MITSUBISHI ELECTRIC

Programmable Controller

MELSEC iQ-R series

MELSEC iQ-R OPC UA Server Module
User's Manual (Application)

-RD81OPC96
-SW1DND-ROPCUA-E (MX OPC UA Module Configurator-R)

SAFETY PRECAUTIONS

(Read these precautions before using this product.)

Before using this product, please read this manual and the relevant manuals carefully and pay full attention to safety to handle the product correctly. If the equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

The precautions given in this manual are concerned with this product only. For the safety precautions of the programmable controller system, refer to the MELSEC iQ-R Module Configuration Manual.

In this manual, the safety precautions are classified into two levels: " ⚠ WARNING" and " ⚠ CAUTION".

⚠ **WARNING**	Indicates that incorrect handling may cause hazardous conditions, resulting in death or severe injury.

⚠ **CAUTION**	Indicates that incorrect handling may cause hazardous conditions, resulting in minor or moderate injury or property damage.

Under some circumstances, failure to observe the precautions given under " ⚠ CAUTION" may lead to serious consequences.

Observe the precautions of both levels because they are important for personal and system safety.

Make sure that the end users read this manual and then keep the manual in a safe place for future reference.

[Design Precautions]

⚠WARNING

● Configure safety circuits external to the programmable controller to ensure that the entire system operates safely even when a fault occurs in the external power supply or the programmable controller. Failure to do so may result in an accident due to an incorrect output or malfunction.

   (1) Emergency stop circuits, protection circuits, and protective interlock circuits for conflicting operations (such as forward/reverse rotations or upper/lower limit positioning) must be configured external to the programmable controller.

   (2) When the programmable controller detects an abnormal condition, it stops the operation and all outputs are:

     • Turned off if the overcurrent or overvoltage protection of the power supply module is activated.

     • Held or turned off according to the parameter setting if the self-diagnostic function of the CPU module detects an error such as a watchdog timer error.

   (3) All outputs may be turned on if an error occurs in a part, such as an I/O control part, where the CPU module cannot detect any error. To ensure safety operation in such a case, provide a safety mechanism or a fail-safe circuit external to the programmable controller. For a fail-safe circuit example, refer to "General Safety Requirements" in the MELSEC iQ-R Module Configuration Manual.

   (4) Outputs may remain on or off due to a failure of a component such as a relay and transistor in an output circuit. Configure an external circuit for monitoring output signals that could cause a serious accident.

● In an output circuit, when a load current exceeding the rated current or an overcurrent caused by a load short-circuit flows for a long time, it may cause smoke and fire. To prevent this, configure an external safety circuit, such as a fuse.

● Configure a circuit so that the programmable controller is turned on first and then the external power supply. If the external power supply is turned on first, an accident may occur due to an incorrect output or malfunction.

● Configure a circuit so that the external power supply is turned off first and then the programmable controller. If the programmable controller is turned off first, an accident may occur due to an incorrect output or malfunction.

● For the operating status of each station after a communication failure, refer to manuals for the network used. For the manuals, please consult your local Mitsubishi representative. Incorrect output or malfunction due to a communication failure may result in an accident.

● When connecting an external device with a CPU module or intelligent function module to modify data of a running programmable controller, configure an interlock circuit in the program to ensure that the entire system will always operate safely. For other forms of control (such as program modification, parameter change, forced output, or operating status change) of a running programmable controller, read the relevant manuals carefully and ensure that the operation is safe before proceeding. Improper operation may damage machines or cause accidents. When a Safety CPU is used, data cannot be modified while the Safety CPU is in SAFETY MODE.

● Especially, when a remote programmable controller is controlled by an external device, immediate action cannot be taken if a problem occurs in the programmable controller due to a communication failure. To prevent this, configure an interlock circuit in the program, and determine corrective actions to be taken between the external device and CPU module in case of a communication failure.

[Design Precautions]

⚠ WARNING

● Do not write any data to the "system area" and "write-protect area" of the buffer memory in the module. Also, do not use any "use prohibited" signals as an output signal from the CPU module to each module. Doing so may cause malfunction of the programmable controller system. For the "system area", "write-protect area", and the "use prohibited" signals, refer to the user's manual for the module used. For areas used for safety communications, they are protected from being written by users, and thus safety communications failure caused by data writing does not occur.

● If a communication cable is disconnected, the network may be unstable, resulting in a communication failure of multiple stations. Configure an interlock circuit in the program to ensure that the entire system will always operate safely even if communications fail. Incorrect output or malfunction due to a communication failure may result in an accident. When safety communications are used, an interlock by the safety station interlock function protects the system from an incorrect output or malfunction.

[Design Precautions]

⚠ CAUTION

● Do not install the control lines or communication cables together with the main circuit lines or power cables. Doing so may result in malfunction due to electromagnetic interference. Keep a distance of 100mm or more between those cables.

● During control of an inductive load such as a lamp, heater, or solenoid valve, a large current (approximately ten times greater than normal) may flow when the output is turned from off to on. Therefore, use a module that has a sufficient current rating.

● After the CPU module is powered on or is reset, the time taken to enter the RUN status varies depending on the system configuration, parameter settings, and/or program size. Design circuits so that the entire system will always operate safely, regardless of the time.

● Do not power off the programmable controller or reset the CPU module while the settings are being written. Doing so will make the data in the flash ROM and SD memory card undefined. The values need to be set in the buffer memory and written to the flash ROM and SD memory card again. Doing so also may cause malfunction or failure of the module.

● When changing the operating status of the CPU module from external devices (such as the remote RUN/STOP functions), select "Do Not Open by Program" for "Opening Method" of "Module Parameter". If "Open by Program" is selected, an execution of the remote STOP function causes the communication line to close. Consequently, the CPU module cannot reopen the line, and external devices cannot execute the remote RUN function.

[Security Precautions]

⚠ WARNING

● To maintain the security (confidentiality, integrity, and availability) of the programmable controller and the system against unauthorized access, denial-of-service (DoS) attacks, computer viruses, and other cyberattacks from external devices via the network, take appropriate measures such as firewalls, virtual private networks (VPNs), and antivirus solutions.

[Installation Precautions]

⚠WARNING

● Shut off the external power supply (all phases) used in the system before mounting or removing the module. Failure to do so may result in electric shock or cause the module to fail or malfunction.

[Installation Precautions]

⚠CAUTION

● Use the programmable controller in an environment that meets the general specifications in the MELSEC iQ-R Module Configuration Manual. Failure to do so may result in electric shock, fire, malfunction, or damage to or deterioration of the product.

● To mount a module, place the concave part(s) located at the bottom onto the guide(s) of the base unit, and push in the module until the hook(s) located at the top snaps into place. Incorrect interconnection may cause malfunction, failure, or drop of the module.

● To mount a module with no module fixing hook, place the concave part(s) located at the bottom onto the guide(s) of the base unit, push in the module, and fix it with screw(s). Incorrect interconnection may cause malfunction, failure, or drop of the module.

● When using the programmable controller in an environment of frequent vibrations, fix the module with a screw.

● Tighten the screws within the specified torque range. Undertightening can cause drop of the component or wire, short circuit, or malfunction. Overtightening can damage the screw and/or module, resulting in drop, short circuit, or malfunction. For the specified torque range, refer to the MELSEC iQ-R Module Configuration Manual.

● When using an extension cable, connect it to the extension cable connector of the base unit securely. Check the connection for looseness. Poor contact may cause malfunction.

● When using an SD memory card, fully insert it into the SD memory card slot. Check that it is inserted completely. Poor contact may cause malfunction.

● Securely insert an extended SRAM cassette or a battery-less option cassette into the cassette connector of the CPU module. After insertion, close the cassette cover and check that the cassette is inserted completely. Poor contact may cause malfunction.

● Beware that the module could be very hot while power is on and immediately after power-off.

● Do not directly touch any conductive parts and electronic components of the module, SD memory card, extended SRAM cassette, battery-less option cassette, or connector. Doing so can cause malfunction or failure of the module.

[Wiring Precautions]

⚠WARNING

● Shut off the external power supply (all phases) used in the system before installation and wiring. Failure to do so may result in electric shock or cause the module to fail or malfunction.

● After installation and wiring, attach a blank cover module (RG60) to each empty slot before powering on the system for operation. Also, attach an extension connector protective cover[*1] to each unused extension cable connector as necessary. Directly touching any conductive parts of the connectors while power is on may result in electric shock.

*1 For details, please consult your local Mitsubishi Electric representative.

[Wiring Precautions]

⚠CAUTION

● Individually ground the FG and LG terminals of the programmable controller with a ground resistance of 100 ohms or less. Failure to do so may result in electric shock or malfunction.

● Use applicable solderless terminals and tighten them within the specified torque range. If any spade solderless terminal is used, it may be disconnected when the terminal screw comes loose, resulting in failure.

● Check the rated voltage and signal layout before wiring to the module, and connect the cables correctly. Connecting a power supply with a different voltage rating or incorrect wiring may cause fire or failure.

● Connectors for external devices must be crimped or pressed with the tool specified by the manufacturer, or must be correctly soldered. Incomplete connections may cause short circuit, fire, or malfunction.

● Securely connect the connector to the module. Poor contact may cause malfunction.

● Do not install the control lines or communication cables together with the main circuit lines or power cables. Doing so may result in malfunction due to noise. Keep a distance of 100mm or more between those cables.

● Place the cables in a duct or clamp them. If not, dangling cables may swing or inadvertently be pulled, resulting in malfunction or damage to modules or cables.
In addition, the weight of the cables may put stress on modules in an environment of strong vibrations and shocks.
Do not clamp the extension cables with the jacket stripped. Doing so may change the characteristics of the cables, resulting in malfunction.

● Check the interface type and correctly connect the cable. Incorrect wiring (connecting the cable to an incorrect interface) may cause failure of the module and external device.

● Tighten the terminal screws or connector screws within the specified torque range. Undertightening can cause drop of the screw, short circuit, fire, or malfunction. Overtightening can damage the screw and/or module, resulting in drop, short circuit, fire, or malfunction.

● When disconnecting the cable from the module, do not pull the cable by the cable part. For the cable with connector, hold the connector part of the cable. For the cable connected to the terminal block, loosen the terminal screw. Pulling the cable connected to the module may result in malfunction or damage to the module or cable.

● Prevent foreign matter such as dust or wire chips from entering the module. Such foreign matter can cause a fire, failure, or malfunction.

● When a protective film is attached to the top of the module, remove it before system operation. If not, inadequate heat dissipation of the module may cause a fire, failure, or malfunction.

[Wiring Precautions]

⚠CAUTION

● Programmable controllers must be installed in control panels. Connect the main power supply to the power supply module in the control panel through a relay terminal block. Wiring and replacement of a power supply module must be performed by qualified maintenance personnel with knowledge of protection against electric shock. For wiring, refer to the MELSEC iQ-R Module Configuration Manual.

● For Ethernet cables to be used in the system, select the ones that meet the specifications in the user's manual for the module used. If not, normal data transmission is not guaranteed.

[Startup and Maintenance Precautions]

⚠WARNING

● Do not touch any terminal while power is on. Doing so will cause electric shock or malfunction.

● Correctly connect the battery connector. Do not charge, disassemble, heat, short-circuit, solder, or throw the battery into the fire. Also, do not expose it to liquid or strong shock. Doing so will cause the battery to produce heat, explode, ignite, or leak, resulting in injury and fire.

● Shut off the external power supply (all phases) used in the system before cleaning the module or retightening the terminal screws, connector screws, or module fixing screws. Failure to do so may result in electric shock.

[Startup and Maintenance Precautions]

⚠CAUTION

- When connecting an external device with a CPU module or intelligent function module to modify data of a running programmable controller, configure an interlock circuit in the program to ensure that the entire system will always operate safely. For other forms of control (such as program modification, parameter change, forced output, or operating status change) of a running programmable controller, read the relevant manuals carefully and ensure that the operation is safe before proceeding. Improper operation may damage machines or cause accidents.

- Especially, when a remote programmable controller is controlled by an external device, immediate action cannot be taken if a problem occurs in the programmable controller due to a communication failure. To prevent this, configure an interlock circuit in the program, and determine corrective actions to be taken between the external device and CPU module in case of a communication failure.

- Do not disassemble or modify the modules. Doing so may cause failure, malfunction, injury, or a fire.

- Use any radio communication device such as a cellular phone or PHS (Personal Handy-phone System) 25cm or more away in all directions from the programmable controller. Failure to do so may cause malfunction.

- Shut off the external power supply (all phases) used in the system before mounting or removing the module. Failure to do so may cause the module to fail or malfunction.

- Tighten the screws within the specified torque range. Undertightening can cause drop of the component or wire, short circuit, or malfunction. Overtightening can damage the screw and/or module, resulting in drop, short circuit, or malfunction.

- After the first use of the product, do not perform each of the following operations more than 50 times (IEC 61131-2/JIS B 3502 compliant).
  Exceeding the limit may cause malfunction.
    - Mounting/removing the module to/from the base unit
    - Inserting/removing the extended SRAM cassette or battery-less option cassette to/from the CPU module
    - Mounting/removing the terminal block to/from the module
    - Connecting/disconnecting the extension cable to/from the base unit

- After the first use of the product, do not insert/remove the SD memory card to/from the CPU module more than 500 times. Exceeding the limit may cause malfunction.

