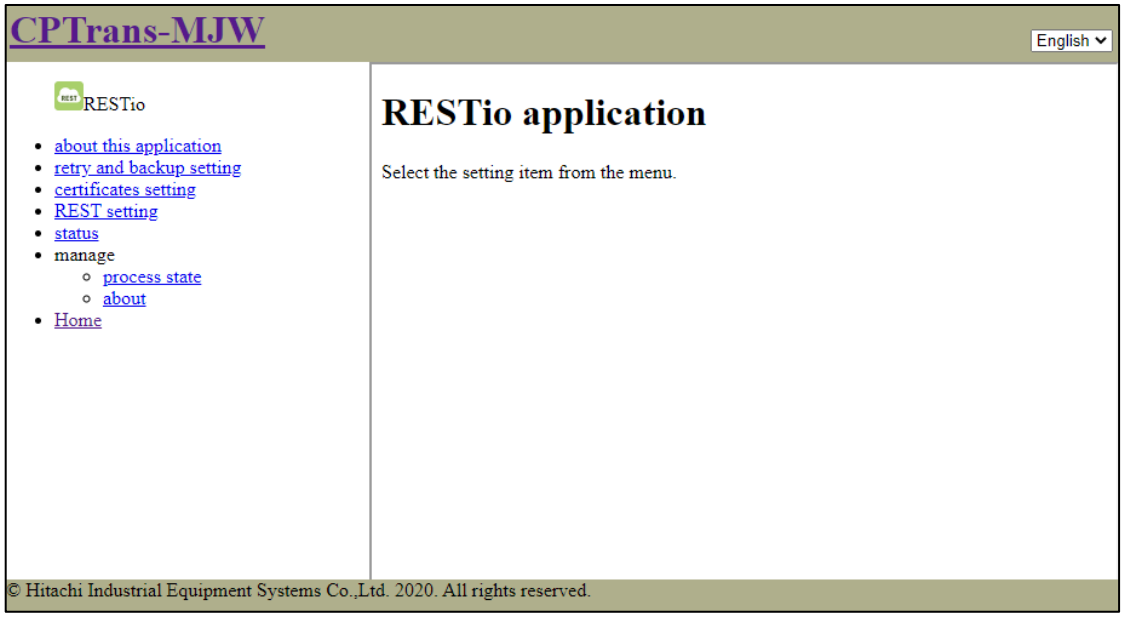



**Figure 5.68 Initial window of RESTio application**

### 5.16.1 Retry and backup setting

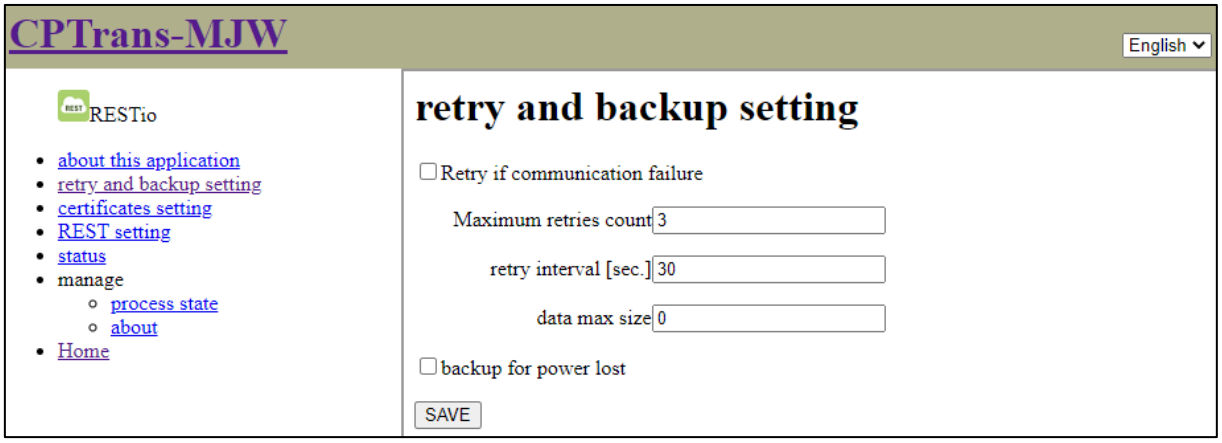



**Figure 5.69 Retry and backup setting**

The details of the "Retry and backup setting" screen are shown below.

(1) Perform retry due to communication failure

| Item | Description |
|---|---|
| Retry if communication failure | Specifies whether the retransmission function is enabled or disabled.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Maximum retries count | Specifies the number of retransmissions when communication fails. |
| Retry interval [sec] | Specify the time interval between retransmissions when communication fails. |
| Data max size | Specify the maximum data size to be saved when communication fails.<br>Setting range: Up to 1000000 |

(2) Perform backup against power interruption

| Item | Description |
|---|---|
| Backup for power lost | Enables or disables the function to save the transmitted data to the backup file in case of power off.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |

### 5.16.2 Set certificate

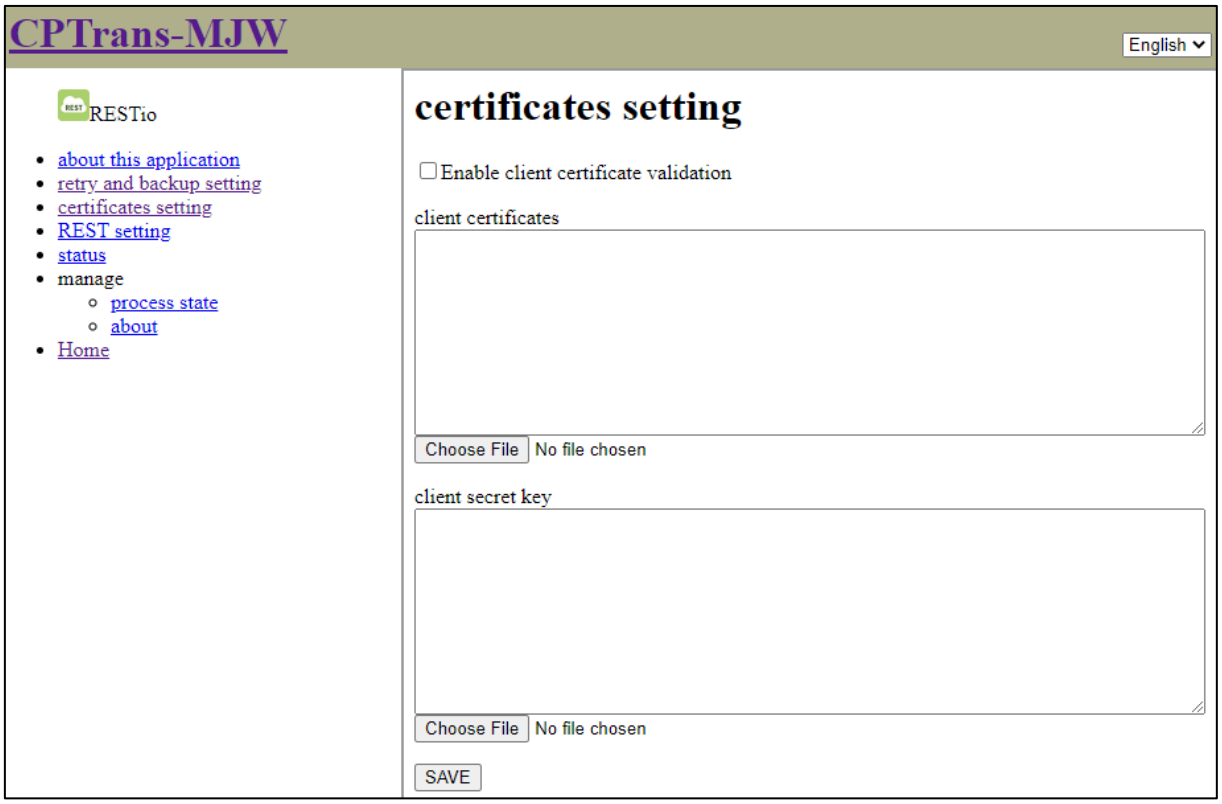



**Figure 5.70 Certificates setting**

The details of the "Certificate Setting" screen are shown below.

(1) Client certificate

| Item | Description |
|---|---|
| Enable client certificate validation | Enables or disables the client certificate function using the client certificate.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Client certificates | Register the client certificate. Select directly or select a file to register. |

(2) Client secret key

| Item | Description |
|---|---|
| Client secret key | Register the client private key. Select directly or select a file to register. |

### 5.16.3 REST Settings

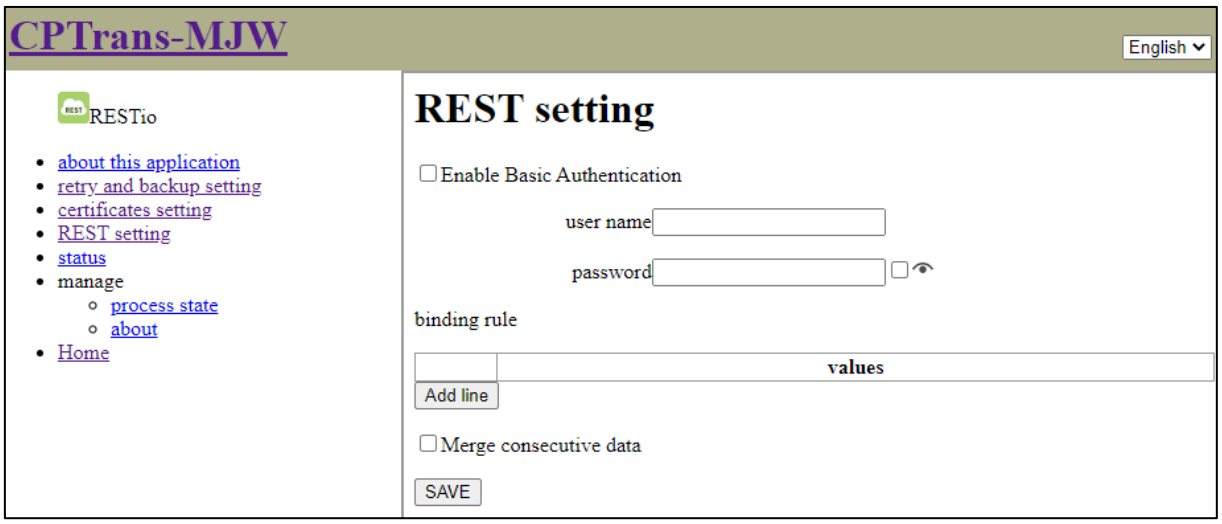



**Figure 5.71 REST setting**

REST Settings window is detailed below.

(1) REST Settings

| Item | Description |
|---|---|
| Enable Basic Authentication | Specifies whether authentication is enabled. |
| User name | Specifies the user name for authentication. |
| Password | Specify the password for authentication. |
| Binding rule | Registers the communication content for each key value included in the destination information in iopoll.<br><br>Item: Key — Description: The key-value part of iopoll that follows rest with a "." as the destination.<br>Item: URL — Description: Specifies the URL of the destination.<br>Item: Header — Description: Specifies the content of the header.<br>Item: Method — Description: Specifies HTTP method.<br>Setting range:<br>1: URL (no encoding)<br>2: URL (URL Encoding)<br>3: POST<br>4: PUT |
| Merge successive data | Specify whether to enable or disable the function to send consecutive data concatenated.<br>Setting range:<br>Checked: valid, unchecked: invalid |

5.16.4 Status

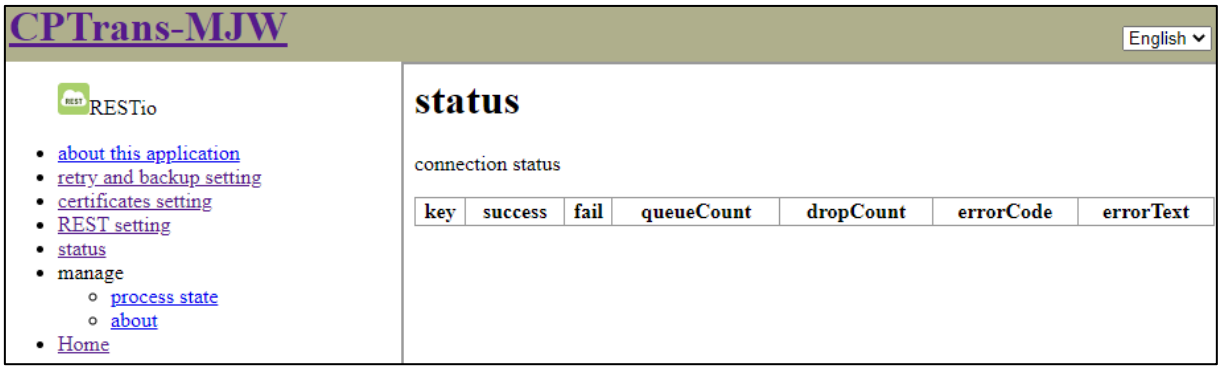



**Figure 5.72 Status**

Details of the Status screen are shown below.

(1) Connection Status

| Item | Description |
|---|---|
| Key | The keyvalue in iopoll destination information. |
| Success | This is the number of successful REST communications. |
| Fail | This is the number of failed REST communications. |
| QueueCount | Number of unsent data. |
| DropCount | Number of data discarded due to communication failure. |
| ErrorCode | Displays the error code of REST communication result. |
| ErrorText | Displays the textual content of REST communication. |

## 5.17 232 through

The 232 through application is described below.

| Icon | Overview |
|---|---|
|  | Supports the ability to convert TCP communication and RS232. |