- Do not touch the metal terminals on the back side of the SD memory card. Doing so may cause malfunction or failure of the module.

- Do not touch the integrated circuits on the circuit board of an extended SRAM cassette or a battery-less option cassette. Doing so may cause malfunction or failure of the module.

- Do not drop or apply shock to the battery to be installed in the module. Doing so may damage the battery, causing the battery fluid to leak inside the battery. If the battery is dropped or any shock is applied to it, dispose of it without using.

- Startup and maintenance of a control panel must be performed by qualified maintenance personnel with knowledge of protection against electric shock. Lock the control panel so that only qualified maintenance personnel can operate it.

[Startup and Maintenance Precautions]

⚠CAUTION

- Before handling the module, touch a conducting object such as a grounded metal to discharge the static electricity from the human body. Wearing a grounded antistatic wrist strap is recommended. Failure to discharge the static electricity may cause the module to fail or malfunction.
- After unpacking, eliminate static electricity from the module to prevent electrostatic discharge from affecting the module. If an electrostatically charged module comes in contact with a grounded metal object, a sudden electrostatic discharge of the module may cause failure.
  For details on how to eliminate static electricity from the module, refer to the following.
  Antistatic Precautions Before Using MELSEC iQ-R Series Products (FA-A-0368)
- Use a clean and dry cloth to wipe off dirt on the module.

[Operating Precautions]

⚠CAUTION

- When changing data and operating status, and modifying program of the running programmable controller from an external device such as a personal computer connected to an intelligent function module, read relevant manuals carefully and ensure the safety before operation. Incorrect change or modification may cause system malfunction, damage to the machines, or accidents.
- Do not power off the programmable controller or reset the CPU module while the setting values in the buffer memory are being written to the flash ROM in the module. Doing so will make the data in the flash ROM and SD memory card undefined. The values need to be set in the buffer memory and written to the flash ROM and SD memory card again. Doing so can cause malfunction or failure of the module.

[Disposal Precautions]

⚠CAUTION

- When disposing of this product, treat it as industrial waste.
- When disposing of batteries, separate them from other wastes according to the local regulations. For details on battery regulations in EU member states, refer to the MELSEC iQ-R Module Configuration Manual.

[Transportation Precautions]

⚠CAUTION

- When transporting lithium batteries, follow the transportation regulations. For details on the regulated models, refer to the MELSEC iQ-R Module Configuration Manual.
- The halogens (such as fluorine, chlorine, bromine, and iodine), which are contained in a fumigant used for disinfection and pest control of wood packaging materials, may cause failure of the product. Prevent the entry of fumigant residues into the product or consider other methods (such as heat treatment) instead of fumigation. The disinfection and pest control measures must be applied to unprocessed raw wood.

CONDITIONS OF USE FOR THE PRODUCT

(1) MELSEC programmable controller ("the PRODUCT") shall be used in conditions;

i) where any problem, fault or failure occurring in the PRODUCT, if any, shall not lead to any major or serious accident; and

ii) where the backup and fail-safe function are systematically or automatically provided outside of the PRODUCT for the case of any problem, fault or failure occurring in the PRODUCT.

(2) The PRODUCT has been designed and manufactured for the purpose of being used in general industries.

MITSUBISHI ELECTRIC SHALL HAVE NO RESPONSIBILITY OR LIABILITY (INCLUDING, BUT NOT LIMITED TO ANY AND ALL RESPONSIBILITY OR LIABILITY BASED ON CONTRACT, WARRANTY, TORT, PRODUCT LIABILITY) FOR ANY INJURY OR DEATH TO PERSONS OR LOSS OR DAMAGE TO PROPERTY CAUSED BY the PRODUCT THAT ARE OPERATED OR USED IN APPLICATION NOT INTENDED OR EXCLUDED BY INSTRUCTIONS, PRECAUTIONS, OR WARNING CONTAINED IN MITSUBISHI ELECTRIC USER'S, INSTRUCTION AND/OR SAFETY MANUALS, TECHNICAL BULLETINS AND GUIDELINES FOR the PRODUCT.

("Prohibited Application")

Prohibited Applications include, but not limited to, the use of the PRODUCT in;

- Nuclear Power Plants and any other power plants operated by Power companies, and/or any other cases in which the public could be affected if any problem or fault occurs in the PRODUCT.

- Railway companies or Public service purposes, and/or any other cases in which establishment of a special quality assurance system is required by the Purchaser or End User.

- Aircraft or Aerospace, Medical applications, Train equipment, transport equipment such as Elevator and Escalator, Incineration and Fuel devices, Vehicles, Manned transportation, Equipment for Recreation and Amusement, and Safety devices, handling of Nuclear or Hazardous Materials or Chemicals, Mining and Drilling, and/or other applications where there is a significant risk of injury to the public or property.

Notwithstanding the above restrictions, Mitsubishi Electric may in its sole discretion, authorize use of the PRODUCT in one or more of the Prohibited Applications, provided that the usage of the PRODUCT is limited only for the specific applications agreed to by Mitsubishi Electric and provided further that no special quality assurance or fail-safe, redundant or other safety features which exceed the general specifications of the PRODUCTs are required. For details, please contact the Mitsubishi Electric representative in your region.

(3) Mitsubishi Electric shall have no responsibility or liability for any problems involving programmable controller trouble and system trouble caused by DoS attacks, unauthorized access, computer viruses, and other cyberattacks.

INTRODUCTION

Thank you for purchasing the Mitsubishi Electric MELSEC iQ-R series programmable controllers.

MX OPC UA Module Configurator-R has the tag mode and information model mode. For the overview of each mode, refer to the following.

📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

This manual describes the contents for using the tag mode and common to each mode.

For using the information model mode, read the following manual.

📖MELSEC iQ-R OPC UA Server Module User's Manual (Information Model)

Before using this product, please read this manual and the relevant manuals carefully and develop familiarity with the functions and performance of the MELSEC iQ-R series programmable controller to handle the product correctly.

When applying the program examples provided in this manual to an actual system, ensure the applicability and confirm that it will not cause system control problems.

Please make sure that the end users read this manual.

> **Point** 🔑
>
> The program examples shown in this manual are the examples in which an OPC UA server module (RD81OPC96) is assigned to the input/output No. X/Y0 to X/Y1F unless otherwise specified. To use the program examples shown in this manual, the input/output number assignment is required. For details on the assignment of input/output number, refer to the following:
>
> 📖MELSEC iQ-R Module Configuration Manual

Relevant product

RD81OPC96

CONTENTS

CONTENTS

13

RELEVANT MANUALS

Manual name [manual number]	Description	Available form
MELSEC iQ-R OPC UA Server Module User's Manual (Application) [SH-081694ENG] (this manual)	Functions, configuration tool, parameter setting, troubleshooting, input/output signals, and buffer memory in the tag mode (and common to each mode) of an OPC UA server module	Print book e-Manual PDF
MELSEC iQ-R OPC UA Server Module User's Manual (Startup) [SH-081693ENG]	Specifications, procedure for operation, wiring, and operation examples in the tag mode (and common to each mode) of an OPC UA server module	Print book e-Manual PDF
MELSEC iQ-R OPC UA Server Module User's Manual (Information Model) [SH-082679ENG]	Specifications, procedure for operation, functions, configuration tool, and troubleshooting in the information model mode of an OPC UA server module	Print book e-Manual PDF
GX Works3 Operating Manual [SH-081215ENG]	System configurations, parameter settings, and operation methods for the online function in GX Works3	e-Manual PDF
MELSEC iQ-R Module Configuration Manual [SH-081262ENG]	The combination of the MELSEC iQ-R series modules, common information on the installation/wiring in the system, and specifications of the power supply module, base unit, SD memory card, and battery	Print book e-Manual PDF

Point

e-Manual refers to the Mitsubishi Electric FA electronic book manuals that can be browsed using a dedicated tool.

e-Manual has the following features:

• Required information can be cross-searched in multiple manuals.

• Other manuals can be accessed from the links in the manual.

• Hardware specifications of each part can be found from the product figures.

• Pages that users often browse can be bookmarked.

• Sample programs can be copied to an engineering tool.

TERMS

Unless otherwise specified, this manual uses the following terms.

Term	Description
Address space	Data that contains information of an access target device, a group, and a tag
Clamping	It is to control a value in the range of the set upper and lower limit values.
Discovery server	A server that manages endpoints of each OPC UA server on a network
Engineering tool	A tool used for setting up programmable controllers, programming, debugging, and maintenance. For the supported tools, refer to the following: 📖MELSEC iQ-R Module Configuration Manual

For definitions of terms for safety CPUs, refer to the following:
📖MELSEC iQ-R CPU Module User's Manual (Application)

GENERIC TERMS AND ABBREVIATIONS

Unless otherwise specified, this manual uses the following generic terms and abbreviations.

Generic term/abbreviation	Description
Configuration tool	MX OPC UA Module Configurator-R
Information model mode	A mode that supports information models. Nodes published to an AddressSpace can be imported from an information model file (XML file), and data can be set (mapped) for each Node.
MC Works64	Mitsubishi Electric SCADA software package
OPC UA	OPC Unified Architecture. Platform independent service-oriented architecture that integrates all the functionality of each OPC Classic specification into an extensible framework.
OPC UA server module	A MELSEC iQ-R OPC UA server module
Tag mode	A mode for setting tags or groups (Nodes) published to an AddressSpace. Tags or groups can be created, and data used for tags can be set.

1 FUNCTIONS

This chapter explains the details on the functions of an OPC UA server module.

1.1 OPC UA Server Function

Data Access function

This function allows an OPC UA client to access tags (devices of a CPU module such as one on the own station or on a network) and structure labels[1] registered in the address space set in the configuration tool.

 *1   Members of a structure are treated as tags.

A tag value registered in the address space is updated based on a set polling cycle.

A function related to Data Access supports 'Standard DataChange Subscription Server Facet' of the OPC UA specifications.

(1) OPC UA server module
(2) OPC UA client
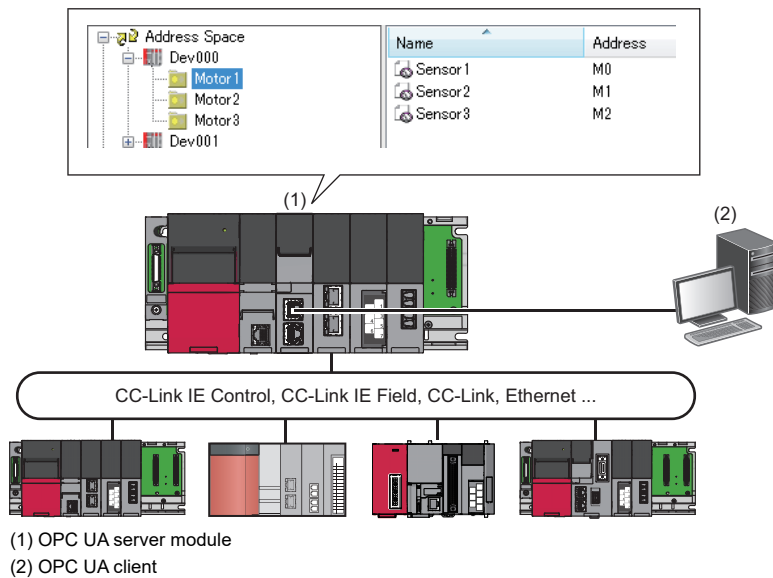
Setting method

For the setting method of the address space, refer to the following:

🔗 Page 32 Address Space Setting

Data type

For accessible data types, refer to the following:

📖 MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

Timing to read data in an OPC UA client (Read)

When an OPC UA client requests to read a tag value in the address space, a tag value at the time when the communication time and the OPC UA processing time elapse from the request timing is read.
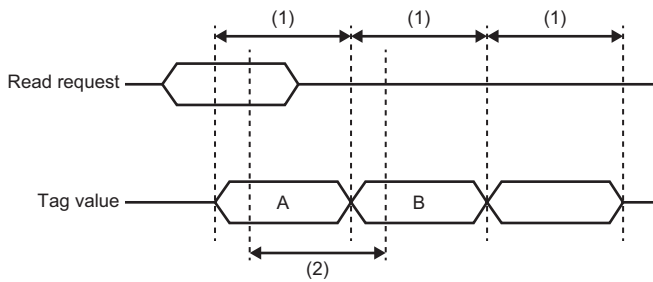
A: Tag value at the request timing of an OPC UA client
B: Tag value to notify an OPC UA client
(1) Polling cycle
(2) Communication time + OPC UA processing

Timing to write data from an OPC UA client (Write)

When an OPC UA client requests to write a tag value in the address space, the tag value is written when the communication time and the OPC UA processing time elapse from the request timing.
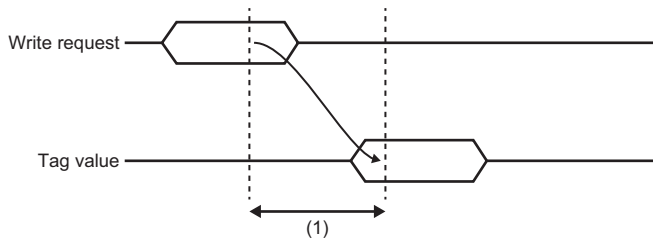
(1) Communication time + OPC UA processing

Security function

This function prevents assets stored in an OPC UA server module from being stolen, falsified, operated incorrectly, and executed improperly due to unauthorized access from a third party.

Security setting function

This function sets security for the connection between an OPC UA server module and OPC UA client.

■Security policy

Security policies can be set in the configuration tool. (☞ Page 59 OPC UA Server Setting)

When setting a security policy, operations (security policies to be enabled) differ for each combination of the firmware version of an OPC UA server module and software version of the configuration tool.

| Firmware version	Software version '1.07H' or later (Selection with the checkbox)	Software version '1.06G' or earlier (Selection in the combo box)
'08' or later	• Security policies can be set to enable or disable in any combination. • When unselecting all checkboxes, "None" is selected and all security policies including "None" are enabled.	• When selecting "None," all security policies are enabled.[1] • When selecting a security policy other than "None," all security policies equal to or stronger than the selected one are enabled.[2]
'06' or '07'	All security policies equal to or stronger than the selected one are enabled.[2] However, the security policies ('Basic128Rsa15' and 'Basic256') are not enabled, because they are not recommended. • When selecting "None," "None" and "Basic256Sha256" are enabled. • When selecting "Basic128Rsa15," "Basic256," and "Basic256Sha256," only "Basic256Sha256" is enabled.	
'05' or earlier	All security policies equal to or stronger than the selected one are enabled.[2]	

[1] 'Aes256-Sha256-RsaPss' and 'Aes128-Sha256-RsaOaep' are also enabled.

[2] The order of strength is as follows. ('Basic256Sha256' is supported in firmware version '02' or later.)
None < Basic128Rsa15 < Basic256 < Basic256Sha256

■Security mode

Security modes can be set in the configuration tool. (☞ Page 59 OPC UA Server Setting)

All security modes equal to or stronger than the set one are enabled.[1]

[1] The order of strength is as follows:
None < Sign < Sign & Encrypt

User authentication function

This function controls access to an OPC UA server module to prevent unauthorized access by users other than specific users.

■Authentication with a user name and password

Authentication with a user name and password is performed when accessing an OPC UA server module from the configuration tool or an OPC UA client.

Item	Specification	Setting method
Number of users	Up to 16 users	☞ Page 55 Security Setting
User Name	Length: Up to 32 characters	
Password	Length: Up to 32 characters	
Default user	User name: RD81OPC96 Password: MITSUBISHI	

■Authentication with a certificate

Authentication with a certificate is performed when accessing an OPC UA server module from an OPC UA client.

For details on the setting method, refer to the following:

☞ Page 55 Security Setting

Conversion function

This function converts device values and values in the engineering unit.

Device values and values in the engineering unit are converted by specifying their ranges.

Conversion type

The following table shows the available conversion for an OPC UA server module.

Conversion type	Description	Setting method
None (Double type)	To convert values to Double type. (Values themselves are not converted.) The engineering unit (EU) and a device value (IR) cannot be set.	☞ Page 50 Conversion Definition Setting
Linear	To convert values by using a linear function.	
Square root	To convert values by using a quadratic function.	

Linear function conversion

The following formula is used for linear function conversion (linear conversion).

■When reading a value from a device

$$y = E_{Min} + \frac{(E_{Max} - E_{Min}) \times (x - R_{Min})}{(R_{Max} - R_{Min})}$$

x: Device value

y: Value in the engineering unit

R_{Max}: Maximum device value (IR)

R_{Min}: Minimum device value (IR)

E_{Max}: Maximum value of the engineering unit (EU)

E_{Min}: Minimum value of the engineering unit (EU)

■When writing a value to a device

$$x = R_{Min} + \frac{(y - E_{Min}) \times (R_{Max} - R_{Min})}{(E_{Max} - E_{Min})}$$

x: Device value

y: Value in the engineering unit

R_{Max}: Maximum device value (IR)

R_{Min}: Minimum device value (IR)

E_{Max}: Maximum value of the engineering unit (EU)

E_{Min}: Minimum value of the engineering unit (EU)

Quadratic function conversion

The following formula is used for quadratic function conversion (square-root conversion).

■When reading a value from a device

$$y = E_{Min} + \frac{(E_{Max} - E_{Min}) \times \sqrt{(x - R_{Min})}}{\sqrt{(R_{Max} - R_{Min})}}$$

x: Device value

y: Value in the engineering unit

R_{Max}: Maximum device value (IR)

R_{Min}: Minimum device value (IR)

E_{Max}: Maximum value of the engineering unit (EU)

E_{Min}: Minimum value of the engineering unit (EU)

■When writing a value to a device

$$x = R_{Min} + \frac{(y - E_{Min})^2 \times (R_{Max} - R_{Min})}{(E_{Max} - E_{Min})^2}$$

x: Device value

y: Value in the engineering unit

R_{Max}: Maximum device value (IR)

R_{Min}: Minimum device value (IR)

E_{Max}: Maximum value of the engineering unit (EU)

E_{Min}: Minimum value of the engineering unit (EU)

Clamping

When selecting "Linear" or "Square Root" for "Conversion Type," values in the engineering unit exceeding the setting range after conversion can be rounded to a specified range by clamping. Note that clamping is not performed for writing.

The following table shows the clamping types that can be specified for an OPC UA server module.

Clamping type	Description
None	No clamping.
Engineering Unit	The minimum value and the maximum value of the engineering unit are set as the clamp values.
Details	A specified minimum value and maximum value are set as clamp values.

1.2　Other Functions

Self-diagnostics function

This function performs the self-diagnostic test to check the hardware of an OPC UA server module.

The following tests are included in the self-diagnostics.

- ☞ Page 95 Automatic hardware test
- ☞ Page 96 Hardware test for LED check

SD memory card format function

This function formats an SD memory card.

After formatting, the volume label will be RD81OPC96.

The operating status of an OPC UA server module will be in "STOP" state after formatting.

For the formatting method, refer to the following:

☞ Page 83 SD memory card diagnostic

Firmware update function

This function acquires a firmware update file from the Mitsubishi Electric FA website to update the firmware version.

For the module models that support this function, precautions that are common to those modules, and update procedure, refer to the following:

📖 MELSEC iQ-R Module Configuration Manual

Restriction

Before using the firmware update function, check the firmware version of an OPC UA server module.
(☞ Page 169 Added and Changed Functions)

Considerations

The following shows the considerations for an OPC UA server module when using the firmware update function.

■Startup time of an OPC UA server module

The startup time of an OPC UA server module may differ depending on the firmware version, and a firmware update may affect system behavior.

To make a system program run on the startup of an OPC UA server module, configure an interlock using input/output signals.
(☞ Page 113 Input/Output Signals)

Initialization function

This function initializes a firmware update-prohibited password retained in an OPC UA server module.

Operating procedure

1. Select "Module Initialization Setting" in "Basic Settings" ⇨ "Various Operations Settings" ⇨ "Mode Settings" for an OPC UA server module in an engineering tool. (☞ Page 90 Basic Setting)

2. Set the CPU module to the STOP state, and write the parameters.

3. Reset the CPU module.
After it is reset, the initialization function is performed automatically. The LED display for initialization is as follows:

Status		RUN LED status	ERR LED status
Initialization completed	Normal completion	ON	OFF
	Abnormal completion	ON	ON

4. When the initialization is completed normally, return the mode setting changed in step 1 to "Online" and reset the CPU module.

5. When the initialization is completed abnormally, check if measures are taken to reduce noise of the programmable controller system, and perform the initialization again. If it is completed abnormally again, a hardware failure may occur in an OPC UA server module. Please contact your local Mitsubishi Electric sales office or representative.
Do not use an electric screwdriver when removing the module. Loose the module fixing screws completely to remove the module.

Global label-related data update function

This function updates data related to global labels by communicating with a CPU module.

Global labels are assigned to addresses of device memories in a CPU module but the addresses change due to the influence of other global labels, programs, FBs, and CPU parameters. This function checks whether global labels are matched or mismatched at the following timings and updates related data when they are mismatched; therefore, the operation can continue without changing the setting of an OPC UA server.

- Starting an OPC UA server module
- Updating the setting of an OPC UA server module
- Reading/writing data

For details on importing global labels, refer to the following:

☞ Page 63 Global Label and Common Device Comment Import Function

Considerations

■Considerations for specifications

- If the name and data structure are not the same, related data cannot be updated.
- This function does not apply changes in data types of global labels in an import source project (GX Works3 project). If a data type is changed[*1], update data related to global labels (☞ Page 73 Updating data related to global labels) in the configuration tool or import the global labels (☞ Page 65 Importing global labels), then write and update the setting. Otherwise, any of the following operations is applied according to the data size relation, which may cause a problem on the system.

*1 Whether the data type of a global label is changed can be checked in the configuration tool. (☞ Page 74 "Update Data Related to Global Label" screen)

Size relation	When reading tag values from an OPC UA client	When writing tag values from an OPC UA client
CPU module ≥ OPC UA server module	A correct value is read depending on the range of values in a CPU module, but an incorrect value may be read due to a sign bit or data missing in oversized data.	A correct value is written depending on the range of each value, but an unintended value may be written to a CPU module due to a sign bit or not writing oversized data.
CPU module < OPC UA server module	No problems.	Oversized data is written to a CPU module, which may cause unintended behavior of a program.

- If a device is assigned to a structure type global label with a structure type member, the global label-related data update function cannot be used. A global label unavailable error (error code: 1921H) occurs and the Data Access function cannot be used.

  To solve this problem, perform the following:

  - Unselect the checkbox of "Update data related global label from the OPC UA server module" in the "Address Space(Target Device)" screen of the configuration tool.

Ex.

When setting the structure ST_B for the data type of member Struct_B of the structure ST_A in GX Works3

A global label unavailable error (error code: 1921H) occurs because a device is assigned to a member of ST_B.

○: Applicable, ×: Not applicable

Structure A		Structure B		Assigned device	Setting in which a global label unavailable error (error code: 1921H) occurs
Structure	Label name (member name)	Structure	Label name (member name)		
ST_A	LabelA_1	—	—	D10	×
	LabelA_2	—	—	None	×
	Struct_B	ST_B	LabelA_1	D100	○
			LabelA_2	None	×

■Considerations for operations

- If an address with a global label assigned changes while updating related data, the update fails and a related data updating failure (event code: 24003) is registered. In this case, a related data updating start (event code: 24000) and related data updating failure (event code: 24003) are not registered until either of the following operations is performed:

  The related data is successfully updated and a related data updating finish (event code: 24001) is registered.

  The setting of an OPC UA server module is updated.

- While updating related data, the following operations are applied:

  Data is not read from/written to the CPU module.

  When an OPC UA client requests to read a tag value in the address space, a retained cache value is returned.

  When an OPC UA client requests to write a tag value in the address space, "BadCommunication" is returned.

- If data related to global labels are mismatched between a CPU module and OPC UA server module, the operation of the OPC UA server module differs depending on whether this function is enabled or disabled.

This function	Device-unassigned global label	Operation
Enabled	Included/not included	• It takes longer to start an OPC UA server module and update the setting.
Disabled	Included	• For device-unassigned global labels: Data cannot be read/written. • For device-assigned global labels: Data reading/writing continues for a related tag and structure label. • A global label mismatch error (error code: 1920H) occurs.[1]
	Not included	• Data reading/writing continues.[2] • No error occurs.[2][3]

[1] It can be cleared by matching a GX Works3 project used for the setting of an OPC UA server module and one written to a CPU module, then writing the setting to the OPC UA server module and updating it.

[2] This case applies when using a project for a configuration tool with version '1.05F' or earlier.

[3] Data is read from/written to a device assigned when importing a global label. Even if there is a mismatch between the global label of a CPU module and the device, no error occurs. Update data related to the global label in the configuration tool as necessary, and check if the device is updated. (☞ Page 73 Updating data related to global labels)

Point

When not updating data related to global labels in the configuration tool after importing tags with the global labels specified from a CSV file, the operations are the same as those above when starting an OPC UA server module and updating the setting.

■Other considerations

• Unsupported global labels cannot be imported in the configuration tool; therefore, there is no problem unless an address changes while an OPC UA server module is operating. Note that there is a problem if this function starts running by the following procedure:

Step 1: Change a global label being used in an OPC UA server module to an unsupported one in an import source project.

Step 2: Perform the online program change for the unsupported global label.