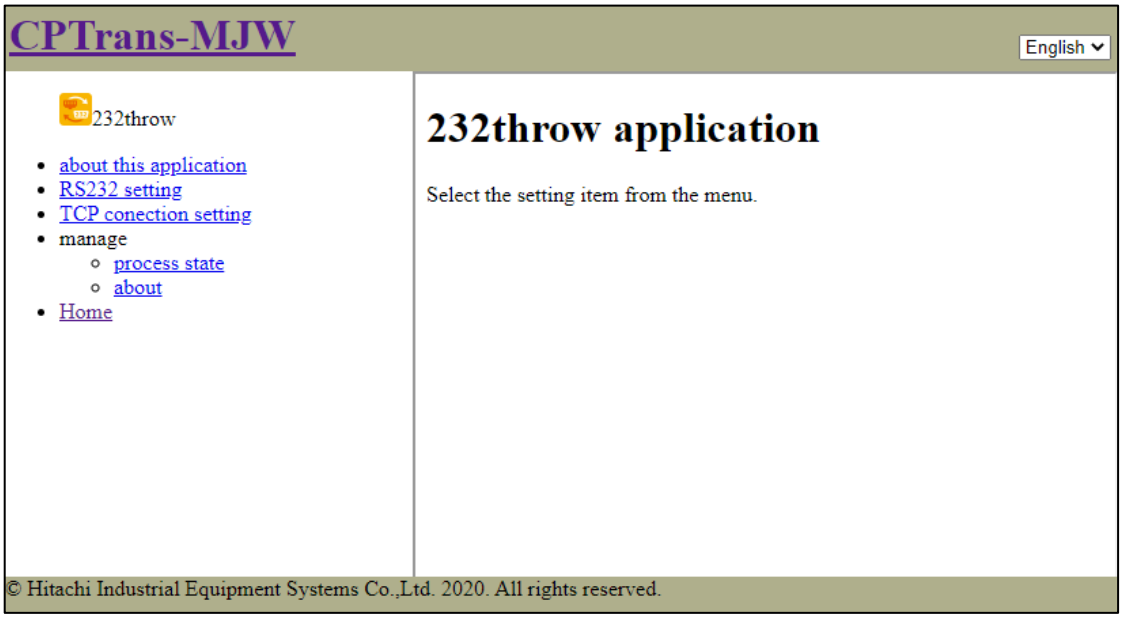



**Figure 5.73 Initial window of 232 through application**

### 5.17.1 RS232 Setting

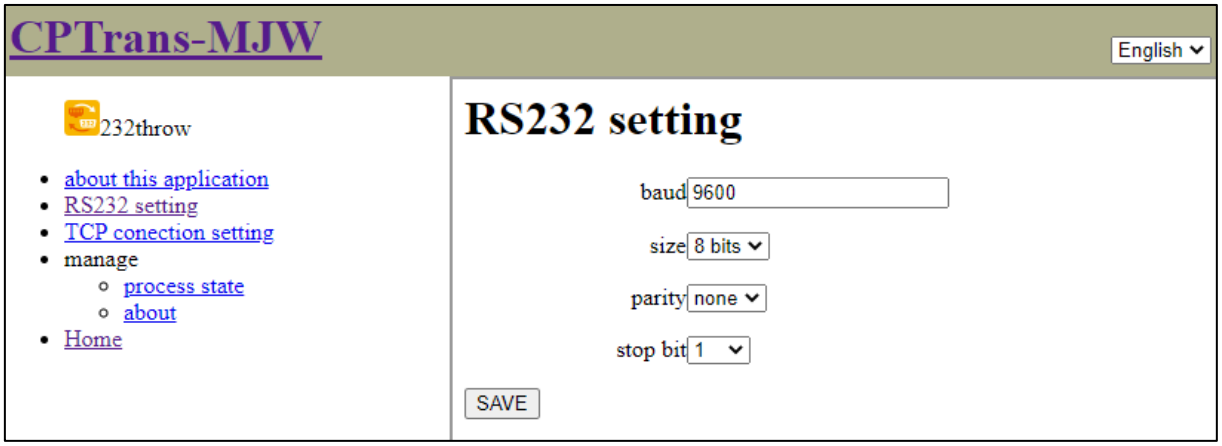



**Figure 5.74 RS232 setting**

RS232 Settings window is detailed below.

(1) RS232 Setting

| Item | Description |
|---|---|
| Baud | Specify the baud rate.<br><br>Setting range: Within 250000<br>(RS485 through is 1000000 max.) |
| Size | Specifies the size of the data bit.<br><br>Options:<br>7: 7 bits<br>8: 8 bits |
| Parity | These bits specify the parity bit setting.<br><br>Options:<br>0: None 1: Even 2: Odd |
| Stop bit | Specifies stop bit for RS232 communication.<br><br>Options:<br>0: 1 bit, 1: 1.5 bits, 2: 2 bits |

### 5.17.2 TCP connection settings

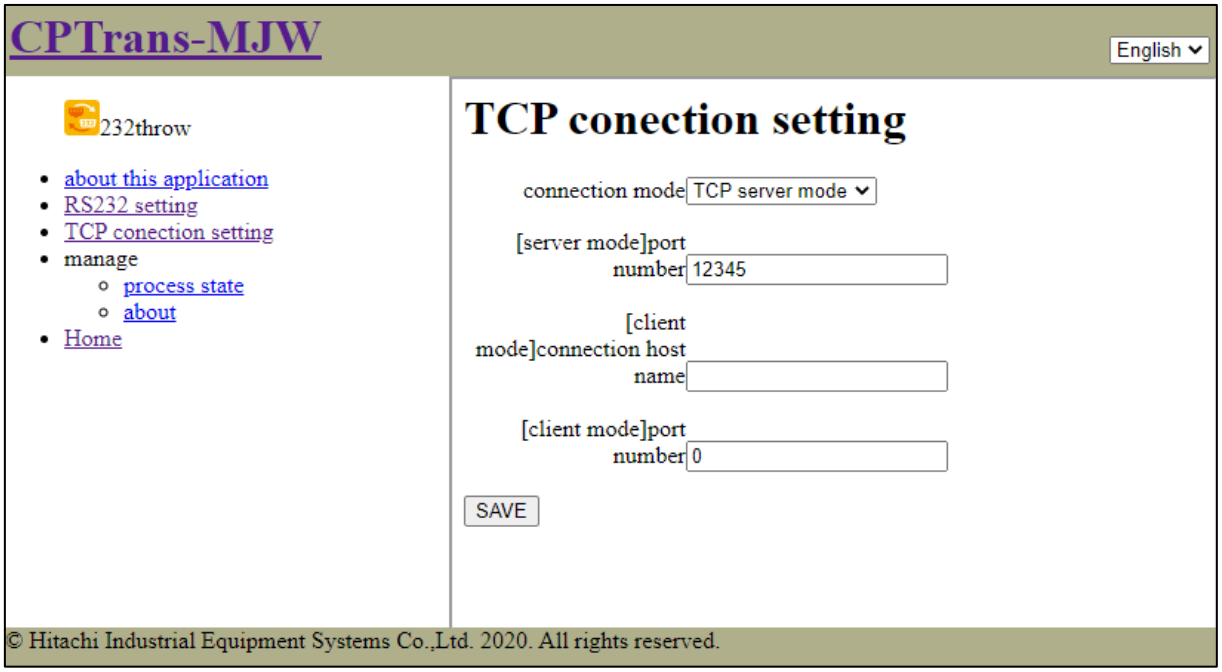



**Figure 5.75 TCP connection setting**

The details of the "TCP connection setting" screen are shown below.

(1) TCP connection settings

| Item | Description |
|---|---|
| Connection mode | Specify the server or client mode.<br><br>Setting range:<br>1: TCP server mode<br>2: TCP client mode |
| [Server Mode] Port Number | Specifies the TCP port number to listen to in server mode.<br><br>Setting range: 0 to 65535 |
| [Client Mode] Connection host name | Specifies the destination host name to which RS232 port-data received in client mode is sent. |
| [Client Mode] Port Number | Specifies the TCP port number to which RS232 port received in client mode is to be sent.<br><br>Setting range: 0 to 65535 |

## 5.18 485 through

The 485 through application is described below.

| Icon | Overview |
|---|---|
|  | Supports the ability to convert TCP communication and RS485. |

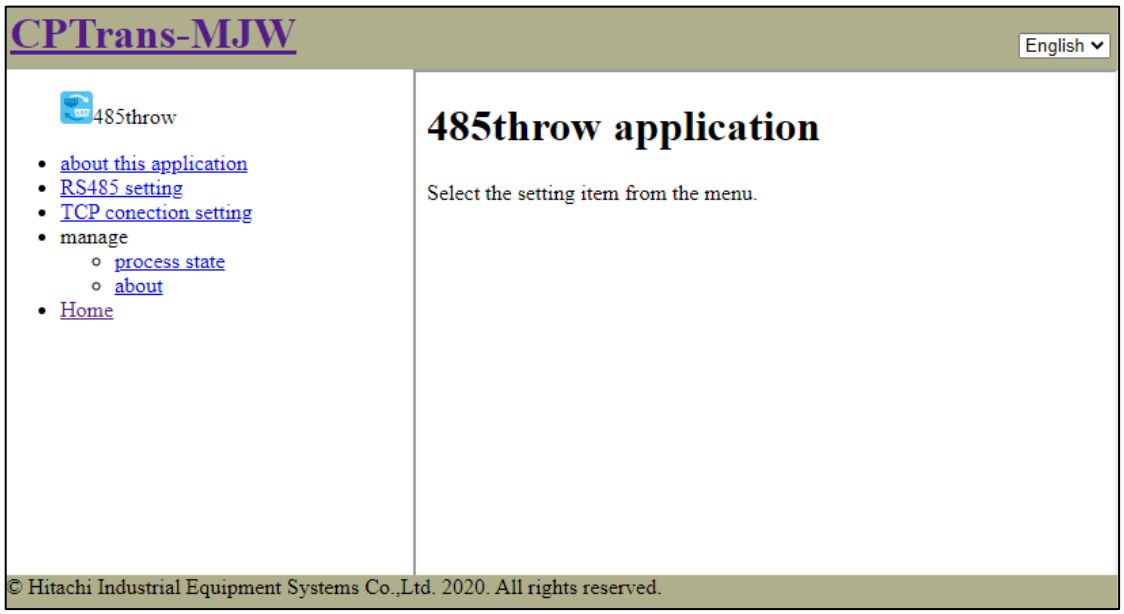



**Figure 5.76 Initial window of 485 through application**

### 5.18.1 RS485 Setting

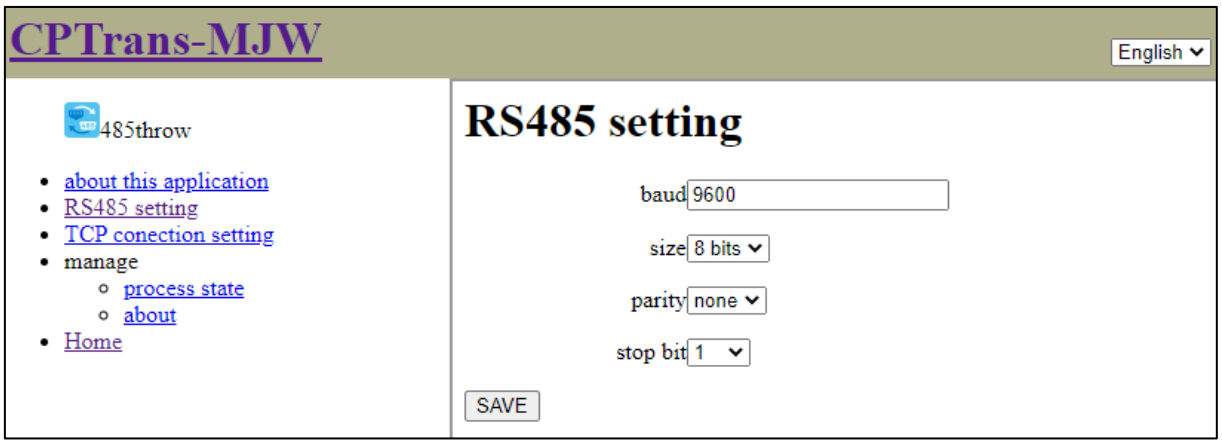



**Figure 5.77 RS485 setting**

RS485 Settings window is detailed below.

(1) RS485 Setting

| Item | Description |
|---|---|
| Baud | Specify the baud rate.<br><br>Setting range: Within 250000<br>(RS485 through is 1000000 max.) |
| Size | Specifies the size of the data bit.<br><br>Options:<br>7: 7 bits<br>8: 8 bits |
| Parity | These bits specify the parity bit setting.<br><br>Options:<br>0: None 1: Even 2: Odd |
| Stop bit | Specifies stop bit for RS232 communication.<br><br>Options:<br>0: 1 bit, 1: 1.5 bits, 2: 2 bits |

### 5.18.2 TCP connection settings

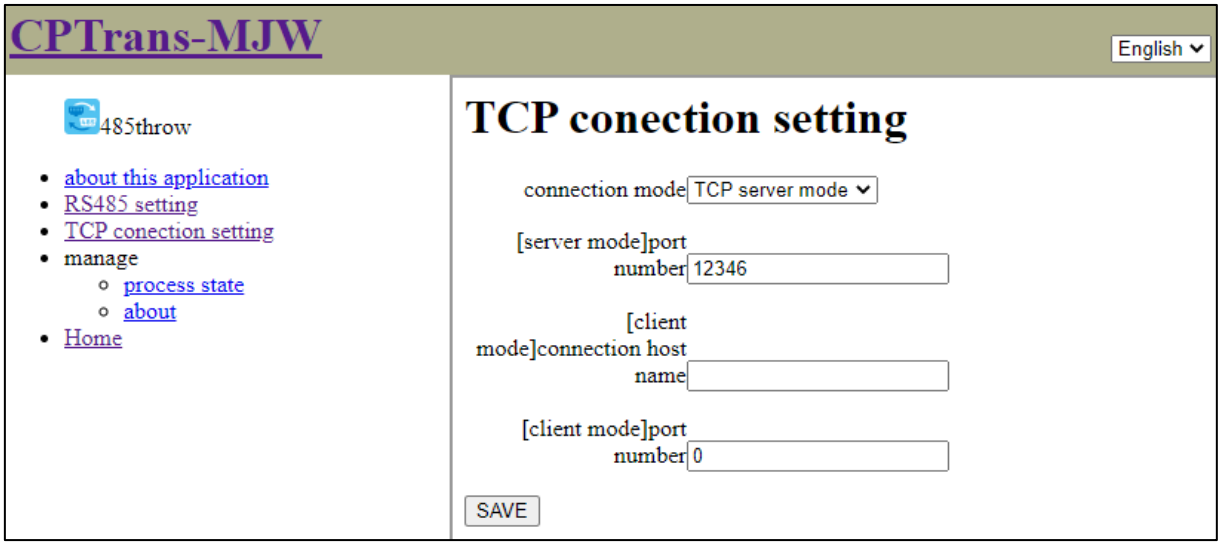



**Figure 5.78 TCP connection setting**

The details of the "TCP connection setting" screen are shown below.

(2) TCP connection settings

| Item | Description |
|---|---|
| Connection mode | Specify the server or client mode.<br><br>Setting range:<br>1: TCP server mode<br>2: TCP client mode |
| [Server Mode] Port Number | Specifies the TCP port number to listen to in server mode.<br><br>Setting range: 0 to 65535 |
| [Client Mode] Connection host name | Specifies the destination host name to which RS485 port-data received in client mode is sent. |
| [Client Mode] Port Number | Specifies the TCP port number to which RS485 port received in client mode is to be sent.<br><br>Setting range: 0 to 65535 |

## 5.19 Datamanager

Datamanager application is described below.

| Icon | Overview |
|---|---|
|  | Supports the ability to acquire information on connected devices and send it to an external device. |

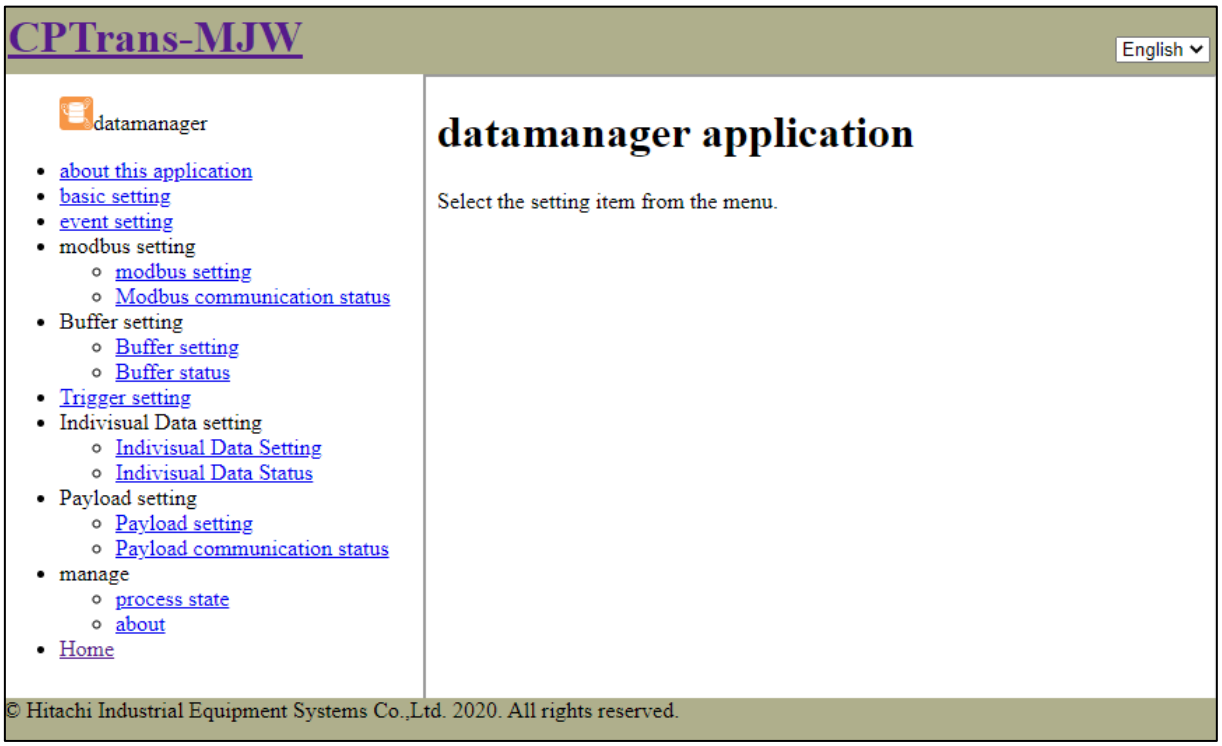



**Figure 5.79 Initial window of datamanager application**

### 5.19.1 Basic setting


**Figure 5.80 Basic setting**

The basic settings screen details are shown below.

| Item | Description |
|---|---|
| Enable for this application | Enables or disables datamanager application.<br>No check: Do not start app (stop process)<br>Checked: Launch app |
| Start communication after startup | Specifies whether to communicate with device IO and network IO when datamanager application is started.<br>No check: Do not communicate at startup<br>Checked: Communication is performed at startup. |

5.19.2 Event Settings

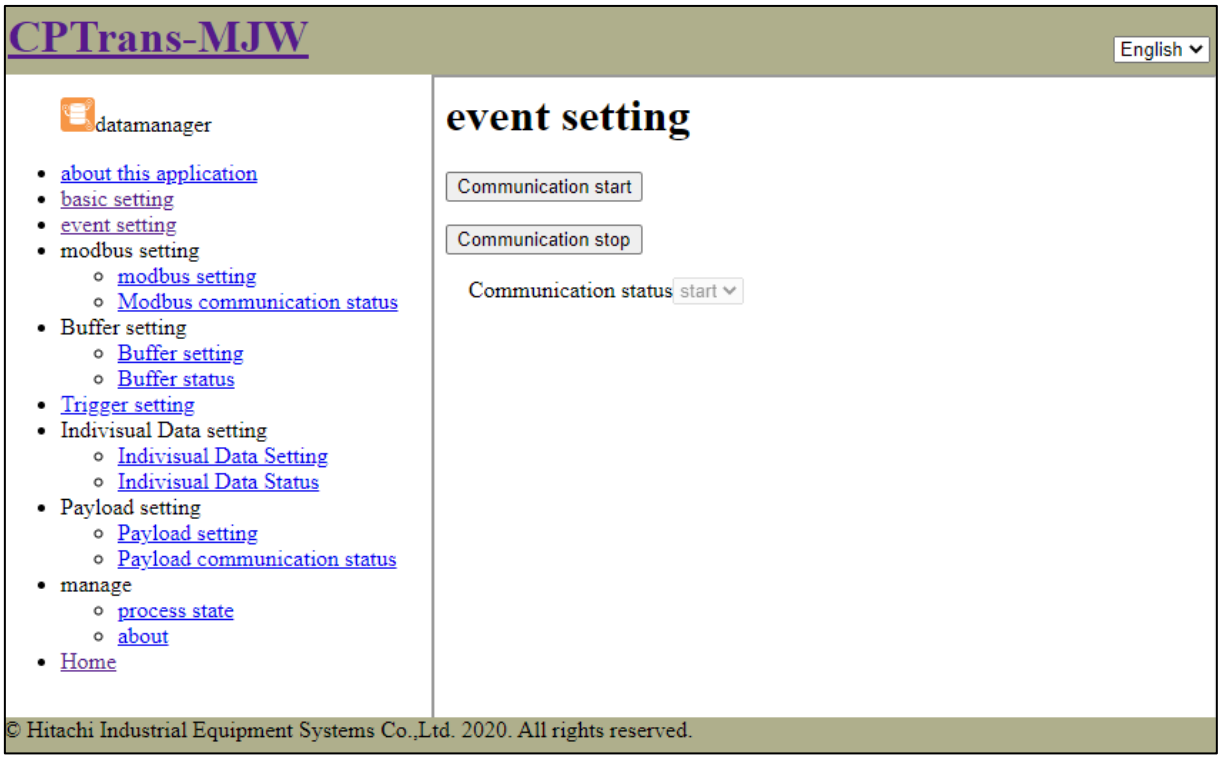



**Figure 5.81 Event setting**

The details of the "Event Setting" screen are shown below.

| Item | Description |
|---|---|
| Communication start | Gets information about connected devices and starts sending them to an external device. |
| Communication stop | Stops acquiring information on the connected device and sending it to an external device. |
| Communication status | Displays the status of whether the event control function of datamanager application is enabled or disabled.<br>Stopped: Communication stopped<br>Communication in progress: Communication start status |

### 5.19.3 Modbus Settings

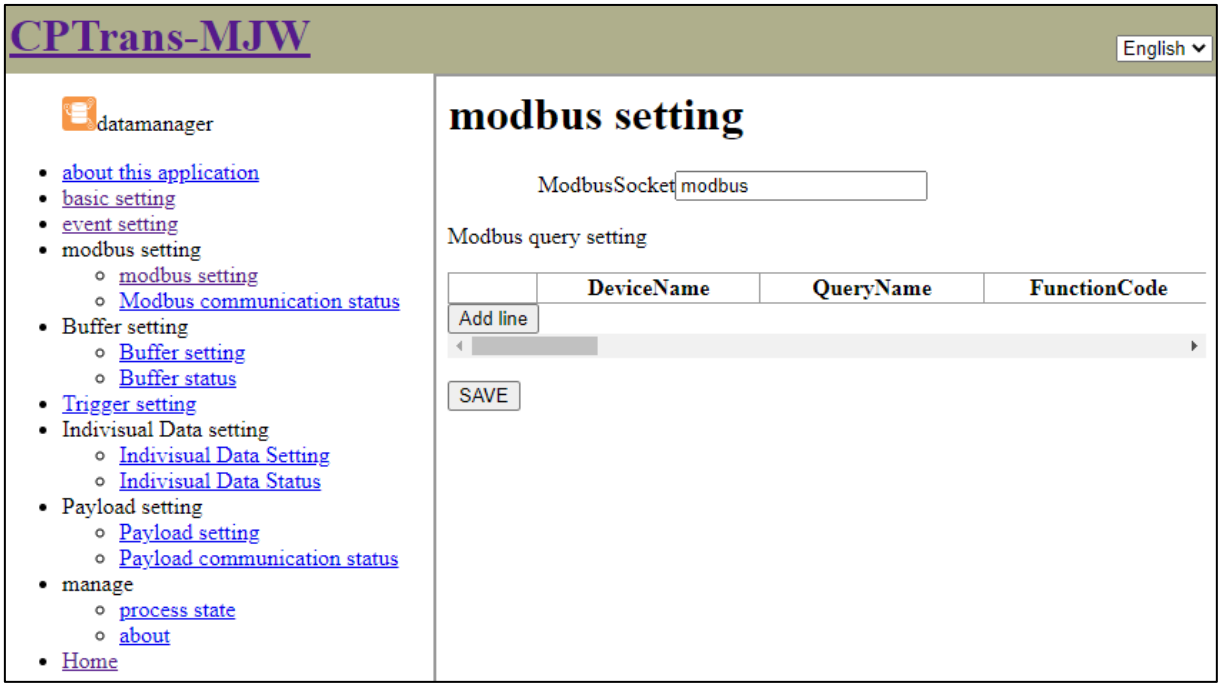



**Figure 5.82 Modbus setting**

Modbus Settings window is detailed below.

| Item | Description |
|---|---|
| Modbus socket | Sets the name of modbus communication socket. |
| Modbus querying settings | Set Modbus query info. |
| Device name | Sets the destination device name for Modbus queries. |
| Query Name | Set this Modbus queryname.<br>Setting range: 1 to 100 characters |
| Function code | Sets the function code of this Modbus query.<br>1: Read Coil Status (see below)<br>2: Read Input Status (not supported)<br>3: Read Holding Register<br>4: Read Input Register |
| Query start address | Sets the starting address of this Modbus query.<br>Setting range :0～65535 |
| Number of Register | Sets the number of registers required by this Modbus query.<br>Setting range :1～128 |
| Query Send Period | Set the sending interval [ms] for this Modbus query.<br>Setting range :1～86400000 |

| Item | Description |
|---|---|
| Response Timeout | Set GetResponse wait timer [ms].<br>Setting range: 1 to 1000 |
| Modbus response error judgment | This bit specifies whether to set the specified value (modbus[].errorValue) in the value stored in the data buffer when the number of times that a response to a Modbus query has been received exceeds the threshold (modbus[].errorCheckThreshold).<br>Setting range:<br>False: Specified value is not set.<br>True: Setting a Specification |
| Number of modbus response error judgment | Sets the threshold counter for setting the specified value (modbus[].errorValue) in the value of the data buffer in the event that a response to a Modbus query has been received or an error is returned.<br>Setting range :0～1000 |
| Set value when the error judgment threshold is exceeded | Set the value to be written to the data buffer when the threshold of error judgment is exceeded.<br>Setting range :0 x 00～0 xFF |
| Data buffer name | Sets the name of the data buffer to store the register data of the response to this Modbus query.<br>Setting range: 1 to 100 characters |
| Start Index | Specifies an index whose leading register data included in the response to this Modbus query is 0.<br>Setting range :0～127 |
| Update Period [s] | Sets the frequency at which the data buffer is updated in response to this Modbus query.<br>Setting range :1～86400 |
| Trigger condition | For the response to this Modbus query, specify the name (triggerCondition[].name) of the trigger condition for which transmission at change (onChange) is enabled.<br>Setting range: 0 to 100 characters |
| Response Buffer Name | Specifies the name of the data buffer to store the register data to be returned in the response to this Modbus query.<br>Setting range: 0 to 100 characters |

### 5.19.4 Modbus communication status

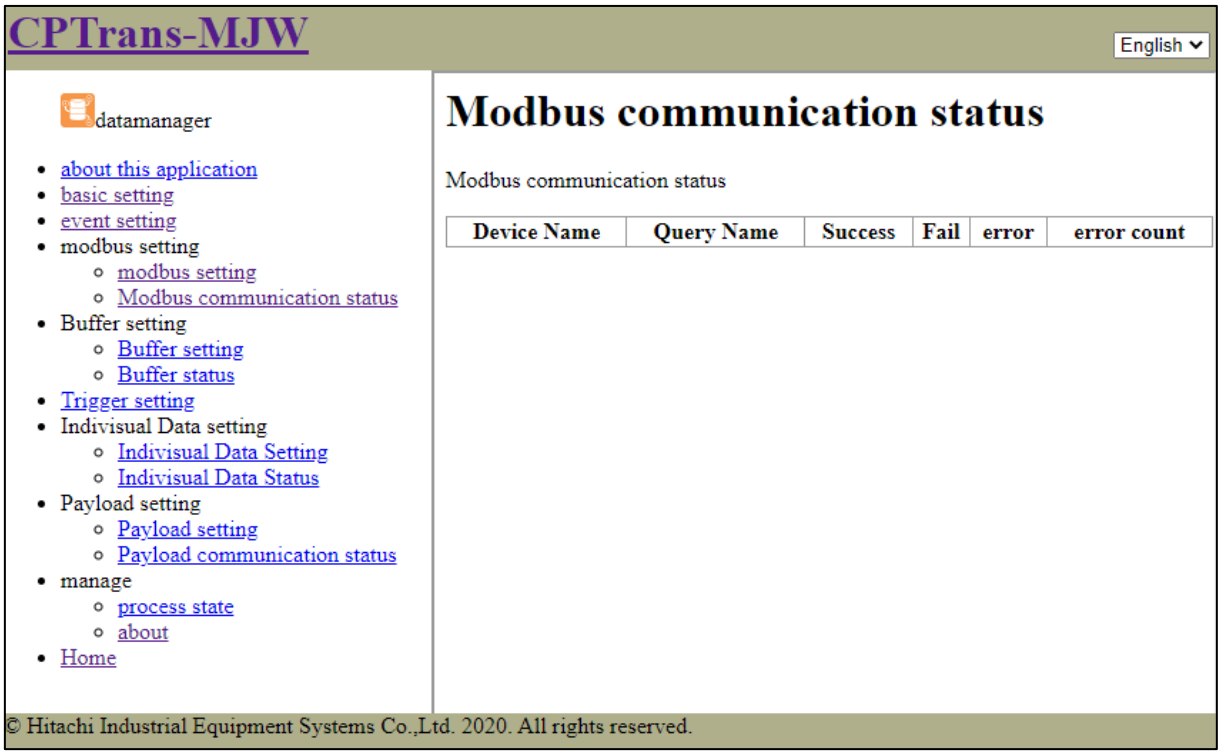



**Figure 5.83 Modbus communication status**

Modbus (I/O) messages status window is detailed below.

| Item | Description |
|---|---|
| Device name | Displays the device name of Modbus setting. |
| Query Name | Displays the name of Modbus setting query. |
| Success | Displays the number of successful SET request communications. |
| Fail | Displays the number of unsuccessful communication attempts for the SET request. |
| Error | Displays gmio error number.<br>0: Normal<br>1: Connection failure<br>2: No response<br>3: Connection not supported<br>4: KEY incorrect<br>5: Invalid data<br>6: No response to the key (such as the corresponding key not present)<br>7: IO error<br>8: Error response returned from access destination device<br>9: Timeout after access<br>10: Grammar error of metatext, etc. |
| Error count | Displays the number of times errors and judgements (timeouts, etc.) were made in Modbus response. |