Unsupported global labels are as follows:

No.	Unsupported global label			Operation	Workaround (○: Available, ×: Not available)	
	Device assignment	Array	Condition			
1	Not assigned	Included	The following data types are used: • Timer • Counter • Retentive timer • Long timer • Long counter • Long retentive timer	A device memory type error (error code: 1806H) occurs.	○	When using any of the data types listed in the left for an array, assign a device. (For the long timer and long retentive timer, only the current values (LTN, LSTN) can be used.)
2	Assigned	Included	The following devices are assigned to bit type arrays: • Long timer (LT) • Long retentive timer (LST)		×	For an array, neither the contacts (LTS, LSTS) nor coils (LTC, LSTC) of a long timer or long retentive timer can be used.
3	Assigned	Included	Bit specification or digit specification is used.		○	Assign another device for which bit specification or digit specification is not used, or unassign a device.
4	Not assigned	Included/not included	The following class is used: • VAR_GLOBAL_CONSTANT	A global label unavailable error (error code: 1921H) occurs.	○	Perform the following operations to replace the class. • Change the class to one other than 'VAR_GLOBAL_CONSTANT.' • Set the initial value.

• When using a device-unassigned global label, an error (error code: 1904H) detected in a CPU module may occur.

Error occurrence condition	Corrective action	Workaround
The timing when a target CPU module switches from STOP to RUN overlaps with the following processing: • Data reading by polling • Data writing from an OPC UA client	Turn 'Error clear request' (Y10) ON. (If the error occurrence condition does not apply, refer to the user's manual for the CPU module to check the source error code (4031H).)	Stop an OPC UA server module before switching the CPU module from STOP to RUN, then restart it. ■Stopping method • Turn 'OPC UA server pause request' (Y2) ON. • Stop the OPC UA server module in the configuration tool. (☞ Page 81 Stop of an OPC UA server module) ■Restarting method • Turn 'OPC UA server resume request' (Y1) ON. • Restart the OPC UA server module in the configuration tool. (☞ Page 81 Restart of an OPC UA server module)

Setting method

The configuration tool can be used to enable or disable this function. (☞ Page 32 Access target device)

■Cases in which enabling this function is recommended

No.	Condition	Description
1	The online program change is performed.	Even if an address with a global label assigned changes due to the online program change, the operation can continue without changing the setting of an OPC UA server module.
2	The following settings for a CPU module are changed frequently. • Other global labels • Program • FB • CPU parameter	Even if an address with a global label assigned changes due to the setting change of a CPU module, the operation can start without changing the setting of an OPC UA server module.

■Cases in which disabling this function is recommended

No.	Condition	Description
1	Devices are assigned to all global labels.	When an address with a global label assigned changes, the processing time for updating related data can be avoided each time data is read from/written to the address. However, when changing an assigned device, it is required to enable this function, or specify a GX Works3 project after the change and update data related to the global label in the configuration tool, then write it to an OPC UA server module and update the setting.
2	A CPU module is reset or the power is turned OFF and ON repeatedly, such as during debugging.	When an address with a global label assigned changes, the processing time for updating related data can be avoided each time an OPC UA server module is started and a setting is updated. However, it is required to specify a GX Works3 project after the change and update data related to the global label in the configuration tool, then write it to an OPC UA server module and update the setting.

Checking methods for the operating status

The operating status can be checked with an event or in the buffer memory.

Item	Checking method	Reference
Related data updating start/finish	Event (system monitor of an engineering tool ⇨ [Event History])	Page 111 Event Code List 📖 GX Works3 Operating Manual
Related data being updated	Buffer memory	Page 126 Label update information (Un\G8609 to 8624)

2 MX OPC UA Module Configurator-R

This chapter explains MX OPC UA Module Configurator-R.

2.1 MX OPC UA Module Configurator-R

MX OPC UA Module Configurator-R (tag mode) is a tool for setting tags or groups (Nodes) published to an AddressSpace.
Tags or groups can be created, and data used for tags can be set.

For details on the startup method and screen configuration of MX OPC UA Module Configurator-R, refer to the following:

MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

For using the information model mode, refer to the following:

MELSEC iQ-R OPC UA Server Module User's Manual (Information Model)

2.2 Project File Handling

This section describes the details on handling project files.

Project file compatibility

The following combinations are not compatible. When reading a project file from an OPC UA server module, start the configuration tool in a mode supporting the project.
 • Project file in the tag mode and the configuration tool in the information model mode
 • Project file in the information model mode and the configuration tool in the tag mode

Creating a new project

Create a new project.
The project being edited is discarded.

Operating procedure

Select [File] ⇨ [New].

Opening a project

Read a saved project.

Operating procedure

1. Select [File] ⇨ [Open Project].

2. Select a target file in the "Open" screen, and click the [Open] button.

Saving a project

Save a setting being edited to a project file.

Saving a project

Operating procedure

Select [File] ⇨ [Save].

Naming and saving a project

Operating procedure

1. Select [File] ⇨ [Save as].

2. Specify a save location and file name in the "Save as" screen, then click the [Save] button.

Opening a recently opened project file

Select a recently opened project file to open.

Operating procedure

Select [File] ⇨ [(recently opened project)].

Importing a CSV file

Any setting can be applied to a project being edited by selecting it from a CSV file edited in an application such as spreadsheet software.

For the CSV file format, refer to the following:

☞ Page 139 CSV File Format

Considerations

For a new project file created in the configuration tool, the default polling definition and user settings are configured. When importing a CSV file without changing these settings, they remain configured after the import. To delete these default settings and apply the contents of the CSV file, import the file by the following procedure.

In addition, the configuration tool starts in a state for creating a new project file; therefore, the same applies when importing a CSV file immediately after the start.

Operating procedure

1. Select [File] ⇨ [Close].

2. Select [File] ⇨ [Import] ⇨ [CSV File].

3. Select all settings in the "Import from CSV Files" screen, and click the [Import] button.

Supplementary information

The operations for non-existent CSV files in the operations above are as follows:

Non-existent CSV file	Operation
ADDRESS_SPACE.CSV	Not to be imported.
STRUCTURE.CSV	Not to be imported.
TARGET_DEVICE.CSV	Not to be imported.
CONVERSION.CSV	Not to be imported.
POLLING.CSV	The default polling definition is added.[1][2]
SECURITY.CSV	The same default value as when creating a new project file is set.
USER_SETTING.CSV	The default user is added.[3][4]
NETWORK.CSV	The same default value as when creating a new project file is set.
OPCUA_SERVER.CSV	The same default value as when creating a new project file is set.

[1] The default settings are as follows:
Name: 1000 ms
Use as default Polling Rate: Enabled
Rate: 1000 ms

[2] Applicable when a POLLING.CSV file exists but is not selected as an import target.

[3] The default settings are as follows:
User Name: RD81OPC96
Password: MITSUBISHI
Accessibility from the configuration tool: Enabled (accessible)
Accessibility from an OPC UA client: Enabled (accessible)

[4] Applicable when a USER_SETTING.CSV file exists but is not selected as an import target, or it cannot be selected as an import target because the password is blank.

Import procedure

Operating procedure

1. Select [File] ⇨ [Import] ⇨ [CSV File].

2. Specify the folder in which a CSV file to be imported is stored in the "Browse For Folder" screen, and click the [OK] button.

3. Select the checkbox of a setting to be imported in the area of "Import source."

4. Click the [Import] button.
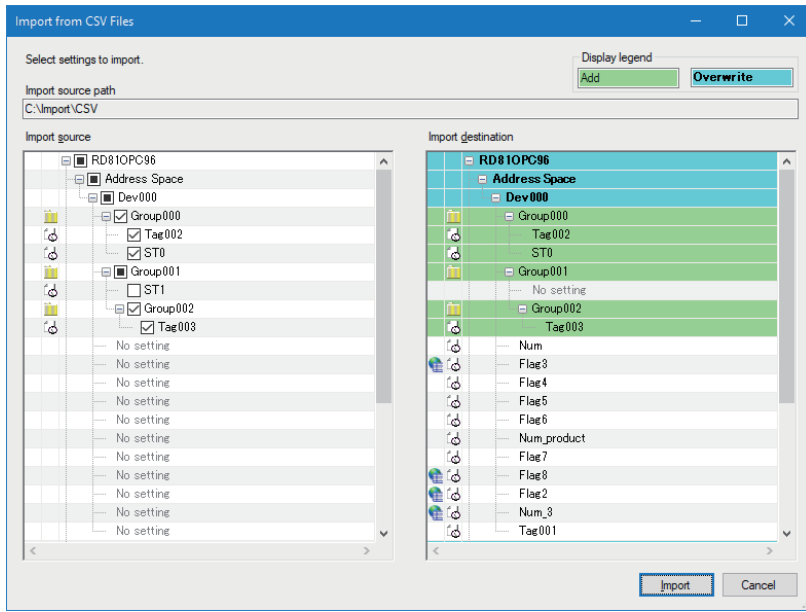
Point

The icon (🌐) indicating that it is related data appears for the following:

Tags with global label-related data specification (LABEL_RELATION) set

Structure labels including structure label members with global label-related data specification (LABEL_RELATION) set

Restriction

- Groups, tags, and structure labels in the ninth hierarchy and later are not displayed.
- Groups in the eighth hierarchy and later cannot be imported.
- Tags and structure labels in the ninth hierarchy and later cannot be imported.
- TIME type structure labels with the byte order swap set are not supported. If imported, a warning log is output.
- When importing a structure label with a structure array as a member, the setting values for "Access Rights," "Swap Word/Byte Order," "Convert to word," and "Conversion" of the first element (member under _0) of the array also apply to other elements.
- When importing a tag to which a global label with a timer, long timer, counter, long counter, retentive timer, or long retentive timer type is related, be sure to update data related to the global label before writing a project to a module after the import. Otherwise, a global label unavailable error (error code: 1921H) occurs in the module.

5. Update data related to global labels as necessary. (☞ Page 73 Updating data related to global labels)

Considerations on import

■For importing a setting with the parent-child relationship or reference relationship

When selecting the checkbox of a setting with the parent-child relationship or reference relationship in the import source area, the checkboxes of settings related to the setting are also selected. To exclude them from the import target, unselect their checkboxes manually. Note that the checkboxes of access target devices and groups cannot be selected individually. The methods for importing them individually are as follows.

Access target device

Perform either of the following operations:

- Exclude 'ADDRESS_SPACE.CSV' from the import source folder before import.
- Import an access target device with selecting the checkbox of at least one item under the access target device, then delete unnecessary items after the import.

Group

Import a group with selecting the checkbox of at least one item under the group, then delete unnecessary items after the import.

■If there is any setting item with the same name in an import destination

If the name of a setting item to be imported is the same as one in an import destination, the setting in the import destination is overwritten.

Exporting a CSV file

Output a project being edited in a CSV file format.

For the CSV file format, refer to the following:

☞ Page 139 CSV File Format

Export procedure

Operating procedure

1. Select [File] ⇨ [Export] ⇨ [CSV File].

2. Specify an export destination in the "Browse For Folder" screen, and click the [OK] button.

Restriction🖐

- TIME type structure labels with the byte order swap set are not supported. If exported, the byte order swap setting is disabled.
- For a structure label with a structure array as a member, only the first element (member under _0) of the array is exported.

2.3 Address Space Setting

Access target device

The following shows the screen for setting an access target device accessed by an OPC UA server module.

Window

■When adding a new item

1. Select "Address Space" in the tree view.

2. Select [Edit] ⇨ [New Target Device].

■When editing an item

Double-click an item (▥) under "Address Space" in the tree view.

Displayed items

Item	Description
Name	Set the name of an access target device (up to 256 characters).
Description	Set the description for an access target device (up to 128 characters).
[Communication Setting] button	Click this to open the "Communication Setting" screen. ☞ Page 33 Communication setting
Enable	Select the checkbox to enable the connection to an access target device.
Server I/F	The setting of a communication route is displayed.
Module Name	The setting of the module type of an access source system is displayed.
Use the global label/common device comment	Select the checkbox to use the global label and common device comment import function. ☞ Page 63 Global Label and Common Device Comment Import Function
Global Label/Common Device Comment Import Source Setting	The path of an engineering tool project specified as an import source is displayed. Specify an import source project in the "Select the Global Label/Common Device Comment Import Source Project" screen displayed by clicking the [...] button.
Update data related global label from the OPC UA server module	Select the checkbox to enable the global label-related data update function. ☞ Page 23 Global label-related data update function
Last Change Date of Global Label	The last update date and time of an import source project used when importing a global label is displayed.

Communication setting

The following shows the screen for setting a connection route to access a device from an OPC UA server module.

Window

Click the [Communication Setting] button in the "Address Space(Target Device)" screen.

Displayed items

Item		Description
Other Station Specification		Select "Own Station" when accessing a device on the system on which an OPC UA server module is mounted. Select "Other Station" when accessing a device connected via a network.
Host System Setting	Module Type	Select the type of a module on the access source system side.
	Station No.	Set the station number of a module on the access source system side (0 to 120).
	Start I/O No.	Set the start I/O number of a module on the access source system side (0 to FE0[*1]).
	Time Out	Set a communication timeout time.
Target (Relay Station) System Setting	IP Address[*2]	Set the IP address of a module on the access target (relay station) system side.
	Network No.[*3]	Set the network number of a module on the access target (relay station) system side (1 to 239).
	Station No.[*4]	Set the station number[*5] of a module on the access target (relay station) system side.
	Other Network Specification	Select "Via Other System" when accessing another network via a system set in the access target (relay station) system side setting.
	Module Type[*6][*7]	Select the type of a module on the routed system side.
	Start I/O No.[*8]	Set the start I/O number of a module on the routed system side (0 to FE0[*1]).
Target (Target Station) System Setting	CPU Series	Select the series of an access target CPU module.
	Multi CPU	Select the CPU number when an access target CPU is in a multiple CPU system.
	Network No.[*9]	Set the network number of a module on the access target (target station) system side (1 to 239).
	Station No.	Set the station number[*10] of a module on the access target (target station) system side.