5.19.5 Data buffer setting

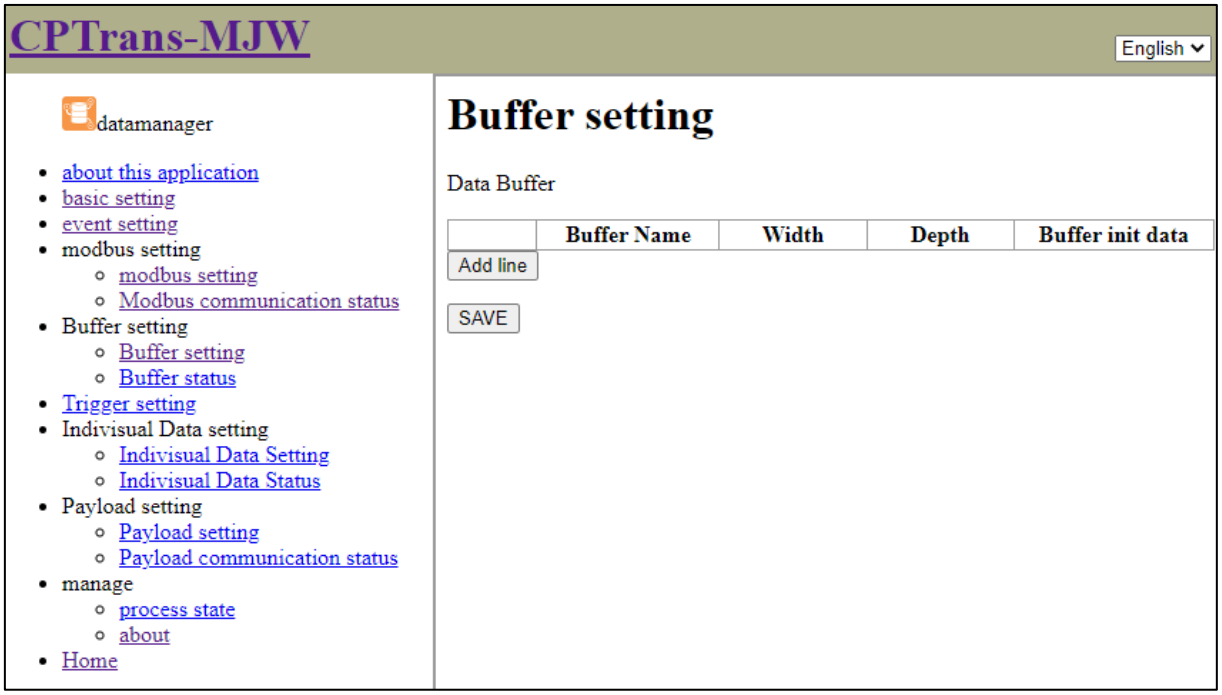



**Figure 5.84 Buffer setting**

Details of the "Data Buffer Setting" screen are shown below.

| Item | Description |
|---|---|
| Buffer Name | Sets the data buffer name.<br>Setting range: 1 to 100 characters |
| Width | Sets the data width (Byte) of the data buffer.<br>Setting range :1 to 256 |
| Depth | Sets the number of data items in the data buffer.<br>Setting range :1 to 256 |
| Buffer init data | Set the initial value to be specified when the data buffer is created.<br>Setting range :0x00～0xFF |

### 5.19.6 Buffer state

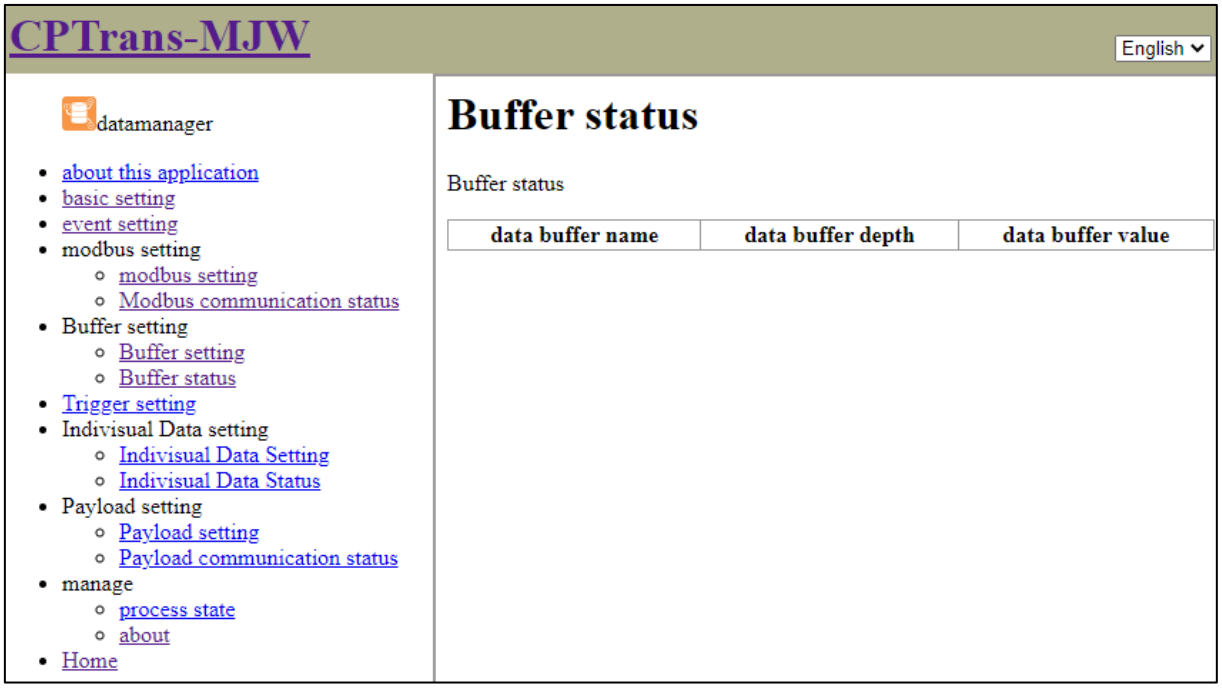



**Figure 5.85 Buffer status**

Details of the "Buffer Status" screen are shown below.

| Item | Description |
|---|---|
| Data buffer name | Displays the data buffer name. |
| Data buffer depth | Displays the number of data buffers. |
| Data buffer value | Displays the current value of the data buffer. |

5.19.7 Trigger setting

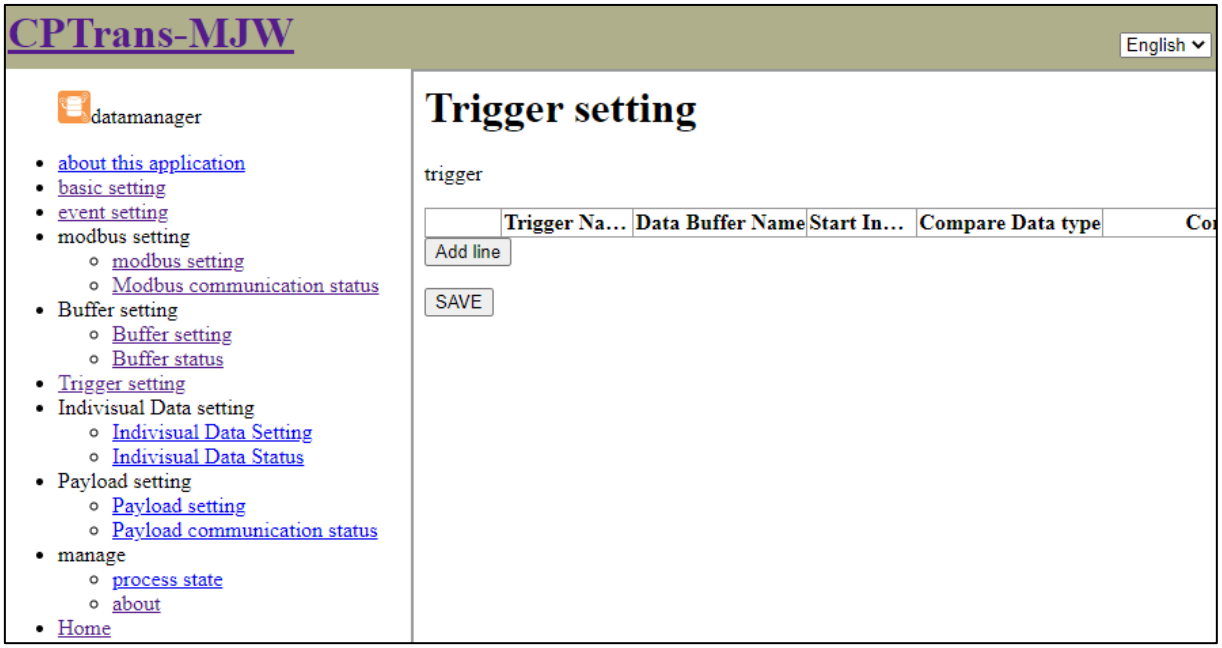



**Figure 5.86 Trigger setting**

The details of the "Trigger setting" screen are shown below.

| Item | Description |
|---|---|
| Trigger Name | Sets the name of the trigger condition.<br>Setting range: 1 to 100 characters |
| Data buffer name | Specifies the name of the data buffer to be used when a trigger condition expression is specified as 21 to 26.<br>Setting range: 1 to 100 characters |
| Start Index | Set the target byte position in this individual condition.<br>Setting range :0 to 255 |
| Compare Data type | Set the data format to be compared.<br>* Stored in big endian |
| Condition | Specifies the conditions under which the individual conditions are met. |
| Compare value | Set the value to be compared.<br>Setting range :0 to 0xFFFFFFFF |

### 5.19.8 Individual data setting

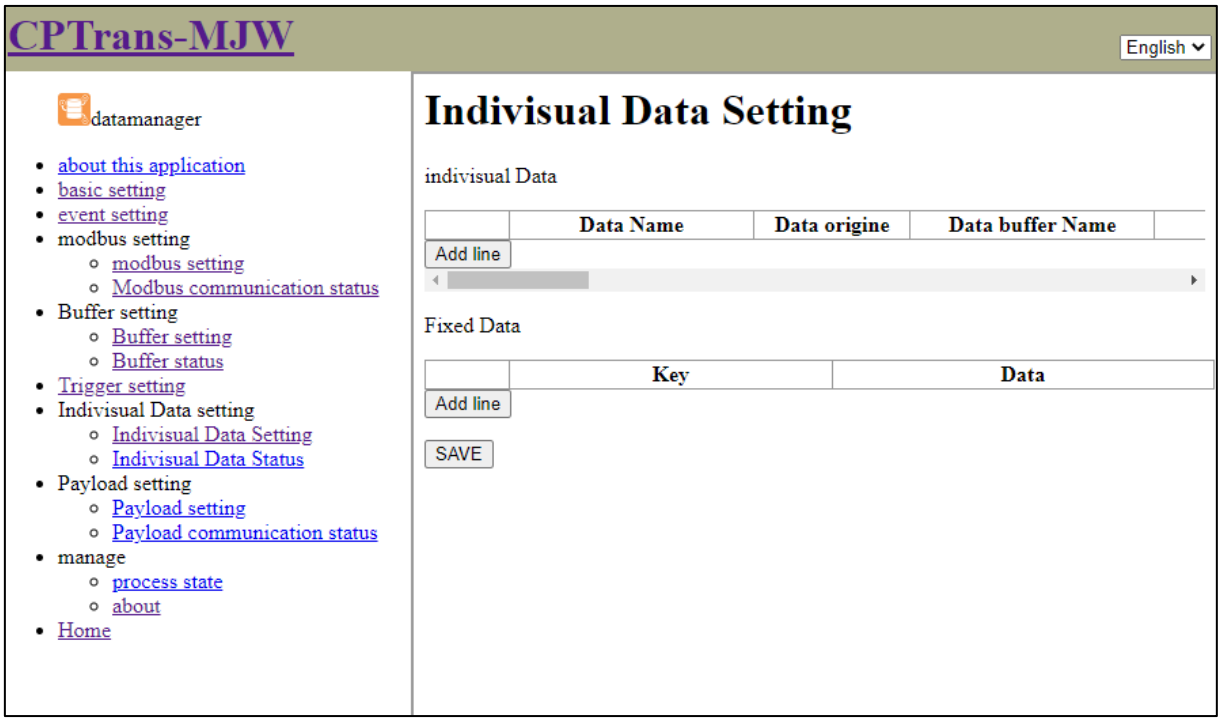



**Figure 5.87 Individual Data Setting**

Details of the "Individual data setting" screen are shown below.

(1) Individual data

| Item | Description |
|---|---|
| Data name | Set the individual data name.<br>Setting range: 1 to 100 characters |
| Data origin | Sets the individual data generation source.<br>1. Data buffer<br>3. Fixed value |
| Data buffer name | Sets the name of the data buffer in which the source data for generating this individual data is stored.<br>Setting range: 1 to 100 characters |
| Depth | These bits set the depth (refresh depth) of the data stored in the data buffer that is referenced by this individual data.<br>Setting range :0 to 255 |
| Width Index | Among the data stored in the data buffer, this bit sets the position (number of bytes) of the data referenced by this individual data.<br>Setting range :0 to 255 |
| Length | Sets the number of bytes of data to be referenced by this individual data.<br>Setting range :1 to 256 |
| Add Time to Data | The time when this individual data was collected is included in the transmitted data. |

| Item | Description |
|---|---|
| Data Omission Condition | Compare with the data sent last time, and set whether to include individual data in payload data.<br>0. Not omit<br>1. Equal Data<br>2. Equal Data and Time<br>3. Data Difference exceeds threshold<br>4. Time Difference exceeds threshold<br>5. Over<br>6. Less than |
| Retention time [s] | Sets the retention time of the previous value of the saved individual data.<br>Setting range :0 to 86400 |
| Threshold | Set the threshold value of the data abbreviation condition.<br>Setting range :0 to 0xFFFFFFFF |
| Data key | Sets the key when the data source is a fixed value.<br>Setting range: 0 to 128 characters |
| Binary format | Set the format when writing individual data in binary format. |
| Calculation Type | Sets the operation (maximum/minimum/average) to be performed to create this individual data.<br>0: Not calculate<br>1: Calculate the Max value<br>2: Calculate the Min value<br>3: Calculate the Average value |
| Digits after the decimal point | Sets the number of decimal places to include when the payload referencing this individual data is in text format.<br>Setting range :0 to 5 |
| Interpretation of data type | Set the data type to be used for this individual data.<br>0: Treat as unsigned integer<br>1: Treat as a signed integer<br>2: Treat as a signed floating-point number<br>3: Treat as a character (ASCII code) |
| Byte order specification | Sets the byte order when reading bytes from the data buffer and when storing this discrete data in a payload in binary format.<br>0: Treat as big endian<br>1: Treat as little endian |

(2) Fixed value

| Item | Description |
|---|---|
| Key | Specifies the key specified by the data key. |
| Data | Set a fixed value. |

### 5.19.9 Individual data state

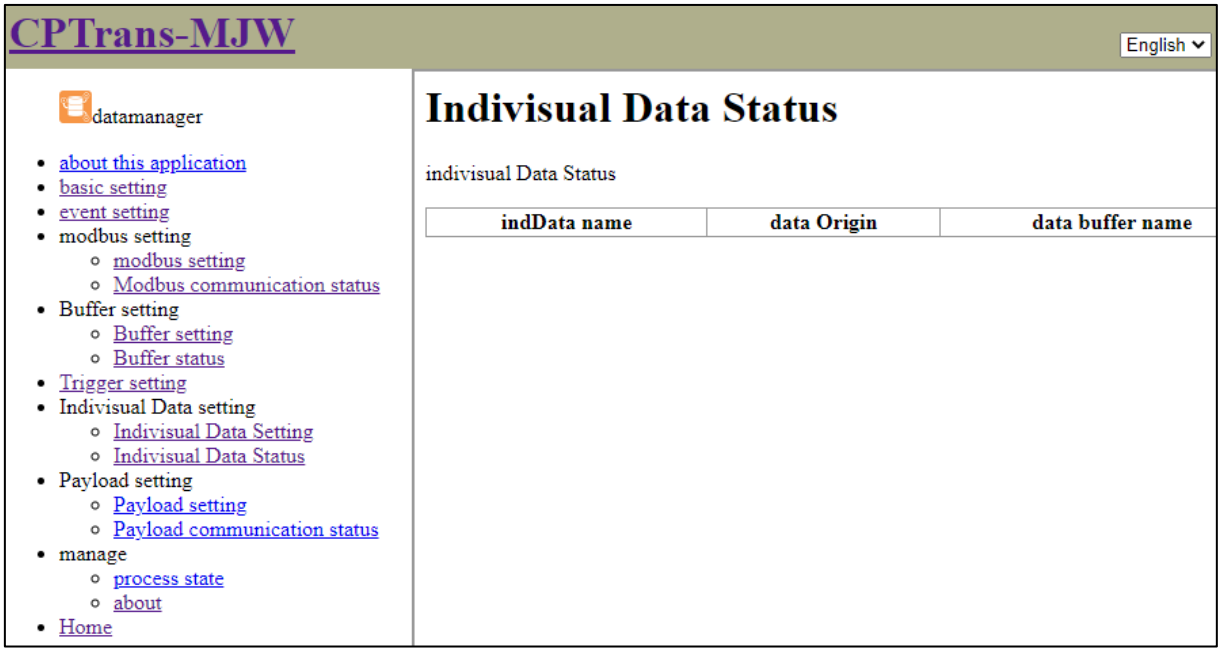



**Figure 5.88 Individual Data Status**

Details of the "Individual data status" screen are shown below.

| Item | Description |
|---|---|
| IndData name | Displays the individual data name. |
| Data origin | Displays the individual data generation source. |
| Data buffer name | This displays the name of the data buffer in which the source data for generating this individual data is stored. |
| Data buffer depth | Among the data stored in the data buffer, the depth (refresh) of the data referenced by this individual data is displayed. |
| Width index | Among the data stored in the data buffer, this displays the position (number of bytes) of the data referenced by this individual data. |
| Byte | Displays the number of bytes of data to be referenced by individual data. |
| Calculation type | Displays the operation type to be performed to create individual data. |
| IndData value | Displays individual data values. |

### 5.19.10 Payload setting

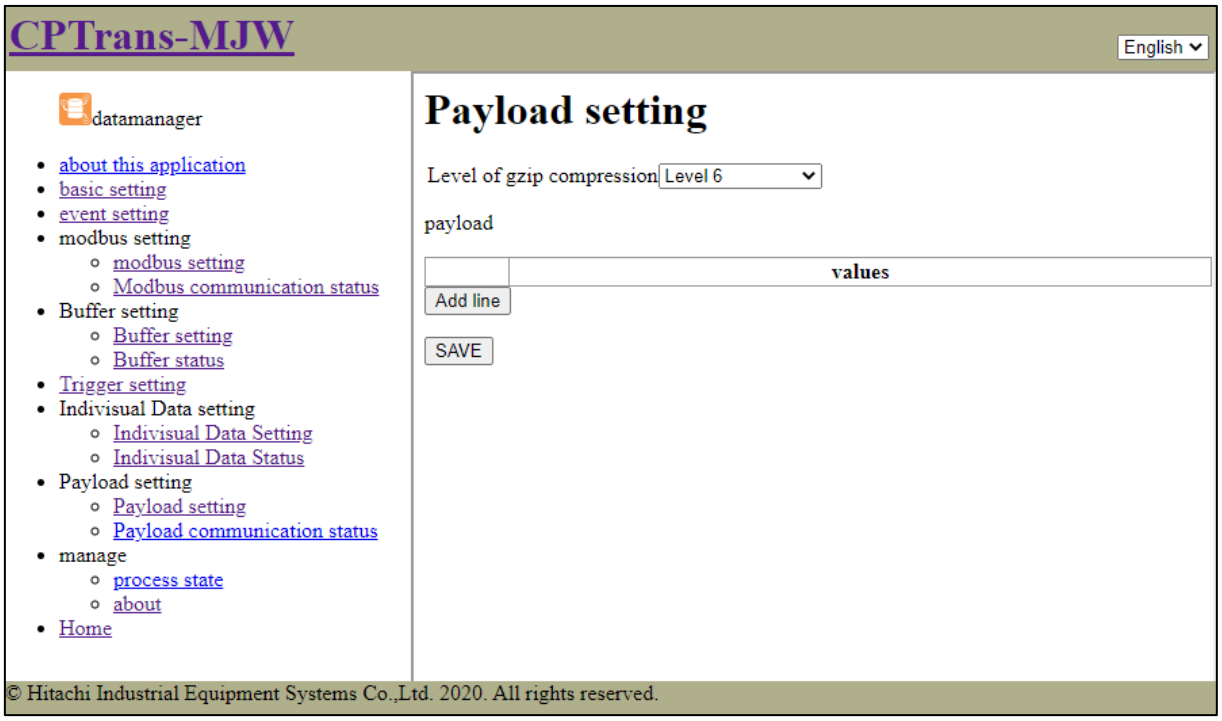



**Figure 5.89 Payload setting**

Details of the "Payload Setting" screen are shown below.

| Item | Description |
|---|---|
| Level of gzip compression | Specifies the degree of compression when gzip compressing a text-formatted payload. |
| Target application | Set the socket name that the Network IO app OPEN.<br>Setting range: 1 to 30 characters |
| Payload name | Set the payload data name.<br>Setting range: 1 to 100 characters |
| Send Wake Up | Set whether to transmit payload data at startup. |
| Send Timing | Set the payload data transmission timing.<br>1. Periodical<br>2. On-demand<br>3. Schedules<br>4. Trigger |
| Send Period | Set the payload data transmission cycle.<br>Setting range :0 to 90000 |
| Send Hour | Set the payload data send time.<br>Setting range :0 to 23 |
| Time zone mode | Set the time zone mode of the payload data transmission time. |
| Time zone [minutes] | Set the time zone of the payload data transmission time.<br>Setting range: -720(UTC -12) to 840(UTC +14) |
| Random width | Sets the random width of the payload data transmission time.<br>Setting range :10 to 1440 |
| Trigger enable | Set the trigger transmission of payload data. |

| Item | Description |
|---|---|
| Key name | Sets the destination topic-string when sending this payload in MQTT.<br>Setting range: 1 to 512 characters |
| Payload data format | Set the payload data transmission format.<br>1. Text format<br>2. Binary form |
| Response Timeout | Sets the response waiting time for the network IO app used for sending messages.<br>Setting range :1 to 1000 |
| Trigger Name | Sets or queries the trigger name for trigger transmission (transmission at transition).<br>Setting range: Max. 100 characters |
| Payload | Specifies the contents of the payload.<br>Setting range: 0 to 32768 characters |
| Compression enable | Sets whether to compress the payload data gzip. |

### 5.19.11 Payload Communication Status

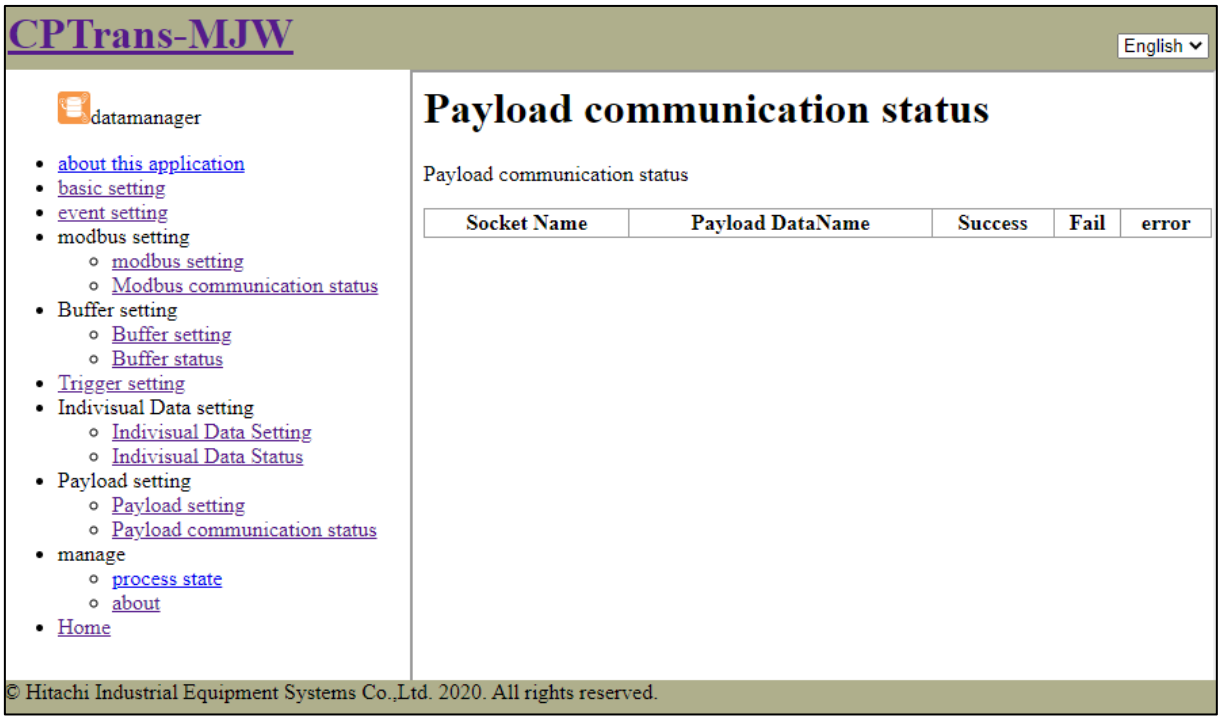



**Figure 5.90 Payload communication status**

Details of the "Payload communication status" screen are shown below.

| Item | Description |
|---|---|
| Socket name | Displays the name of the socket to which the communication destination AP is OPEN. |
| Payload DataName | Displays the payload name of the payload setting.<br>Setting range: 1 to 100 characters |
| Success | Displays the number of successful SET request communications. |
| Fail | Displays the number of unsuccessful communication attempts for the SET request. |
| Error | Displays gmio error number. |

## 5.20 Logsd

Logsd application is described below.

| Icon | Overview |
|---|---|
|  | This app allows you to save app logs to an SD card and download logs to a PC. |


**Figure 5.91 Initial window of logsd application**

5.20.1 Log download

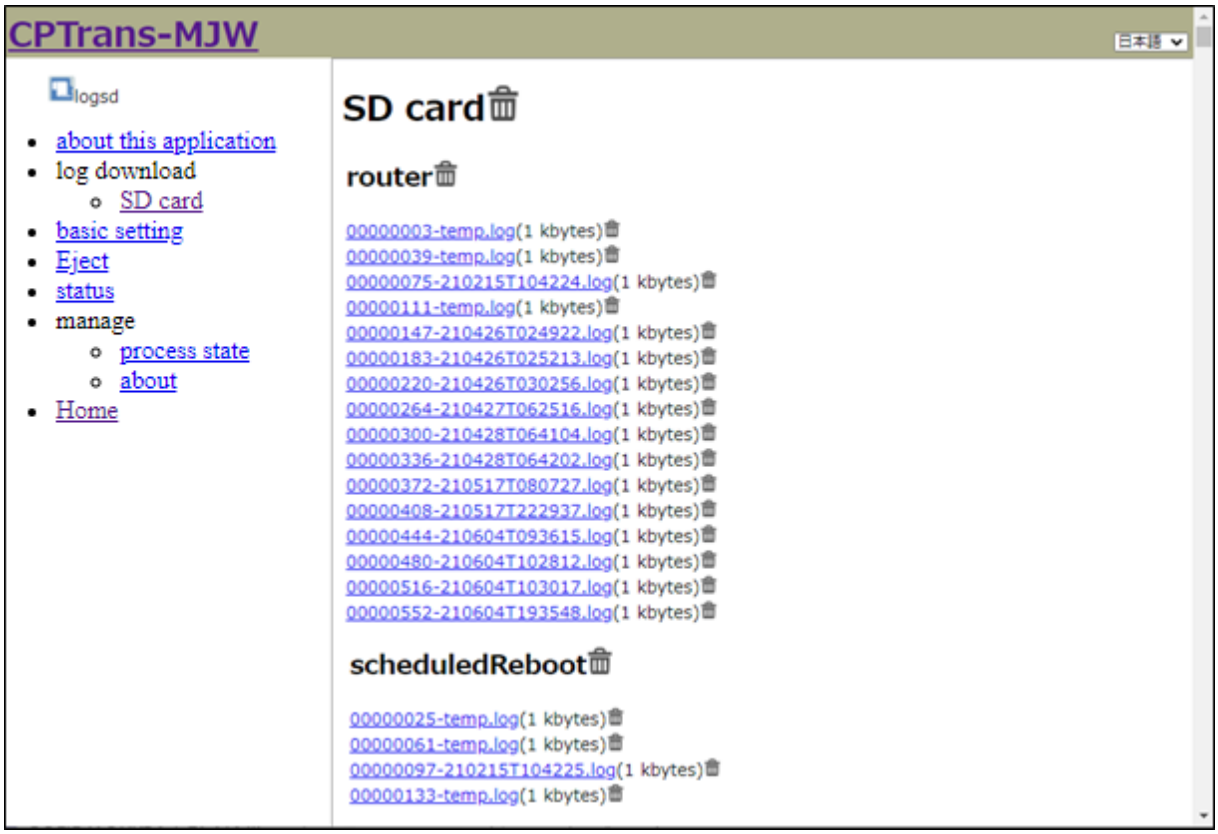



**Figure 5.92 Log download from SD card**

In the "SD card" screen of log download, the log of each app saved on the SD card is displayed for each app. If the file is selected, the file is downloaded to the connected PC.

5.20.2 Basic setting

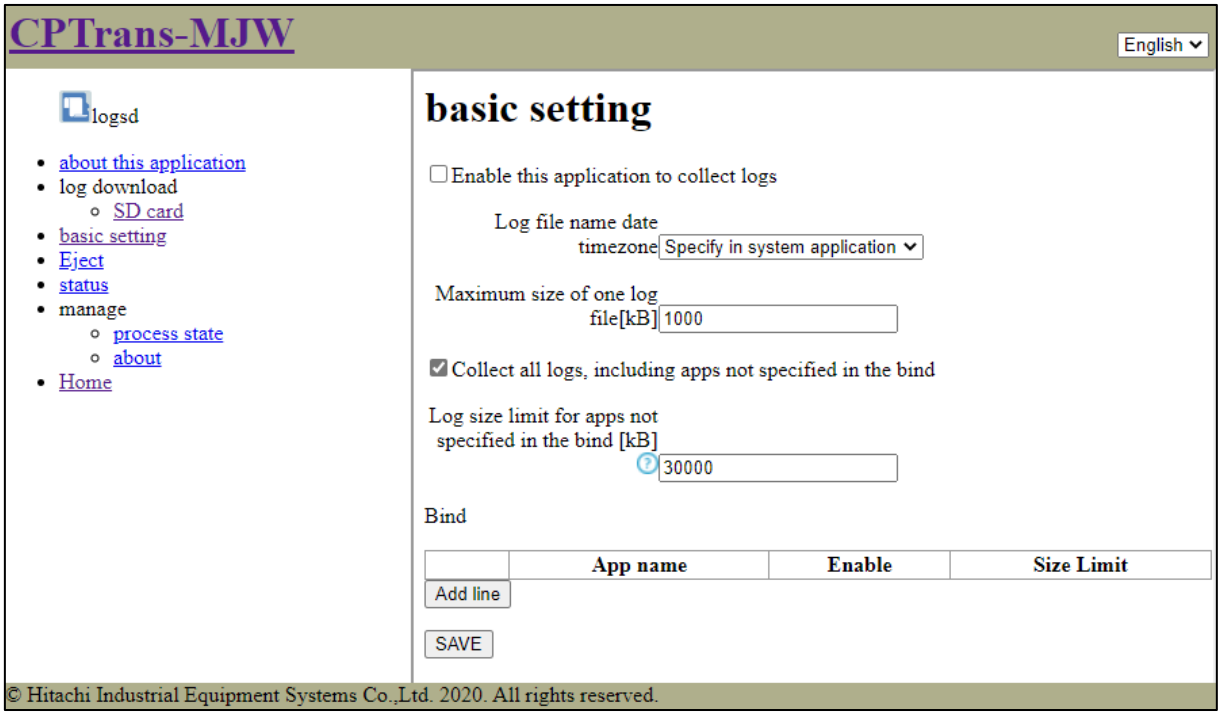



**Figure 5.93 Basic setting**

The basic settings are detailed below.