*1 In hexadecimal and 10-point units

*2 Can be set when selecting either of the following items for "Module Type" in "Host System Setting."
- Built-in Ethernet Port [CH2](Connect to the Ethernet module)
- Built-in Ethernet Port [CH2](Connect to the CPU module (Ethernet port))

*3 Can be set when selecting any of the following items for "Module Type" in "Host System Setting."
- Built-in Ethernet Port [CH2](Connect to the Ethernet module)
- Ethernet Module
- CC-Link IE Control Module
- CC-Link IE Field Module

*4 Can be set when selecting any of the following items for "Module Type" in "Host System Setting."
- Built-in Ethernet Port [CH2](Connect to the Ethernet module)
- Ethernet Module
- CC-Link IE Control Module
- CC-Link IE Field Module
- CC-Link Module

*5 When selecting "CC-Link Module" for "Module Type" in "Host System Setting": 0 to 63
When selecting an item other than "CC-Link Module" for "Module Type" in "Host System Setting": 0 to 120

*6   Can be set when selecting "Via Other System" for "Other Network Specification."
*7   The following items can be selected according to an item selected for "Module Type" in "Host System Setting."
        - "Built-in Ethernet Port [CH2](Connect to the Ethernet module)" is selected: Ethernet/CC-Link IE Control/CC-Link IE Field
        - "Built-in Ethernet Port [CH2](Connect to the CPU module (Ethernet port))" or "CC-Link Module" is selected: Ethernet Module, CC-Link
        IE Control Module, or CC-Link IE Field Module
        - "Ethernet Module," "CC-Link IE Control Module," or "CC-Link IE Field Module" is selected: CC-Link Module
*8   Can be set when selecting any of the following items for "Module Type" in "Host System Setting" and "Via Other System" for "Other
        Network Specification."
        - Ethernet Module
        - CC-Link IE Control Module
        - CC-Link IE Field Module
*9   Can be set when selecting any of the following items for "Module Type" in "Target (Relay Station) System Setting."
        - Ethernet/CC-Link IE Control/CC-Link IE Field
        - Ethernet Module
        - CC-Link IE Control Module
        - CC-Link IE Field Module
*10 When selecting "CC-Link Module" for "Module Type" in "Target (Relay Station) System Setting": 0 to 63
        When selecting an item other than "CC-Link Module" for "Module Type" in "Target (Relay Station) System Setting": 0 to 120

Tag

The following shows the screen for setting a tag accessed by an OPC UA server module.
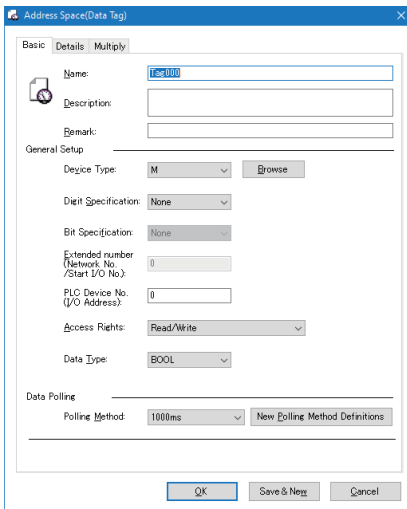
Window

■When adding a new item

1. Select an item (▥ or ▣) under "Address Space" in the tree view.

2. Select [Edit] ⇨ [New Data Tag].

■When editing an item

1. Select an item (▥ or ▣) under "Address Space" in the tree view.

2. Double-click an item (▣) in the list view.

[Basic] tab

Displayed items

Item		Description
Name[*1]		Set the name of a tag (up to 256 characters).
Description		Set the description for a tag (up to 128 characters).
Remark		Set the remark for a tag (up to 128 characters).
General Setup	—	For a tag with a global label imported or one with global label-related data specification (LABEL_RELATION) set which is imported from a CSV file, the icon (🗐) indicating that it is related data appears.
	Device Type[*1]	Select a device type. It can also be selected in the "Support Devices" screen displayed by clicking the [Browse] button. If no device is assigned, "Not Assigned" is displayed.
	Digit Specification[*1*2]	Select a digit to specify for digit specification of a device. (For digit specification, a device is treated as a word device.) For devices that can be digit-specified, refer to the following: 📖 MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
	Bit Specification[*1*2]	Select a bit to specify for bit specification of a device. (For bit specification, a device is treated as a bit device.) For devices that can be bit-specified, refer to the following: 📖 MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
	Extended number (Network No./ Start I/O No.)[*1*2]	Set the extended number (n) of the following devices: • Link direct device (Jn\X, Jn\Y, Jn\B, Jn\SB, Jn\W, Jn\SW)[*3] • Module access device (Un\G, U3En\G)[*4] • CPU buffer memory (U3En\G, U3En\HG)[*4]
	PLC Device No. (I/O Address)[*1*2]	Set the I/O address of an access target.
	Access Rights	Select an access right.
	Data Type[*1*2]	Select a data type. (Only data types that can be set are displayed. (☞ Page 37 Setting availability of data types for each device)) When an extended data type is set in the [Details] tab, the data type corresponding to the setting is displayed.
Data Polling	Polling Method	Select a polling method.
	[New Polling Method Definitions] button	Click this to open the "Polling Method Definitions" screen. ☞ Page 52 Polling Definition Setting
[Save & New] button		Click this to save the setting and display a new tag. • A sequential number is added to the name of a new tag. (Tag→Tag1→Tag2)[*5] • When the last character of a tag name is a number, it is incremented. (Tag000→Tag001→Tag002)[*5] • A number displayed in the field of "PLC Device No. (I/O Address)" is incremented. (M0→M1→M2)

*1 Cannot be edited for related data.
*2 Cannot be edited when "Not Assigned" is displayed for "Device Type."
*3 'n' indicates the network number.
*4 'n' indicates the start I/O number.
*5 When a number to be added already exists, the number is skipped and the next available number is added.

■Setting availability of data types for each device

○: Available, ×: Not available

Data type (extended data type)	Bit device	Digit-specified bit device	Word device	Bit-specified word device	Double-word device
BOOL	○	×	×	○	×
INT	×	○ (K1 to K4)	○	×	×
UINT	×	○ (K1 to K4)	○	×	×
DINT	×	○ (K5 to K8)	○	×	○
UDINT	×	○ (K5 to K8)	○	×	○
TIME	×	○ (K5 to K8)	○	×	○
REAL	×	×	○	×	○
LREAL	×	×	○	×	○
Not Assigned[1]	○[2]	○[2]	○[2]	○[2]	○[2]
(Array of BOOL)	○[3]	×	×	×	×
(Array of INT)	×	×	○	×	×
(Array of UINT)	×	×	○	×	×
(Array of DINT)	×	×	○	×	○
(Array of UDINT)	×	×	○	×	○
(Array of TIME)	×	×	○	×	○
(Array of REAL)	×	×	○	×	○
(Array of LREAL)	×	×	○	×	○
(STRING)	×	×	○	×	×
(WSTRING)	×	×	○	×	×

*1 A project including a setting with the data type of Not Assigned can be used for an OPC UA server module with firmware version '09' or later. If the data type is Not Assigned, it is treated as an invalid tag in the module.

*2 When importing a CSV file in which the data type (DATA_TYPE) is blank, Not Assigned is applied.
If changing the data type from Not Assigned to another one and fixing the tag setting, it cannot be returned to Not Assigned.

*3 × for LTS, LTC, LSTS, and LSTC

[Details] tab

Displayed items

Item		Description
General Setup	Enable Tag	Select the checkbox to enable the tag.
Data Conversion	Swap Word/Byte Order[*1]	Select the checkbox to swap the order of bytes in data. The data type of a device is WORD type: B1/B2 ↔ B2/B1 The data type of a device is LONGWORD type: B1/B2 B3/B4 ↔ B4/B3 B2/B1
	Convert to word[*1][*2]	Select the checkbox to convert a tag value to the word size or double-word size when reading data from or writing data to an OPC UA client is requested. ■INT type tag • Reading: Data is converted to the double-word size and read from an OPC UA client. (A sign is considered.) • Writing: Data is converted to the word size and written to a tag. ■DINT type tag • Reading: Data is converted to the word size and read from an OPC UA client. • Writing: Data is converted to the double-word size and written to a tag. (A sign is considered.)
	Use Conversion[*3]	Select the checkbox to use a conversion definition.
	Conversion	Select a conversion definition.
	[New Conversion Definitions] button	Click this to open the "Conversion Definitions" screen. ☞ Page 50 Conversion Definition Setting
Extended Data Type	Use Advanced Type[*4]	Select the checkbox to use an extended type (array, character string).
	Extended Data Type	Select an extended data type. (Only extended data types that can be set are displayed. (☞ Page 37 Setting availability of data types for each device))
	Number of elements[*5]	Set the number of elements in each dimension of an array.[*6]
	Length[*5]	Set the number of characters in a character string.[*7]
[Save & New] button		Click this to save the setting and display the screen for setting a new tag. • A sequential number is added to the name of a new tag. (Tag→Tag1→Tag2)[*8] • When the last character of a tag name is a number, it is incremented. (Tag000→Tag001→Tag002)[*8] • A number displayed in the field of "PLC Device No. (I/O Address)" is incremented. (M0→M1→M2)

*1　Setting availability differs depending on a selected data type (extended data type). (☞ Page 39 Setting availability of data types (extended data types))
*2　Cannot be set when selecting the checkbox of "Use Conversion."
*3　Cannot be set when selecting "STRING" or "WSTRING" for the extended data type.
*4　Cannot be edited in the following cases:
　　- Related data
　　- "Not Assigned" is displayed for "Device Type" in the [Basic] tab.
　　- There is no extended data type that can be set. (☞ Page 37 Setting availability of data types for each device)
*5　The display item switches according to a selected extended data type.
　　"STRING" or "WSTRING": Length
　　Others: Number of elements
*6　For the upper limit value (maximum number of array elements), refer to the following:
　　📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
*7　For the upper limit value (maximum number of characters), refer to the following:
　　📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
*8　When a number to be added already exists, the number is skipped and the next available number is added.

■Setting availability of data types (extended data types)

○: Available, ×: Not available

Data type (extended data type)	Byte order swap	Conversion to the word size
BOOL	×	×
INT	○	○
UINT	○	○
DINT	○	○
UDINT	○	○
TIME	×	×
REAL	○	×
LREAL	○	×
Not Assigned	×	×
(Array of BOOL)	×	×
(Array of INT)	○	○
(Array of UINT)	○	○
(Array of DINT)	○	○
(Array of UDINT)	○	○
(Array of TIME)	×	×
(Array of REAL)	○	×
(Array of LREAL)	○	×
(STRING)	○	×
(WSTRING)	○	×

■Examples

Ex.

The following shows examples for swapping the order of bytes.

```
<WORD>                                          <LONGWORD>
(1) 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0            (1) 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0
     \___B1___/ \___B2___/                          \__B1__/ \__B2__/ \__B3__/ \__B4__/
            ⇩                                                      ⇩
(2) 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1            (2) 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1
     \___B2___/ \___B1___/                          \__B4__/ \__B3__/ \__B2__/ \__B1__/
```

(1) Tag value

(2) Value in an OPC UA client

Ex.

The following shows examples for converting an INT type tag to the word size.

Reading

```
(1)                         1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
                    (3)              ⇩
(2) 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1
```

(1) Tag value

(2) Value in an OPC UA client

(3) Sign (considered)

Writing

```
(1)                         0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0
                    (3)              ⇧
(2) 1 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0
```

(1) Tag value

(2) Value in an OPC UA client

(3) Sign (not considered)

[Multiply] tab

Displayed items

Item	Description
Multiply when saving	Select the checkbox to duplicate a tag when saving.
Start No.	Set the start number of a number added to a tag name when duplicating.
Numeric Places	Set the number of digits in the numeric part of a tag name.
Number of items	Set the number of tags to duplicate.
Name	Enter the base of a tag name.
[Multiply] button	Click this to duplicate a tag while keeping the set contents.
[Save & New] button	Click this to save the setting and display the screen for setting a new tag. • A sequential number is added to the name of a new tag. (Tag→Tag1→Tag2)[*1] • When the last character of a tag name is a number, it is incremented. (Tag000→Tag001→Tag002)[*1] • A number displayed in the field of "PLC Device No. (I/O Address)" is incremented. (M0→M1→M2)

*1   When a number to be added already exists, the number is skipped and the next available number is added.

Ex.

The following shows a setting example and tags duplicated based on the setting.

• Tag setting

[Basic] tab	[Multiply] tab

• Duplicated tags

Structure label

The following shows the procedures for setting a structure label in the address space.

The data structure of a structure set in the following section can be created in the address space.