(1) Basic setting

| Item | Description |
|---|---|
| Enable this application to collect logs | Enables or disables the log collection function.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Log file name date timezone | Sets the time zone for the date of the log file name to be saved.<br><br>Options:<br>・Without time zone (using UTC)*Not supported<br>・Default value specified by system application |
| Maximum size of one log file [kB] | Sets the maximum size of one file in the log.<br><br>Setting range:500 to 1000<br>Initial value :1000 |
| Collect all logs, including apps not specified in the bind | Specifies whether to collect all logs, including apps not specified in the binding.<br><br>Setting range:<br>Checked: Enabled (Get all app logs)<br>No check: Disabled (Obtain only app log specified by bind) |
| Log size limit for apps not specified in bind [kB] | Specifies the limit on the log size (folder size for each app) of apps that are not specified in the binding.<br><br>Setting range: 10000 to 30000<br>Initial value: 30000 |

The Binding Settings screen details are shown below.

| Item | Description |
|---|---|
| App name | Enter the app name (appid) to save. |
| Enable | Specifies whether or not to collect the specified app logs.<br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled |
| Size limit | Specifies the limit on the log size of the app (folder size of the app to be saved).<br><br>Setting range: 10000 to 30000 |

5.20.3 Eject

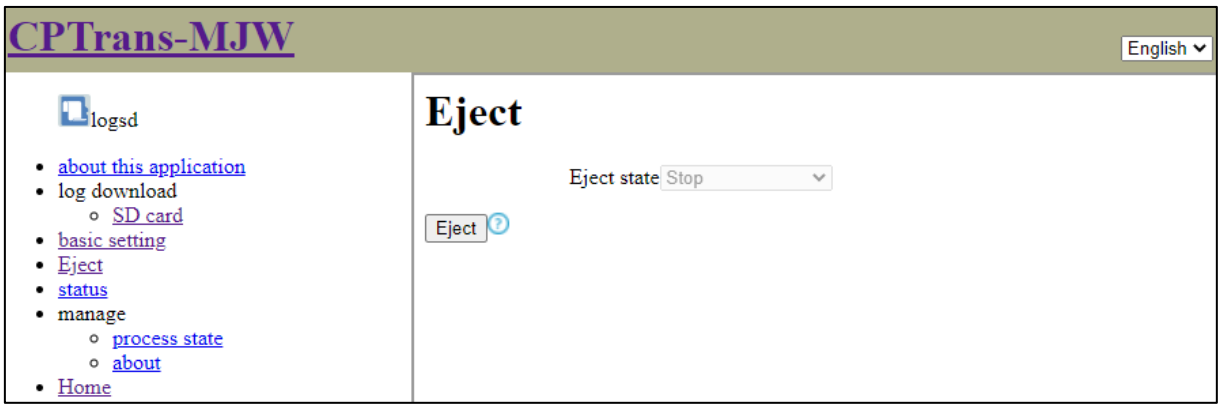



**Figure 5.94 Basic setting**

(1) Eject

| Item | Description |
|---|---|
| Eject state | Displays the eject status.<br>・Stop<br>・Normal operation<br>・Eject in progress<br>・Eject complete |
| Eject | Select this to exit the SD card. |

5.20.4 Status

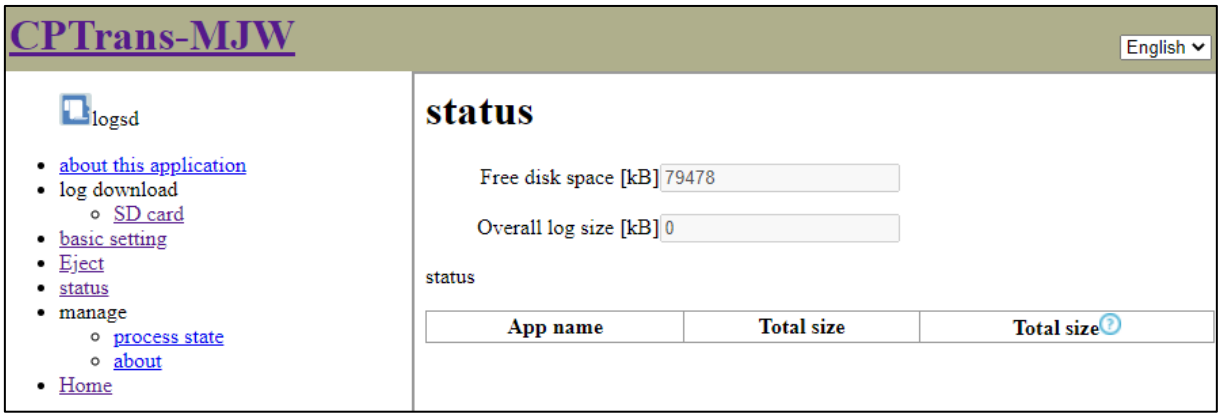



**Figure 5.95 Status**

(1) Status

| Item | Description |
|---|---|
| Free disk space [kB] | Displays the total free space on the SD card. |
| Overall log size [kB] | Select this to exit the SD card. |

Details of the Status screen are shown below.

| Item | Description |
|---|---|
| App name | Displays the app name of the saved log. |
| Total size [kB] | Displays the total size of the log written to the SD card from this product. |
| Total size [kB] | Displays the accumulation of the write size since startup. |

## 5.21 Config mng

Config mng is described below.

| Icon | Overview |
|---|---|
|  | This is an app that allows you to save and capture settings for each app or all settings. |

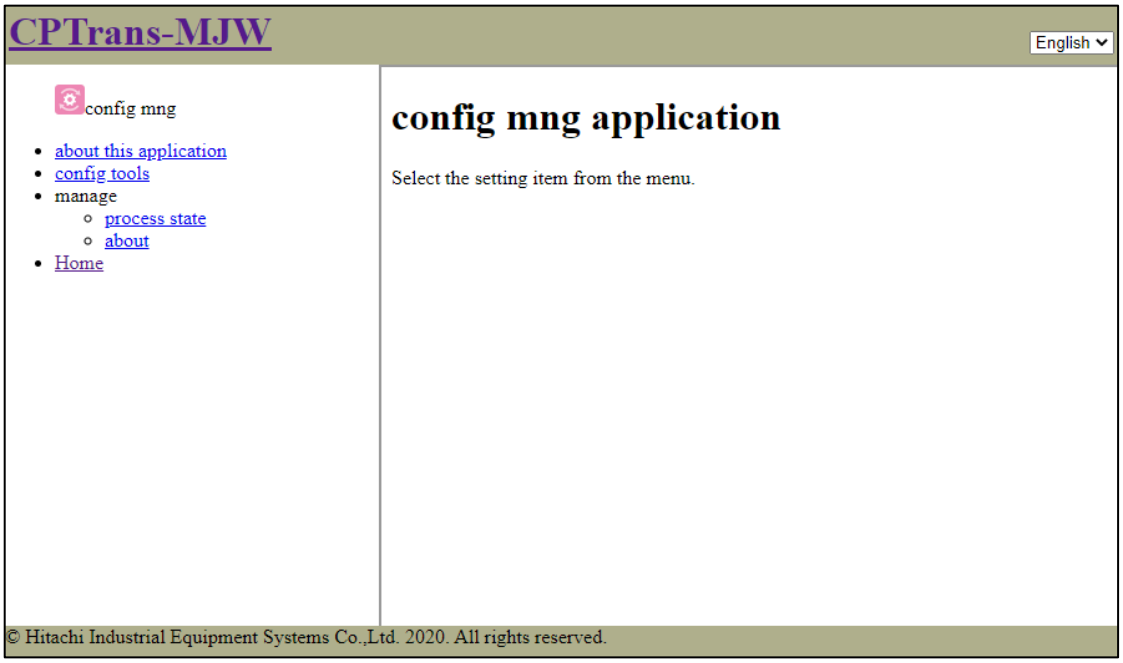



**Figure 5.96 Initial window of config mng application**

The settings can be restored by downloading the settings of each app of this product as text data and uploading the saved text data.

### 5.21.1 Config tools


**Figure 5.97 Config tools**

The details of the configuration tool are shown below.

(1) Download

| Item | Description |
|---|---|
| App selection | Specify the app to read the settings from.<br><br>Options:<br>・"Individual apps ("router", "DDNS General Purpose", etc.)"<br>・(All) |
| Download button | Download the settings of the selected app as text data. |

(2) Upload

| Item | Description |
|---|---|
| Choose file | Select the file you want to upload.<br><br>[Caution]<br>Do not select any text data other than the text data you Download from the Management Application Settings app. |
| Upload button | Upload the selected file.<br><br>Remark: Restarting the product after uploading will reflect the setting. |

## 5.22 Band

Band is described below.

| Icon | Overview |
|---|---|
|  | This is an app that allows to fix and control band for LTE communication. |


**Figure 5.98 Initial window of band application**

### 5.22.1 Band control

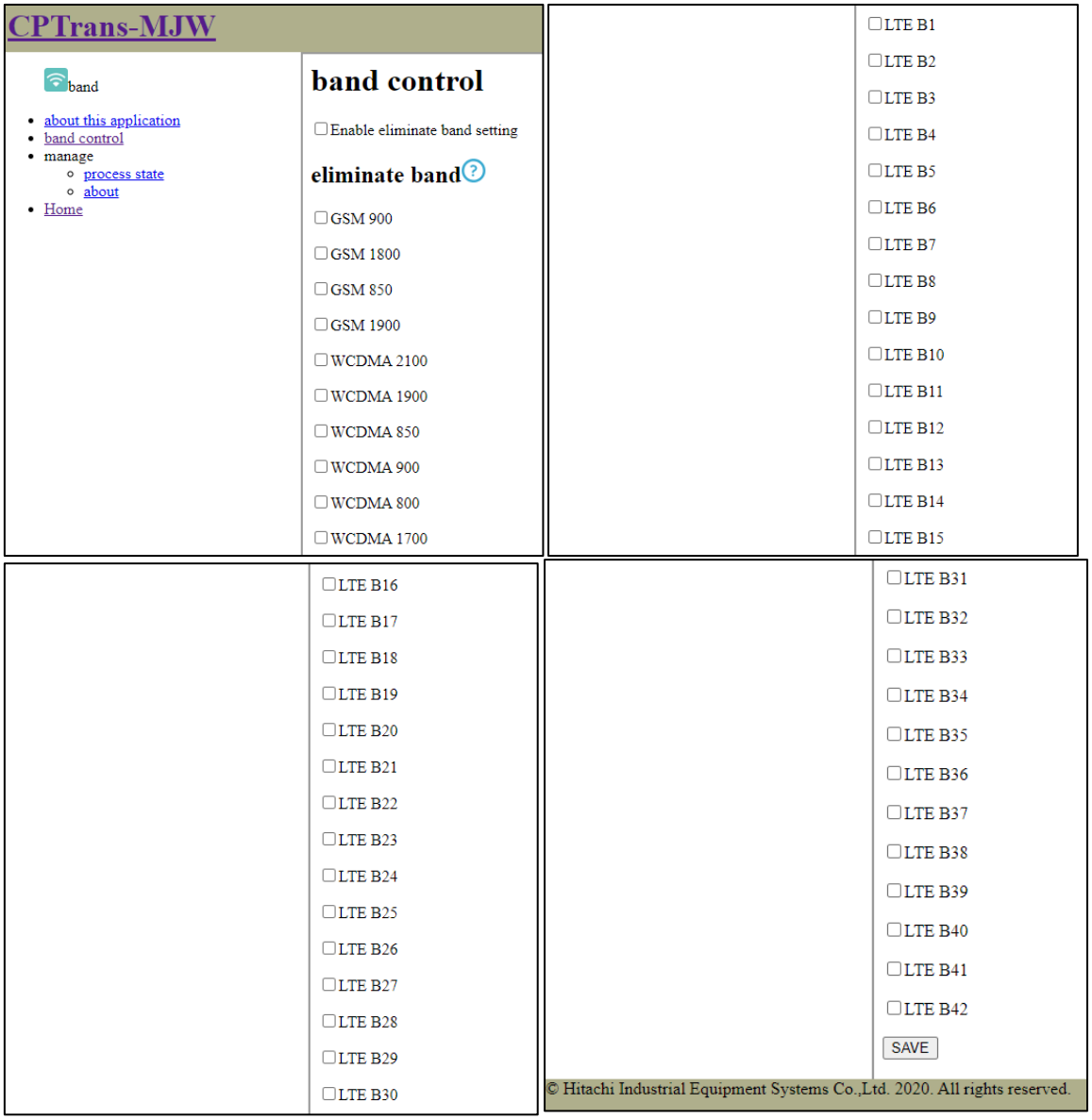



**Figure 5.99 Band control**

| Item | Description |
|---|---|
| Enable eliminate band setting | Enable whether eliminate band when this product connects to the network. |
| GSM 900 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| GSM 1800 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| GSM 850 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| GSM 1900 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| WCDMA 2100 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| WCDMA 1900 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| WCDMA 850 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| WCDMA 900 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| WCDMA 800 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| WCDMA 1700 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B1 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B2 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B3 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B4 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B5 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B6 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B7 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B8 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B9 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B10 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B11 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B12 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B13 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B14 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |

| Item | Description |
|---|---|
| LTE B15 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B16 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B17 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B18 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B19 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B20 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B21 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B22 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B23 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B24 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B25 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B26 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B27 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B28 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B29 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B30 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B31 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B32 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B33 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B34 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B35 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B36 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B37 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B38 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B39 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |

| Item | Description |
|---|---|
| LTE B40 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B41 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |
| LTE B42 | Limit the connection to the band on the left.<br>Checked: Eliminate, No check: Disabled |

## 5.23 Monitoring

Monitoring is described below.

| Icon | Overview |
|---|---|
|  | This is an app that allows to monitor operating status of other application by checking log output from the application. This app can also execute the applications. |


**Figure 5.100 Initial window of monitoring application**

### 5.23.1 Log download

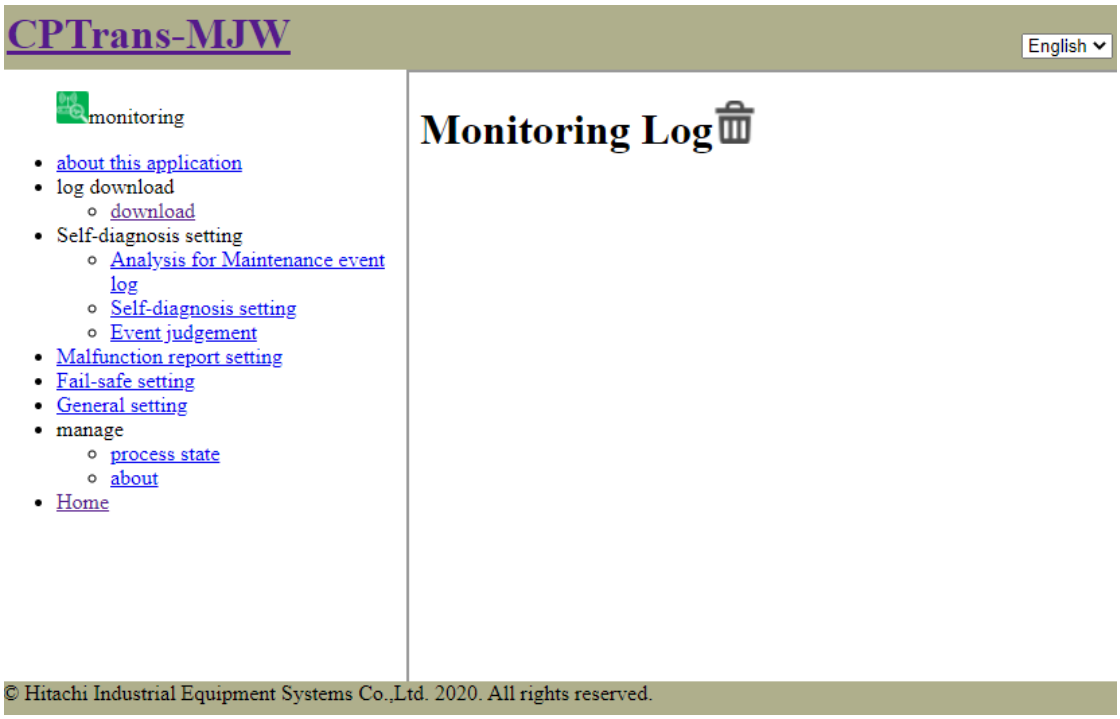



**Figure 5.101 Monitoring log download**

Log data which is stored in the SD card is displayed on this window. The file can be downloaded to connected PC by clicking file name on this application.

### 5.23.2 Self-diagnosis setting

#### 5.23.2.1 Analysis for Maintenance event log

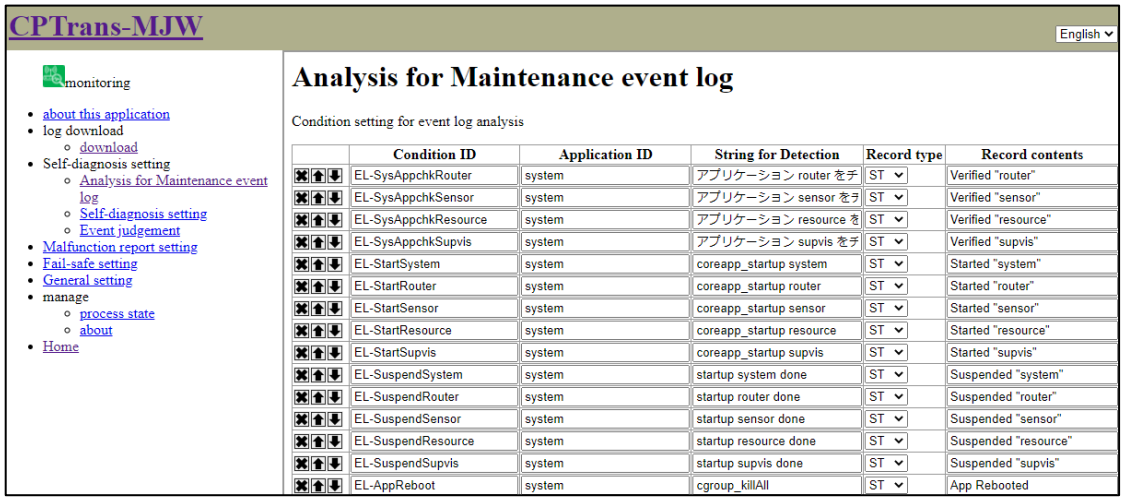



**Figure 5.102 Analysis for Maintenance event log**

| Item | Description |
|---|---|
| Condition ID | An ID information for recognizing an analysis condition. |
| Application ID | Specify target application for referring standard output log. |
| String for detection | Strings data for detection of trigger for record output. |
| Type | Specify type of record.<br><br>#: 1 — Type: ST — Description: Status for each application or transition of state on interface (**S**tate **T**ransition)<br>#: 2 — Type: MM — Description: Management function for connect and disconnect LTE / 3G network (**M**odem **M**anager)<br>#: 3 — Type: ES — Description: Error which occurred on an application (**E**rror **S**tate)<br>#: 4 — Type: FS — Description: Fail-safe function (**F**ail **S**afe)<br>#: 5 — Type: WD — Description: Self-diagnosis for process (software **W**atch-**D**og)<br>#: 6 — Type: EV — Description: Events operated by user (**E**vent)<br>#: 7 — Type: OW — Description: Other events which are not relevant to above (**O**ther**W**ise) |
| Record contents | Descriptions for record data. This item can be specified unique strings. |

### 5.23.2.2 Self-diagnosis setting

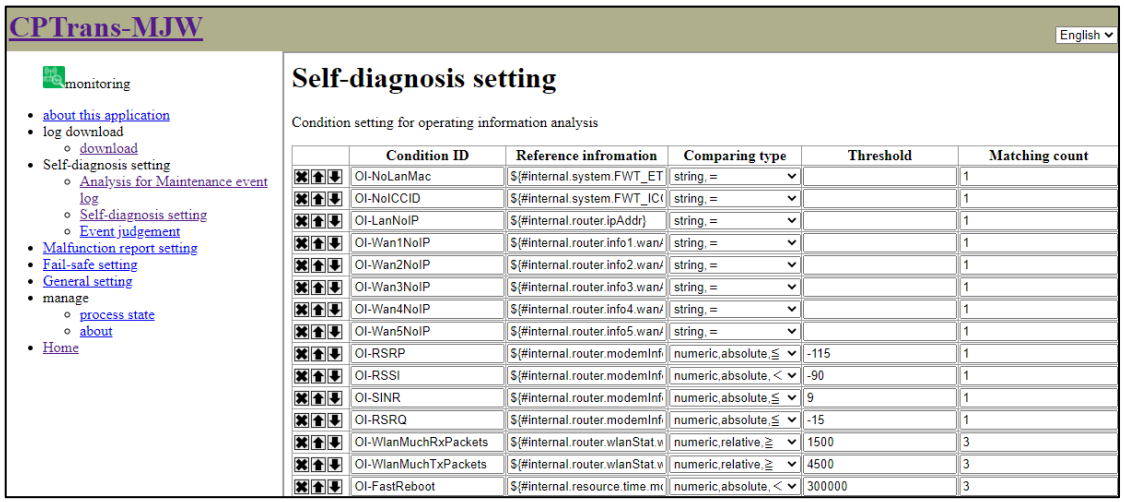



**Figure 5.103 Self-diagnosis setting**

| Item | Description |
|---|---|
| Condition ID | An ID information for recognizing an analysis condition. |
| Reference Information | Specify operating information from other application. Method of referring to other applications is the same as iopoll application. It is gmio (Global Module I/O) described in "${#~}". |
| Type | Specify a condition for comparing. |

| # | Items | Description |
|---|---|---|
| 1 | numeric, absolute, ＝ | Value is equal to threshold (absolute) |
| 2 | numeric, absolute, ≠ | Value is NOT equal to threshold (absolute) |
| 3 | numeric, absolute, ≧ | Value is threshold or higher (absolute) |
| 4 | numeric, absolute, ≦ | Value is threshold or lower (absolute) |
| 5 | numeric, absolute, > | Value is more than threshold (absolute) |
| 6 | numeric, absolute, < | Value is less than threshold (absolute) |
| 7 | numeric, relative, ＝ | Value is equal to threshold (relative) |
| 8 | numeric, relative, ≠ | Value is NOT equal to threshold (relative) |
| 9 | numeric, relative, ≧ | Value is threshold or higher (relative) |
| 10 | numeric, relative, ≦ | Value is threshold or lower (relative) |
| 11 | numeric, relative, > | Value is more than threshold (relative) |
| 12 | numeric, relative, < | Value is less than threshold (relative) |
| 13 | string, ＝ | Value is equal to threshold (string) |
| 14 | string, ≠ | Value is NOT equal to threshold (string) |

| | |
|---|---|
| Threshold | Threshold value for comparison against value. |
| Matching count | Specify number of continuous matchings of above matching condition. |

### 5.23.3 Malfunction report setting

This function is not supported yet.

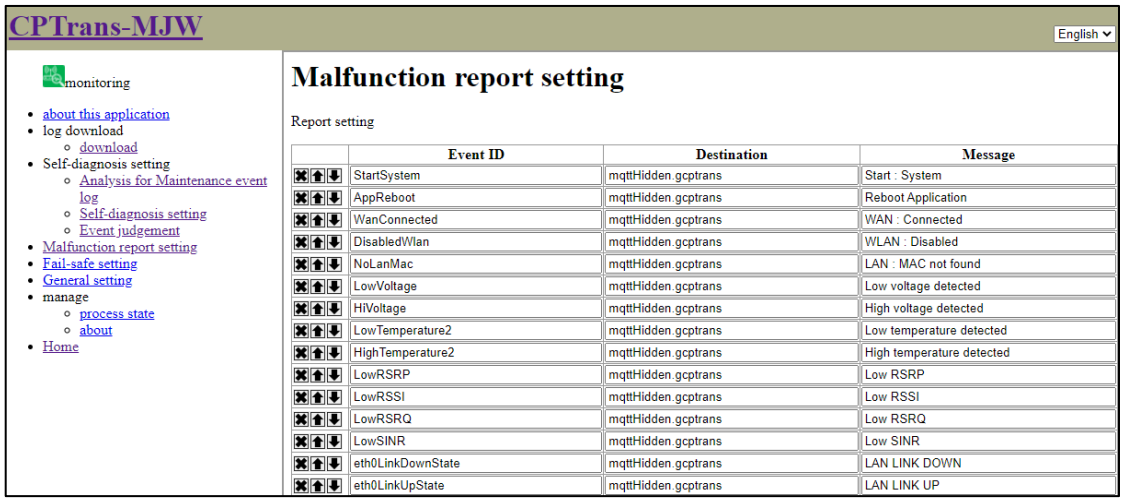



**Figure 5.104 Malfunction report setting**

| Item | Description |
|---|---|
| Event ID | An ID information for recognizing an event condition. |
| Destination | Specify network I/O and topic name for sending notification when an event described in the event ID occurs. |
| Message | Specify message contents which are included in a notification when an event described in the event ID occurs. |

### 5.23.4 Fail-safe setting

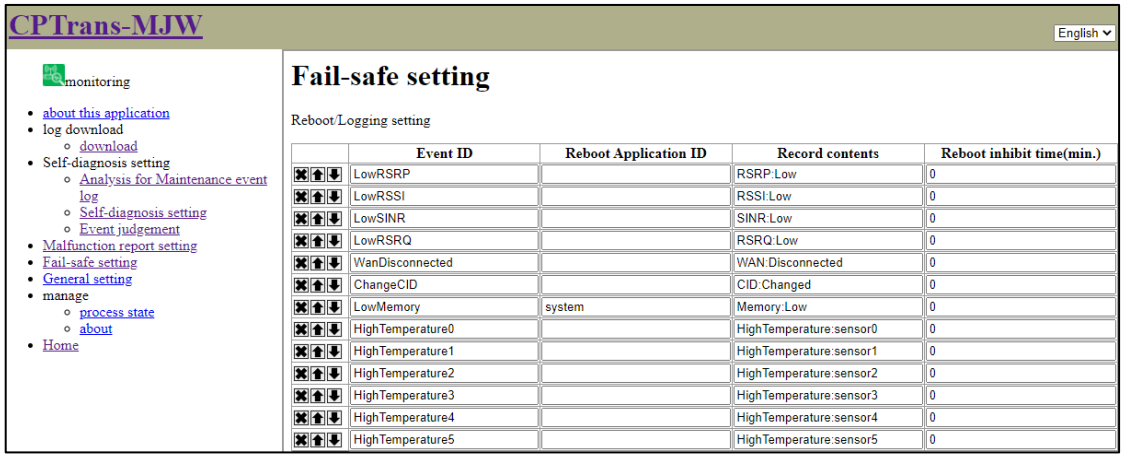



**Figure 5.105 Fail-safe setting**

| Item | Description |
|---|---|
| Event ID | Specify event ID for self-reboot. Event IDs are defined at self-diagnosis function. |
| Reboot Application ID | Specify whether this function execute reboot or not when event ID is issued. To execute system reboot, specify “system”. |
| Record contents | Specify record content to indicate that purpose of reboot is fail-safe.<br>This item can be set for each event ID. |
| Reboot inhibit time(min.) | Specify wait time to start reboot application when above event ID is issued.<br>Purpose of this setting is to avoid unexpected behavior due to immediately reboot at issuing event ID. |

### 5.23.5 General setting

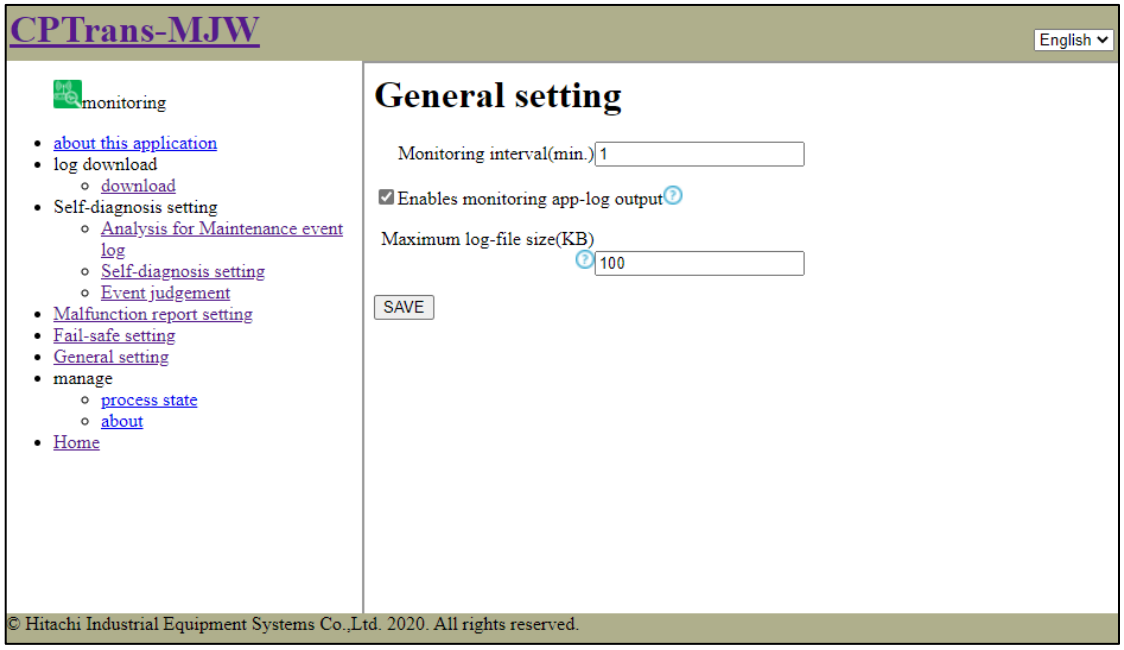



**Figure 5.106 General setting**

| Item | Description |
|---|---|
| Monitoring Interval | Specify interval for monitoring process on this application<br>Setting range: 1 to 65535 |
| Enables monitoring app-log output | Specify whether enable monitoring app-log output or not.<br>Checked: Save log data, no check: log data is not saved |
| Maximum log-file size (KB) | Specify maximum log file size for a file.<br><br>Setting range: 100 to 10000 |

## 5.24 Common to each app

The following describes the common setting items of each app.