☞ Page 53 Structure Definition Setting

Operating procedure

■When adding a new item

1. Select an item (▥ or ▣) under "Address Space" in the tree view.

2. Select [Edit] ⇨ [New Structure Type Declarations].

3. Set each item in the "Structure Label Definitions" screen. (☞ Page 43 Label, Page 44 Address, Page 47 Tag)

■When editing an item

1. Select an item (▥ or ▣) under "Address Space" in the tree view.

2. Select an item (▤) in the list view, then select [Edit] ⇨ [Properties].

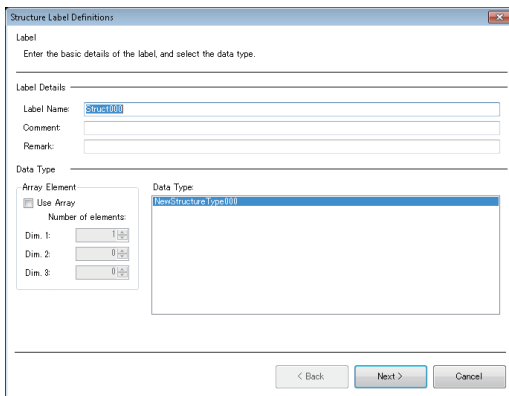*3.* Set each item in the "Structure Label Definitions" screen. (☞ Page 43 Label, Page 44 Address, Page 47 Tag)

> **Point** 🔎
>
> A structure array is displayed with the following icon.
>
> ▣

Label

The following shows the screen for setting the name and data type of a structure label.

Window

Displayed items

Item			Description
Label Details	Label Name[*1]		Set the name of a structure label (1 to 256 characters).[*2]
	Comment		Set a comment (up to 128 characters).
	Remark		Set a remark (up to 128 characters).
Data Type	Array Element	Use Array[*1]	Select the checkbox to use a structure as an array.
		Number of elements[*3]	Set the number of elements in each dimension of an array (1 to 5120).[*4][*5]
	Data Type		Select a structure to use for the data type of a structure label. ☞ Page 53 Structure Definition Setting
[Next] button			Click this to move to the next screen. ☞ Page 44 Address

*1 Cannot be edited for related data.
*2 Up to 800 characters in total can be set for a structure label name and member name (including a member of a structure).
*3 Can be set when selecting the checkbox of "Use Array."
*4 When 1 or more is set for "Dim. 1," a value can be set for "Dim. 2."
*5 When 1 or more is set for "Dim. 2," a value can be set for "Dim. 3."

Precautions

When returning to this screen after setting an address or tag in their respective screens, and selecting another structure for "Data Type" then clicking the [Next] button, their settings are initialized.
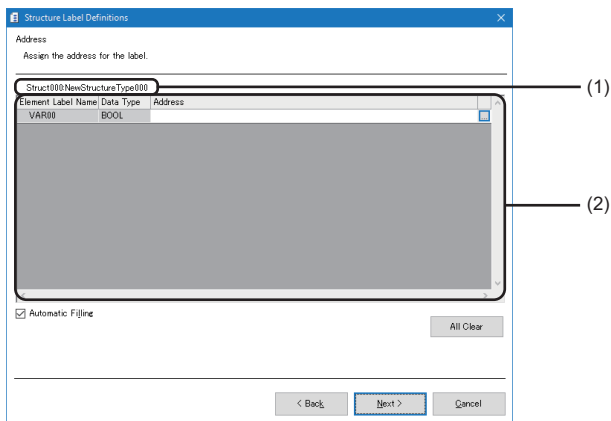
Address

The following shows the screen for assigning an address to each member of a structure.

■When the checkbox of "Use Array" is not selected in the screen for setting a label

Window

Click the [Next] button in the screen for setting labels.

Displayed items

Item		Description
(1) Name		A structure label name and structure name are displayed. For a tag with a global label imported or one with global label-related data specification (LABEL_RELATION) set which is imported from a CSV file, the icon ( ) indicating that it is related data appears.
(2) Member list	Element Label Name	The name of a member of the structure is displayed.
	Data Type	The data type of a member of the structure is displayed.
	Address[*1]	Set an address to assign to a member of the structure (bit specification: available, digit specification: not available).[*2] It can also be set in the "Address Setting" screen displayed by clicking the [...] button. ☞ Page 46 Address setting When selecting the checkbox of "Automatic Filling," addresses are automatically assigned to the subsequent members[*3] of a member for which an address is set.[*4*5*6*7]
Automatic Filling[*1]		Select the checkbox to automatically assign an address[*8].
[All Clear] button[*9]		Click this to delete addresses in a batch.
[Back] button		Click this to move to the previous screen. ☞ Page 43 Label
[Next] button		Click this to move to the next screen. ☞ Page 47 Tag

*1 Cannot be edited for related data.
*2 Displayed in red if an invalid address is set.
*3 Excluding members for which addresses are already set. To automatically assign an address, delete the address set for a target member.
*4 Assigned without duplication.
*5 Assigned to a member the data type of which is BOOL when a bit device is set for an address.
*6 Assigned to a member the data type of which is not BOOL when a device other than a bit device is set for an address.
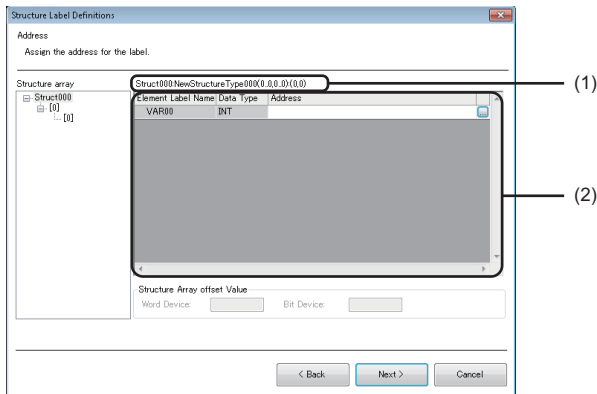*7 Assigned according to the size of a data type.
*8 Performed when a valid address is set for any member of a structure. (If the address already set for a member is changed, it is performed when a valid address different from one before the change is set.)
*9 Cannot be clicked for related data.

■When the checkbox of "Use Array" is selected in the screen for setting a label

Window

Click the [Next] button in the screen for setting labels.

Displayed items

Item		Description
Structure array		Array elements of a structure array are displayed in a tree.
(1) Name		A structure label name and structure name are displayed. For a tag with a global label imported or one with global label-related data specification (LABEL_RELATION) set which is imported from a CSV file, the icon (🖳) indicating that it is related data appears.
(2) Member list	Element Label Name	The name of a member of the structure is displayed.
	Data Type	The data type of a member of the structure is displayed.
	Address*1	Set an address to assign to a member of the structure (bit specification: available, digit specification: not available).*2*3 It can also be set in the "Address Setting" screen displayed by clicking the [...] button. ☞ Page 46 Address setting
Structure Array offset Value*1		Set an offset value*4 of a structure array. Regardless of the size of the structure, a round number can be set for the start address of each array element. • Word Device: Set an offset value for a member of a word device. • Bit Device: Set it as an offset value for a member of a bit device.
[Back] button		Click this to move to the previous screen. ☞ Page 43 Label
[Next] button		Click this to move to the next screen. ☞ Page 47 Tag

*1 Cannot be edited for related data.
*2 Displayed in red if an invalid address is set.
*3 An address can be set only for the following members:
   - The first member among members the data type of which is BOOL
   - The first member among members the data type of which is not BOOL
*4 Can be set up to 99999.

Ex.

The following table shows examples of addresses if setting an offset value when using the structure array shown below.

Start device: D0, structure size: 13, number of elements: 3

Array element	Address of an array element	
	If an offset value is not set	If an offset value is set to 100
1	D0 to D12	D0 to D12
2	D13 to D25	D100 to D112
3	D26 to D38	D200 to D212

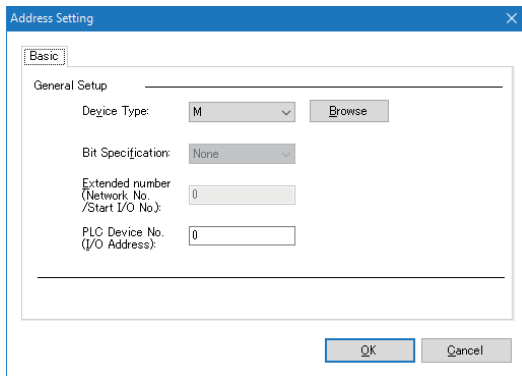### Precautions

Addresses overlap among array elements. Do not set an offset value smaller than the structure size.

■Address setting

Set an address to assign to each member of a structure.

Window

Displayed items

Refer to "General Setup" in the "Address Space(Data Tag)" screen.

Note that "Access Rights," "Data Type," or "Digit Specification" are not displayed.
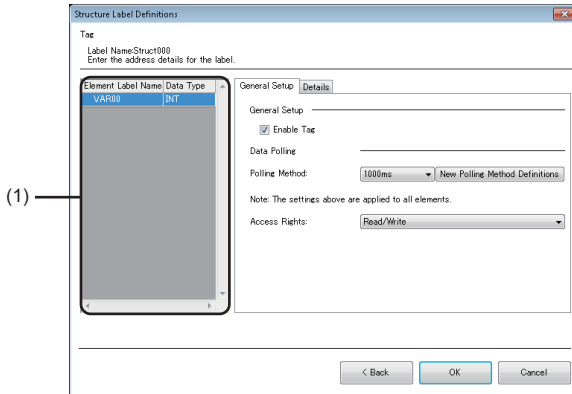
☞ Page 36 [Basic] tab

Tag

The following shows the screen for setting details on each member of a structure.

Window

Click the [Next] button in the screen for setting addresses.

Displayed items

Item		Description
(1) Member list	—	A member of the structure is displayed. The settings of a selected member are displayed on the right side of the screen.
	Element Label Name	The name of a member of the structure is displayed.
	Data Type	The data type of a member of the structure is displayed.
[General Setup] tab	Enable Tag	Select the checkbox to enable the tag. (Applies to all members of the structure.)
	Polling Method	Select a polling definition. (It applies to all members of the structure.)
	[New Polling Method Definitions] button	Click this to open the "Polling Method Definitions" screen. ☞ Page 52 Polling Definition Setting
	Access Rights	Select an access right of a member of the selected structure.
[Details] tab	Swap Word/Byte Order	Select the checkbox to swap the order of bytes in data. The data type of a device is WORD type: B1/B2 ↔ B2/B1 The data type of a device is LONGWORD type: B1/B2 B3/B4 ↔ B4/B3 B2/B1
	Convert to word[*1]	Select the checkbox to convert a tag value to the word size or double-word size when reading data from or writing data to an OPC UA client is requested. ■INT type tag • Reading: Data is converted to the double-word size and read from an OPC UA client. (A sign is considered.) • Writing: Data is converted to the word size and written to a tag. ■DINT type tag • Reading: Data is converted to the word size and read from an OPC UA client. • Writing: Data is converted to the double-word size and written to a tag. (A sign is considered.)
	Use Conversion[*2]	Select the checkbox to use a conversion definition.
	Conversion	Select a conversion definition.
	[New Conversion Definitions] button	Click this to open the "Conversion Definitions" screen. ☞ Page 50 Conversion Definition Setting
[Back] button		Click this to move to the previous screen. ☞ Page 44 Address

*1 Can be set when the data type of a member selected in the member list is INT, UINT, DINT, or UDINT.
*2 Cannot be set when the data type of a member selected in the member list is STRING or WSTRING.

Ex.

The following shows examples for swapping the order of bytes.

<WORD>

(1) `0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0`

      B1   B2

⬇

(2) `1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1`

      B2   B1

<LONGWORD>

(1) `0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0`

    B1   B2   B3   B4

⬇

(2) `1 0 1 0 1 0 1 0 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1 0`

    B4   B3   B2   B1

(1) Tag value

(2) Value in an OPC UA client

Ex.

The following shows examples for converting an INT type tag to the word size.

Reading

(1) `1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1`

⬇

(3)

(2) `1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1`

(1) Tag value

(2) Value in an OPC UA client

(3) Sign (considered)

Writing

(1) `0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0`

(3)

⬆

(2) `1 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0`

(1) Tag value

(2) Value in an OPC UA client

(3) Sign (not considered)

Group

The following shows the screen for setting tags as a group.

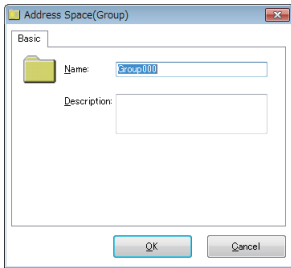A group can also be created as a member of a group.

Window

■When adding a new item

1. Select an item (▥ or 📁) under "Address Space" in the tree view.

2. Select [Edit] ⇨ [New Group].

■When editing an item

Double-click an item (📁) under "Address Space" in the tree view.

Displayed items

Item	Description
Name	Set the name of a group (up to 256 characters).
Description	Set the description for a group (up to 128 characters).

2.4 Conversion Definition Setting

This section shows the screen for setting a definition to convert device values to values in the engineering unit.

For conversion, refer to the following:

☞ Page 19 Conversion function

To apply a conversion definition to a tag, refer to the following:
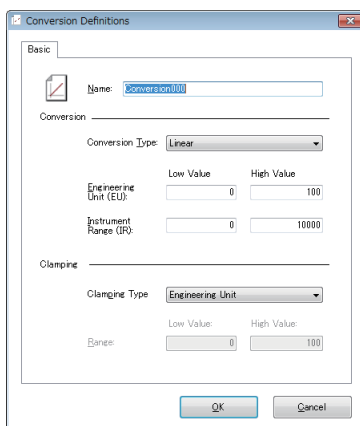
☞ Page 38 [Details] tab

Window

■When adding a new item

1. Select "Conversion Definitions" in the tree view.

2. Select [Edit] ⇨ [New Conversion Definitions].

■When editing an item

1. Select "Conversion Definitions" in the tree view.

2. Double-click an item (📝) in the list view.

Displayed items

Item		Description
Name		Set the name of a conversion definition (up to 50 characters).
Conversion	Conversion Type	Select a conversion type.
	Engineering Unit (EU)[*1]	Set the maximum value and the minimum value of the engineering unit. Setting range: -1.79769313486231E+308 to 1.79769313486231E+308
	Instrument Range (IR)[*1]	Set a device value equivalent to the engineering unit. Setting range: -1.79769313486231E+308 to 1.79769313486231E+308
Clamping	Clamping Type	Select a clamping type.
	Range[*1]	Set the maximum value and the minimum value of clamping. (Range of the Double type) Setting range: -1.79769313486231E+308 to 1.79769313486231E+308

*1 If the number of digits in the mantissa part is set to 16 digits or more, the setting value is converted to an exponent notation when clicking the [OK] button. (The 16th digit of the setting value is rounded off.)
(Example) When setting '1234567890123456,' the value is converted to '1.23456789012346E+15.'

Precautions

Values exceeding the setting range are not treated in conversion operations.

If a device value is not converted according to either of the formulas shown in the following sections, review the setting value.

☞ Page 19 Linear function conversion, Page 20 Quadratic function conversion

Ex.

The following shows the example for each clamp type when converting the device value 3000 according to the following specification.

Conversion type: Linear

Range of the engineering unit (EU): 0 to 400

Range of the device value (IR): 0 to 2000

Clamping Type	Range	Value after conversion
None	—	600
Engineering Unit	0 to 400 (range of the engineering unit (EU))	400
Details	0 to 200	200

2.5 Polling Definition Setting

This section shows the screen for setting a cycle for polling performed by an OPC UA server module to an access target device.

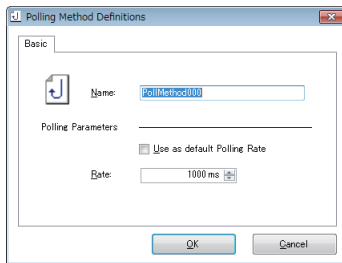To apply a polling definition to a tag, refer to the following:

Window

■When adding a new item

1. Select "Polling Method Definitions" in the tree view.

2. Select [Edit] ⇨ [New Polling Method Definitions].

■When editing an item

1. Select "Polling Method Definitions" in the tree view.

2. Double-click an item (🔁) in the list view.

Displayed items

Item		Description
Name		Set the name of a polling definition (up to 50 characters).
Polling Parameters	Use as default Polling Rate	Select the checkbox to use this setting as the initial setting.
	Rate	Set a polling cycle.

2.6 Structure Definition Setting

This section shows the screen for setting a structure that can be used for the data type of a structure label in the address space.

For structure labels, refer to the following:
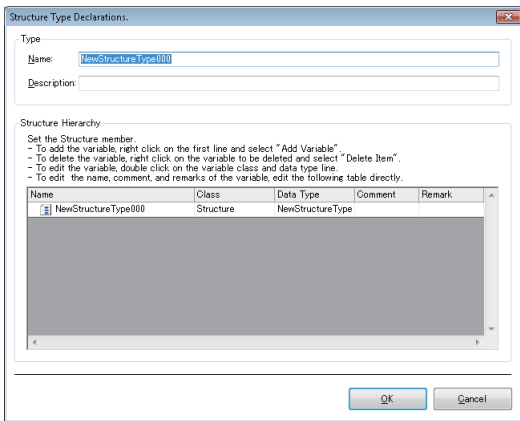☞ Page 42 Structure label

Window

■When adding a new item

1. Select "Structure Type Declarations" in the tree view.

2. Select [Edit] ⇨ [New Structure Type Declarations].

■When editing an item

1. Select "Structure Type Declarations" in the tree view.

2. Select an item (📄) in the list view, then select [Edit] ⇨ [Properties].

Displayed items

Item		Description
Type	Name	Set the name of a structure (1 to 256 characters).[1] When changing this item, the content in "Name" of the structure in the first row in "Structure Hierarchy" is also changed.
	Description	Set the description for a structure (up to 128 characters). When changing this item, the content in "Comment" of the structure in the first row in "Structure Hierarchy" is also changed.
Structure Hierarchy	—	Data structure of a structure is displayed in a tree. A member can be added in the "Add Variable" screen displayed by right-clicking the first row and selecting [Add Variable] from the shortcut menu. ☞ Page 54 Adding a member
	Name	The name of a member of the structure is displayed. Double-click to edit the name (1 to 256 characters).[1]
	Class	The class of a member of the structure is displayed. Double-click to open the "Add Variable" screen and change the class. ☞ Page 54 Adding a member
	Data Type	The data type of a member of the structure is displayed. Double-click to open the "Add Variable" screen and change the data type. ☞ Page 54 Adding a member
	Comment	A comment is displayed. Double-click to edit a comment (up to 128 characters).
	Remark	A remark is displayed. Double-click to edit a remark (up to 128 characters).

*1 Up to 800 characters in total can be set for a structure name and member name (including a member of a structure).

Point

- When changing the contents of "Name" or "Comment" of the structure in the first row, those of "Name" or "Description" in "Type" are also changed.
- When adding a structure array (🖻) to a member, the name of an array element is displayed as follows:

Three-dimensional array: _A_B_C

Two-dimensional array: _A_B

One-dimensional array: _A

A, B, and C indicate an index number of a one-dimensional, two-dimensional, and three-dimensional array, respectively.

Precautions

- The name of a structure used for the data type of a structure label and a structure which is a member of the structure cannot be changed. If the change is needed, unselect the structure used for the data type and select another one.
- Only the members of a structure in the first row can be deleted and edited. If adding another structure to a member, members of the added structure cannot be deleted and edited.
- Array elements of a structure array cannot be deleted and edited.
- When adding another structure to a member of a structure in the first row, a setting that includes a circular reference to a structure cannot be set.

Adding a member

The following shows the screen for adding a member to a structure.

Window
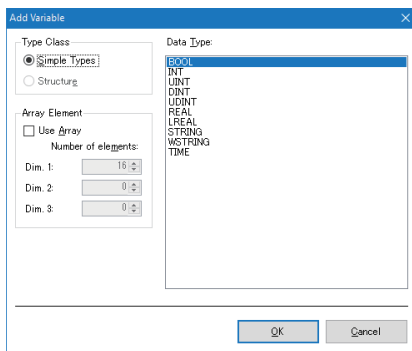
Displayed items

Item		Description
Type Class		Select a type class.
Array Element[*1]	Use Array	Select the checkbox to add a member as an array.
	Number of elements[*2]	Set the number of elements in each dimension of an array.[*3][*4][*5]
String[*1]	Length	Set the length of a character string.[*6]
Data Type		Select a data type.

*1 The display item switches according to a selected type class and data type.
 "Simple Types" is selected for "Type Class" and "STRING" or "WSTRING" for "Data Type": String
 Others: Array Element
*2 Can be set when selecting the checkbox of "Use Array."
*3 For the upper limit value (maximum number of array elements), refer to the following:
 ↵MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
*4 When 1 or more is set for "Dim. 1," a value can be set for "Dim. 2."
*5 When 1 or more is set for "Dim. 2," a value can be set for "Dim. 3."
*6 For the upper limit value (maximum number of characters), refer to the following:
 ↵MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

2.7 Security Setting

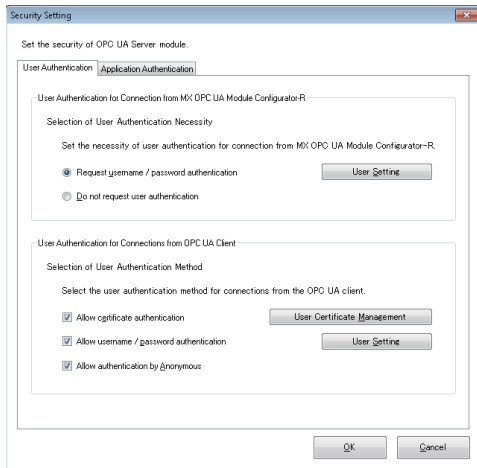This section shows the screen for setting the following authentication to access an OPC UA server module.
 • User authentication for access from the configuration tool or an OPC UA client to an OPC UA server module
 • Application authentication for access from an OPC UA client to an OPC UA server module
For the security setting for an OPC UA server running on an OPC UA server module, refer to the following:
☞ Page 59 OPC UA Server Setting

## Window

Select [Tool] ⇨ [Security Setting].

Displayed items

Item			Description
[User Authentication] tab	User Authentication for Connection from MX OPC UA Module Configurator-R	Request username / password authentication	Select this to perform user authentication with a user name or password when accessing an OPC UA server module from the configuration tool.
		[User Setting] button	Click this to open the "User Setting" screen. ☞ Page 57 User setting
		Do not request user authentication	Select this not to perform user authentication with a user name or password when accessing an OPC UA server module from the configuration tool.
	User Authentication for Connections from OPC UA Client	Allow certificate authentication	Select the checkbox to allow user authentication with a certificate when accessing an OPC UA server module from an OPC UA client.
		[User Certificate Management] button	Click this to open the "Manage User Certificate" screen. ☞ Page 86 User certificate management
		Allow username / password authentication	Select the checkbox to allow user authentication with a user name or password when accessing an OPC UA server module from an OPC UA client.
		[User Setting] button	Click this to open the "User Setting" screen. ☞ Page 57 User setting
		Allow authentication by Anonymous	Select the checkbox to allow Anonymous logon. When allowing Anonymous logon, connections from Anonymous users are allowed.

Item			Description
[Application Authentication] tab	Application Authentication for Connections from OPC UA Clients	Use automatic certificate exchange	Select the checkbox to exchange certificates automatically. When selecting this checkbox, a client certificate is automatically trusted and the connection is allowed. When not selecting this checkbox, store a client certificate in "Trust List" in the "Manage Application Certificate" screen. (☞ Page 84 Application certificate management)
		[Manage Application Certificate] button	Click this to open the "Manage Application Certificate" screen. ☞ Page 84 Application certificate management

Precautions

- Automatically exchanging certificates is not recommended in an open network environment such as the Internet or an intranet, because it allows connections from all OPC UA clients.
- Automatically exchanged certificates are not displayed in the "Manage Application Certificate" screen. (☞ Page 84 Application certificate management)
- Allowing Anonymous logon is not recommended in an open network environment such as the Internet or an intranet, because it allows connections from all users.

User setting

The following shows the screen for setting a user account used for user authentication for accessing an OPC UA server module from the configuration tool and an OPC UA client.

Window
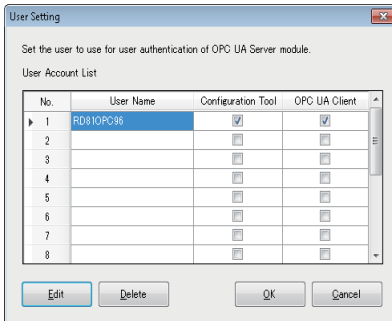
Displayed items

Item		Description
User Account List	User Name	The user name of a user account is displayed.
	Configuration Tool	Whether a user can access an OPC UA server module from the configuration tool is displayed.
	OPC UA Client	Whether a user can access an OPC UA server module from an OPC UA client is displayed.
[Edit] button		Click this to open the "User Account Setting" screen of a selected row. ☞ Page 57 User account setting
[Delete] button		Click this to delete the setting of a selected row.

User account setting

The following shows the procedure for setting details of a user account.

Operating procedure

1. Click the [Edit] button in the "User Setting" screen.

2. Enter a user name and password (up to 32 characters, case-sensitive).

3. Select the checkbox of a target for user authentication.

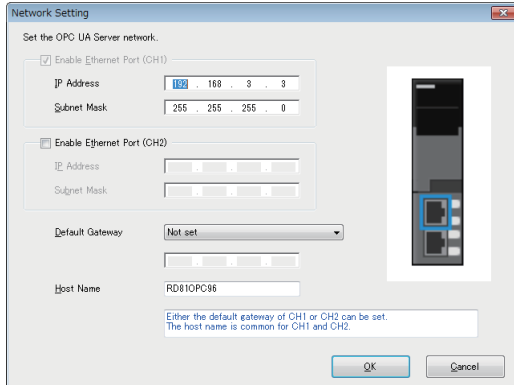*4.* Click the [OK] button.