### 5.24.1 App about Settings

From the menu of each app, in the Manage → "about" window,

The log output level and suspend the app can be set (enable/disable app startup).

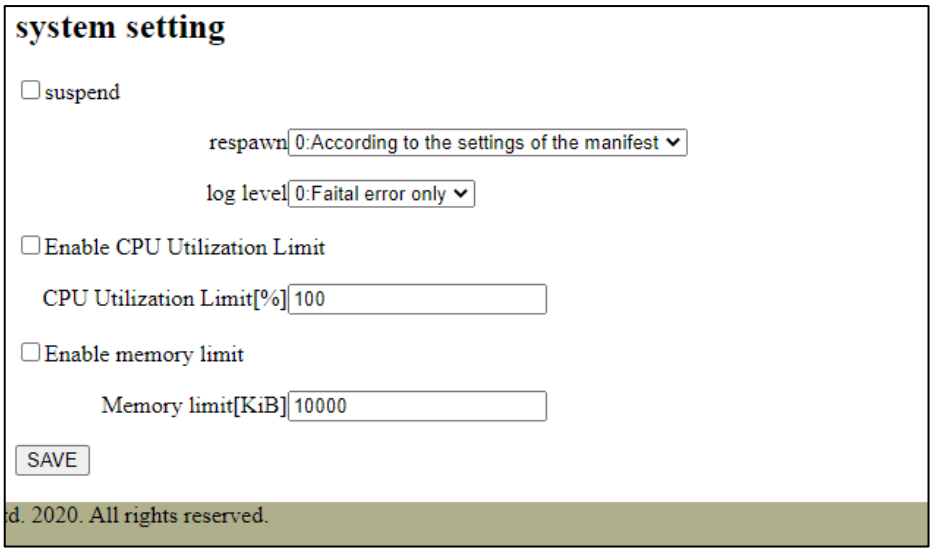
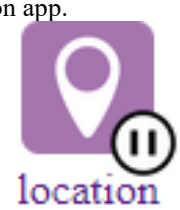



**Figure 5.107 Common setting items of each app**

Details of "System setting items" are shown below.

| Item | Description |
|---|---|
| Suspend | It is possible to enable or disable the startup of the application itself.<br>(If location information app is used, disable this setting.)<br>When this function is enabled, the stop mark "\|\|" is displayed when the app is not running, as in the Location app.<br>  <br><br>Setting range:<br>Checked: Enabled; Not checked: Disabled<br><br>[Caution]<br>For this setting in the "system" app and "router" app,<br>Never set it to "Enable".<br>This product will start up properly and will not be able to operate. |
| Response<br>(Not supported) | [Caution] Do not change the setting. |
| Log Level | Specifies the output level of the log.<br>Level 0: Critical error only<br>Level 1: Show Warnings<br>Level 2: Displays various information.<br>Level 3: View detailed traces |
| Enable CPU Usage Limit<br>(Not supported) | [Caution] Do not change the setting. |
| CPU Usage Limit [%]<br>(Not supported) | [Caution] Do not change the setting. |
| Enable Memory Limit<br>(Not supported) | [Caution] Do not change the setting. |
| Memory limit [KiB]<br>(Not supported) | [Caution] Do not change the setting. |

# 6. Precautions

## 6.1 Precautions for Ethernet

If the communication rate of Ethernet is set to auto (default setting) at startup, communication of Ethernet may fail depending on the connected device.
If this happens, disconnecting and inserting Ethernet cable will restore normal operation. However, if it still fails, fix the communication speed between the product and the connected device.

## 6.2 Notes on Wireless Connectivity in KDDI Networking

If no communication with the wireless network continues after the wireless network is connected, KDDI network releases the session (wireless session or PDN session) between CPTrans⇔KDDI networks even if the non-communication monitoring timer of the PBZ has not expired. When sending packets from CPTrans to the WAN or from the WAN to CPTrans at this timing, the transmitted packets may be discarded. In particular, care must be taken when using UDP without retransmission.
When a packet is exchanged between CPTrans and the wireless network while the session is open, the session (wireless session and PDN session) is established again.
Sessions are released at the following two timings.

(1) When communication with the wireless network has not been performed for 10 seconds after the wireless network has been established
At this time, the PDN session is established, but the wireless session is released.
(2) When no communication continues for 110 seconds after (1)
At this time, it is released until the PDN session.
If a packet is sent to the wireless network in this state, the packet is dropped until the PDN session is re-established.

7. Warranty

The free warranty period for our products is limited to one year from the time you purchase the product or one year from the time the product is delivered to the designated place, whichever is shorter. Note that this free warranty period may not apply if the life of the product is affected by the operating environment or operating conditions.

Note that the warranty described here means the warranty of the delivered product alone, and that any secondary loss caused by the failure of the delivered product is forbidden.

- Do not remove the nameplate sticker attached to the product body. The product-specific serial number is specified. Failure to check the nameplate seal may result in failure or repair.
- If any trouble occurs due to the use of this product, please carefully read this manual and the related documents in this manual before checking. If there are still any defects, please contact the place of purchase.
- Please note that we do not guarantee the operation or performance of this product in the customer network environment. (Although we confirm the connection in our environment, we cannot guarantee the connection in our customer environment. Please verify thoroughly beforehand when using it.)
- Please understand that this product is subject to change without prior notice for product improvement, including the accessories.
- Please note that no warranty of compatibility with the customer system is expressly or implied.
- We assume no responsibility for any damage caused by the software.
- The user is responsible for performing the update. We will bear the cost of responding to this situation.
- Depending on the operating environment and conditions, you may not be able to connect to the LTE or wireless LAN, or you may not be able to obtain a sufficient communication speed.
- This product complies with the Radio Law in Japan, but does not guarantee that it will not affect nearby equipment, etc. Please conduct sufficient verification in advance as necessary.
- This product does not guarantee that there are no security vulnerabilities. Take the necessary security measures as a system.
- Use a stable power supply. Using an unstable power supply may adversely affect the product. In particular, if the power is turned off or the power is not supplied sufficiently immediately after the setting is changed, it may cause a problem with the product.

(Indemnification)

Within or outside the free warranty period, the only scope of our responsibility is to replace the product body. We shall not be held responsible for any damage caused by a security accident, or any other physical or personal damage caused to you by the product malfunction (including secondary costs such as production compensation to the customer, sales compensation, etc., and expenses for repair or restoration of the customer's equipment or facilities, etc.).

・It is agreed by user to the software license upon the start of use of this product.
・We assume no responsibility for any damage caused by the software.
・Updating is performed at the customer's responsibility. In case of our response, we will bear the cost.

8. After-sale service

1） If a failure occurs due to a reason attributable to our responsibility under the normal use condition in accordance with the precautions in the delivered specifications, we will only replace the product with a free of charge for the initial failure. At that time, we will respond only by sending back. In case of support other than the above, all charges will be charged. In addition, please be aware that it will be charged even when we need to respond locally, such as when it is installed on the customer's equipment.

The free warranty period for products replaced under this section shall be the longer of the remaining period of the free warranty at the time of purchase (or delivery) or three months from the date of return of the product to the customer, whichever is longer.

2） Even during the free warranty period, the warranty will not cover any of the following cases.

① The serial number cannot be confirmed on the nameplate.
② The fault is caused by improper condition, environment, or usage other than those specified in the catalog, instruction manual, or specification.
③ Failure caused by improper construction performed by anything other than us.
④ The fault or damage is caused by dropping the product after purchase (or after delivery) or by external pressure, etc.
⑤ Failure due to modifications, repairs, or other modifications to the product without our understanding by the customer
⑥ External factors caused by force majeure such as fire or abnormal voltage, salt damage, gas damage, dust, etc. In addition to failures caused by earthquake, tsunami, lightning, wind and flood damage, and other natural disasters.
⑦ The fault or damage is caused by the device or consumables connected to this product.
⑧ Replacement of consumables, such as accessories
⑨ Travel expenses for repairs on business trips as requested by the customer.
⑩ When corrosion due to water leakage or condensation is found, or when internal boards are damaged or deformed.
⑪ The fault is caused by a reason that cannot be foreseen by the science and technology that was in practical use when the product was shipped from us.
⑫ Failure or damage due to the use of optional parts not provided by us
⑬ When all or part of the item has been modified, modified, or reverse-engineered

3） The cost of the communication contract during the replacement period will be borne by the customer.

4） The data created by the customer when replacing the repair substitute for this product cannot be transferred to the product after replacement. We assume no responsibility for any change, loss, or inability to transfer such data.

5） The unique number assigned to this product will be changed for repair by replacement. Please note in advance.

6） When sending a faulty or repaired product, please contact the status of the fault, customer contact, and return address. Shipping costs shall be borne by the customer, and return costs shall be borne by us. Repairs shall be completed and returned within 15 business days in principle after receipt. However, if there is a reason why we cannot respond within this period, we will determine the date of return after consulting with the customer separately.

7） The retention period of replacement products shall be two years after discontinuance of production. The replacement period is the replacement period. However, please note that it may not be possible to respond due to the lack of replacement products.

9. Precautions for Disposal

Please dispose of this product properly as industrial waste in accordance with local regulations.
For details, contact your local government.

10. Export Trade Control Order

The Products are goods that fall under the provisions of the Ministerial Ordinance on Goods or Technology (Ordinance of the Ministry of Goods, etc.) which provides for goods or technology pursuant to the provisions of Appended Table 1 of the Export Trade Control Order and Appended Table of the Foreign Exchange Order. The product may only be used in Japan. However, you are required to comply with the Export Trade Control Directive in the management and operation of products and documents.

11. Regarding OSS licenses

This product uses software that complies with the following licenses.

1） Apache License

Apache License
Version 2.0, January 2004
https://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction,
And distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by
The copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all
Other entities that control, are controlled by, or are under common
Control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
Direction or management of such entity, whether by contract or
Otherwise, or (ii) ownership of fifty percent (50%) or more of the
Outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
Exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
Including but not limited to software source code, documentation
Source, and configuration files.

"Object" form shall mean any form resulting from mechanical
Transformation or translation of a Source form, including but
Not limited to compiled object code, generated documentation,
And conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or
Object form, made available under the License, as indicated by a
Copyright notice that is included in or attached to the work
(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object
Form, that is based on (or derived from) the Work and for which the
Editorial revisions, annotations, elaborations, or other modifications
Represent, as a whole, an original work of authorship. For the purposes
Of this License, Derivative Works shall not include works that remain
Separable from, or merely link (or bind by name) to the interfaces of,
The Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including

The original version of the Work and any modifications or additions
To that Work or Derivative Works thereof, that is intentionally
Submitted to Licensor for inclusion in the Work by the copyright owner
Or by an individual or Legal Entity authorized to submit on behalf of
The copyright owner. For the purposes of this definition, "submitted"
Means any form of electronic, verbal, or written communication sent
To the Licensor or its representatives, including but not limited to
Communication on electronic mailing lists, source code control systems,
And issue tracking systems that are managed by, or on behalf of, the
Licensor for the purpose of discussing and improving the Work, but
Excluding communication that is conspicuously marked or otherwise
Designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity
On behalf of whom a Contribution has been received by Licensor and
Subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of
This License, each Contributor hereby grants to you a perpetual,
Worldwide, non-exclusive, no-charge, royalty-free, irrevocable
Copyright license to reproduce, prepare Derivative Works of,
Publicly display, publicly perform, sublicense, and distribute the
Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of
This License, each Contributor hereby grants to you a perpetual,
Worldwide, non-exclusive, no-charge, royalty-free, irrevocable
(Except as stated in this section) patent license to make, have made,
Use, offer to sell, sell, import, and otherwise transfer the Work,
Where such license applies only to those patent claims licensable
By such Contributor that are necessarily infringed by their
Contribution(s) alone or by combination of their Contribution(s)
With the Work to which such Contribution(s) was submitted. If You
Institute patent litigation against any entity (including a
Cross-claim or counterclaim in a lawsuit) alleging that the Work
Or a Contribution incorporated within the Work constitutes direct
Or contributory patent infringement, then any patent licenses
Granted to you under this License for that Work shall terminate
As of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
Work or Derivative Works thereof in any medium, with or without
Modifications, and in Source or Object form, provided that you
Meet the following conditions:

(a) You must give any other recipients of the Work or
Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices
Stating that you changed the files; and

(c) You must retain, in the Source form of any Derivative Works
That you distribute, all copyright, patent, trademark, and
Attribution notices from the Source form of the Work,
Excluding those notices that do not pertain to any part of

The Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its Distribution, then any Derivative Works that you distribute must Include a readable copy of the attribution notices contained Within such NOTICE file, excluding those notices that do not Pertain to any part of the Derivative Works, in at least one Of the following places: within a NOTICE text file distributed As part of the Derivative Works; within the Source form or Documentation, if provided along with the Derivative Works; or, Within a display generated by the Derivative Works, if and Wherever such third-party notices normally appear. The contents Of the NOTICE file are for informational purposes only and Do not modify the License. You may add your own attribution Notices within Derivative Works that you distribute, alongside Or as an addendum to the NOTICE text from the Work, provided That such additional attribution notices cannot be construed As modifying the License.

You may add your own copyright statement to your modifications and May provide additional or different license terms and conditions For use, reproduction, or distribution of your modifications, or For any such Derivative Works as a whole, provided your use, Reproduction, and distribution of the Work otherwise complies with The conditions stated in this License.

5. Submission of Contributions. Unless you explicitly state otherwise, Any Contribution intentionally submitted for inclusion in the Work By you to the Licensor shall be under the terms and conditions of This License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify The terms of any separate license agreement you may have executed With Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade Names, trademarks, service marks, or product names of the Licensor, Except as required for reasonable and customary use in describing the Origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or Agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or Implied, including, without limitation, any warranties or conditions Of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the Appropriateness of using or redistributing the Work and assume any Risks associated with your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, Whether in tort (including negligence), contract, or otherwise, Unless required by applicable law (such as deliberate and grossly Negligent acts) or agreed to in writing, shall any Contributor be Liable to You for damages, including any direct, indirect, special, Incidental, or consequential damages of any character arising as a

Result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, Work stoppage, computer failure or malfunction, or any and all Other commercial damages or losses), even if such Contributor Has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing The Work or Derivative Works thereof, you may choose to offer, And charge a fee for, acceptance of support, warranty, indemnity, Or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, you may act only On Your own behalf and on your sole responsibility, not on behalf Of any other Contributor, and only if you agree to indemnify, Defend, and hold each Contributor harmless for any liability Incurred by, or claims asserted against, such Contributor by reason Of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

2） cJSON



3） Libcurl