Point

When only changing a target for user authentication, a new password does not need to be entered.

2.8 Network Setting

This section shows the screen for configuring the setting required for a network connection.

Window

Select [Tool] ⇨ [Network Setting].

Displayed items

Item		Description
Ethernet port (CH1)	Enable Ethernet Port (CH1)	Select the checkbox to use the Ethernet port (CH1).[*1]
	IP Address	Set the IP address (CH1) of an OPC UA server module in decimal.[*2]
	Subnet Mask	Set a subnet mask in decimal when using it.
Ethernet port (CH2)	Enable Ethernet Port (CH2)	Select the checkbox to use the Ethernet port (CH2).
	IP Address	Set the IP address (CH2) of an OPC UA server module in decimal.[*2]
	Subnet Mask	Set a subnet mask in decimal when using it.
Default Gateway		Select the necessity of default gateway, and set an IP address.[*3]
Host Name		Set a host name.

*1 The checkbox status cannot be changed.
*2 A same IP address or an IP address in the same network cannot be set for both CH1 and CH2.
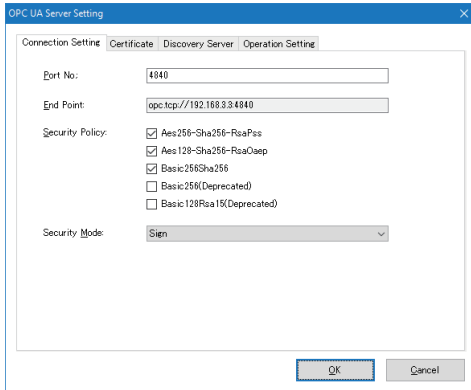*3 Only one of CH1 or CH2 can be registered.
　Communication with the same network as each CH is performed from the corresponding CH only.
　(Even if a default gateway is set for the other CH, communication is not performed from the other one.)

2.9 OPC UA Server Setting

This section shows the screen for configuring the setting for an OPC UA server running on an OPC UA server module.
When connecting from an OPC UA client, use this setting.

Window

Select [Tool] ⇨ [OPC UA Server Setting].

[Connection Setting] tab

Displayed items

Item	Description
Port No.	Set the port number of an OPC UA server (1024 to 65535).
End Point	The endpoint URL of an OPC UA server module is displayed.[*1]
Security Policy	Select the checkbox of a security policy to enable.[*2] When not selecting any checkboxes, None (no security)[*3] is applied. • Aes256-Sha256-RsaPss[*4]: AES 256-bit encryption + SHA-256 (default: selected[*5]) • Aes128-Sha256-RsaOaep[*4]: AES 128-bit encryption + SHA-256 (default: selected[*5]) • Basic256Sha256[*6]: Basic 256-bit encryption + SHA-256 (default: selected[*5]) • Basic256(Deprecated)[*7]: Basic 256-bit encryption (default: unselected) • Basic128Rsa15(Deprecated)[*7]: Basic 128-bit encryption (default: unselected)
Security Mode	Select a security mode.[*8][*9] • None[*10]: No security • Sign[*11]: Data is signed. • Sign & Encrypt[*11]: Data is signed and encrypted.

*1 When changing both the port number and the IP address of the Ethernet port (CH1), the endpoint URL is also changed.
*2 When writing a setting with the default values of the configuration tool with software version '1.08J' or later to an OPC UA server module with firmware version '07' or earlier, a setting file error (error code: 1C10H) occurs. Unselect the checkboxes of "Aes256-Sha256-RsaPss" and "Aes128-Sha256-RsaOaep" then write the setting.
*3 All security policies including "None" are enabled; however, those to be enabled differ for each firmware version of an OPC UA server module. (☞ Page 18 Security policy)
*4 Can be set under the following conditions:
   OPC UA server module: Firmware version '08' or later
   Configuration tool: Software version '1.07H' or later, or "None" is set in software version '1.06G' or earlier
*5 Unselected by default for a configuration tool with software version '1.07H' or earlier.
*6 Can be set under the following conditions:
   OPC UA server module: Firmware version '02' or later
   Configuration tool: Software version '1.01B' or later, or "None" is set in software version '1.00A'
*7 Not recommended in the OPC UA specifications, because it is considered less secure.
   When writing a setting to an OPC UA server module with firmware version '06' or '07,' an OPC UA server operates as if "Basic256Sha256" were selected for the security policy.
*8 All security modes equal to or stronger than the selected one are enabled.
*9 The selection is automatically changed in the following cases:
   When unselecting the checkboxes of all security policies: None
   When selecting any of the checkboxes of security policies while none of them is selected: Sign
*10 Cannot be selected if any of the checkboxes of security policies is selected.
*11 Cannot be selected if none of the checkboxes of security policies is selected.

■Security policy compatibility

The compatibility for a project file and the configuration tool is as follows.

○: Compatible, ×: Not compatible

Software version of the configuration tool when saving a project file	Condition	Software version of the configuration tool when using the project file	
		'1.06G' or earlier	'1.07H' or later
'1.06G' or earlier	—	○	○[*1]
'1.07H' or later	A security policy other than the following is selected: • Aes256-Sha256-RsaPss • Aes128-Sha256-RsaOaep	○[*2]	○
	Either of the following security policies is selected: • Aes256-Sha256-RsaPss • Aes128-Sha256-RsaOaep	×	○

*1 If the project file is saved with a security policy other than "None" selected, the checkboxes of security policies equal to or stronger than the selected one are all selected.
If the project file is saved with "None" selected, no checkboxes are selected.

Selected security policy when saving a project file in software version '1.06G' or earlier (Combo box)	Selected security policy when opening the project file in software version '1.07H' or later (Checkbox)
Basic256Sha256	Basic256Sha256
Basic256	Basic256Sha256 Basic256
Basic128Rsa15	Basic256Sha256 Basic256 Basic128Rsa15
None	No checkboxes selected

*2 When opening the project file, and saving it or writing it to an OPC UA server module, security policies to be enabled for the module differ from those selected in software version '1.07H' or later as shown in the following table. (This also applies when opening the project file again in software version '1.07H' or later.)

Software version '1.07H' or later	Software version '1.06G' or earlier	
Selected security policy when saving a project file (Checkbox)	Selected security policy when opening the project file (Combo box)	Security policy to be enabled for the module
Basic256Sha256 Basic128Rsa15	Basic128Rsa15	Basic256Sha256 Basic256 Basic128Rsa15
Basic256 Basic128Rsa15		
Basic128Rsa15		
Basic256	Basic256	Basic256Sha256 Basic256

Point

When setting a security policy, operations (security policies to be enabled) differ for each firmware version of an OPC UA server module and software version of the configuration tool. For details, refer to the following:

[Certificate] tab

Displayed items

Item	Description
OPC UA Server Name	Set the name of an OPC UA server (1 to 256 characters).
Organization name	Set the name of an organization (1 to 256 characters).
Organization Unit	Set the unit of an organization (1 to 256 characters).
Locality	Set the name of a region (1 to 256 characters).
State	Set a state (1 to 256 characters).
Country	Enter the abbreviation for a country name (2 characters).

For available characters, refer to the following:

☞ Page 129 Available Characters

> **Point**
>
> A certificate (der) is created in the SD memory card inserted in an OPC UA server module with the contents set in the [Certificate] tab.

[Discovery Server] tab

Displayed items

Item	Description
Discovery Server URL	Set the URL of a discovery server (1 to 256 characters). When using a discovery server, an OPC UA client can acquire an endpoint to access each OPC UA server by querying the discovery server.
Registration Interval	Set an interval for registering an endpoint in a discovery server (10000 to 999999).

For available characters, refer to the following:

☞ Page 129 Available Characters

[Operation Setting] tab

Displayed items

Item		Description
Enable Log Output		Select the checkbox to output a communication event log between the configuration tool and an OPC UA server module to an SD memory card. For a log file to be output, refer to the following: ☞ Page 156 Communication event log file
Specify the waiting time for the module operation start	—	Select the checkbox to specify a waiting time until 'Module READY' (X0) turns ON after an OPC UA server module is ready.
	Waiting time	Set a waiting time until 'Module READY' (X0) turns ON.
Reverse the dimensional order of multidimensional arrays		Select the checkbox to change the dimensional order of multidimensional array elements from ascending to descending order.[*1][*2][*3] This setting applies to the following settings: • Multidimensional array tag • Structure label with the data type other than a structure and including multidimensional arrays as structure members

*1 The operation on an OPC UA server module is as follows:

Setting value	Two-dimensional array	Three-dimensional array
Enabled (selected)	Object name [Two dimensions] [One dimension]	Object name [Three dimensions] [Two dimensions] [One dimension]
Disabled (unselected)	Object name [One dimension] [Two dimensions]	Object name [One dimension] [Two dimensions] [Three dimensions]

*2 'Disabled (unselected)' is available for an OPC UA server module with firmware version '09' or later. If writing an invalid setting to an OPC UA server module with firmware version '08' or earlier, a setting file error (error code: 1C10H) occurs.
*3 When importing global labels with multidimensional arrays, select 'disabled (unselected).' Otherwise, the dimensional order of multidimensional arrays accessed from an OPC UA client will differ from global labels of a CPU module.

Point

- A log is not output when the free space of an SD memory card is less than 100 MB.
  Access an SD memory card from a personal computer and others, and delete an unnecessary log.
- To continuously output logs, it is recommended to secure 200 MB or more free space of an SD memory card.
- The waiting time for the module operation start is measured after turning the power OFF and ON, resetting a CPU module, or completing online module change. (The operation after completing online module change is the same as after turning the power OFF and ON and resetting a CPU module.)
  After the waiting time elapses, an OPC UA server module can be connected.

2.10 Global Label and Common Device Comment Import Function

This section describes the function to import global labels (including module labels) and common device comments set in an engineering tool into a project in the configuration tool (they are imported as data of a tag in an OPC UA server module). Data imported from global labels is referred to as related data.[1]

Related tags can be updated according to the changes of global labels in an engineering tool project.

 [1]   Data imported from module labels is not treated as related data.

Data which can be imported is as follows:

○: Available, ×: Not available, —: No data

Item	Engineering tool	Import source project
Common device comment	○	GX Works3 project (.gx3)
Device comment for each program	×	
Global label (Global)	○	
Module label (M+Global)	○	
Local label	×	
System label	—	

Information imported from each item is as follows:

Item	Information
Common device comment	• Comment • Device name
Global label	• Label name • Data type • Assignment (device)
Module label	

For global labels and device comments, refer to the following:

GX Works3 Operating Manual

Considerations for importing data

■Importing global labels

- Global labels can be imported only from a GX Works3 project, not from a GX Works2 project.
- An engineering tool (GX Works3 Version 1.040S or later) must be installed to import global labels.
- GX Works3 projects that require entering a user name and password or cannot be opened in an installed GX Works3 cannot be imported.
- Global labels with devices (data types) that cannot be set in the configuration tool are not imported. (However, they are displayed in the import list.) ☞ Page 37 Setting availability of data types for each device
- If the total of the number of units of basic data (tags) and that of structures (groups) exceeds 204800, global labels for exceeded numbers are not displayed in the import list. If a target global label is not displayed, perform either of the following operations:
  Create a tag or structure label in the configuration tool.
  Reduce the number of global labels set in one project of GX Works3 projects.
- Do not import global labels while operating an engineering tool project. If attempted, the project may not be saved properly.
- If imported global labels are copied or cut, and pasted to another access target device, they are not treated as related data.

■Importing common device comments

- Common device comments can be imported only from a GX Works3 project, not from a GX Works2 project.
- An engineering tool (GX Works3 Version 1.040S or later) must be installed to import common device comments.
- GX Works3 projects that require entering a user name and password or cannot be opened in an installed GX Works3 cannot be imported.
- When 32769 or more common device comments are set in one GX Works3 project, those exceeding 32768 are not displayed in the list. If a target common device comment is not displayed, perform the following operations:
  Create a tag in the configuration tool.
  Reduce the number of common device comments set in one GX Works3 project.
- Do not import common device comments while operating an engineering tool project. If attempted, the project may not be saved properly.
- When one or more comments are set for each device name to the imported common device comments, all the comments are displayed in the list.
- When common device comments are imported, the setting of each comment title is ignored.
  (Example) Common device comments can be imported in the configuration tool regardless of its language (Japanese, English, etc.)

Importing global labels

The following shows the procedure for importing global labels set in an engineering tool as data.

If global labels created in an engineering tool are changed, they are updated in a batch. It is therefore necessary to link the global labels.
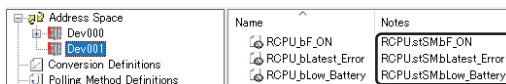
Operating procedure

1. Select an item (▊ or ▣) under "Address Space" in the tree view.

2. Select [Edit] ⇨ [Import Global Label].

3. Select an import source project of global labels in the "Import Global Label (Select Project)" screen, and click the [OK] button.

☞ Page 66 "Import Global Label (Select Project)" screen

4. If there are multiple units of setting data for a global label in an import source project, select setting data in the import source in the "Import Global Label (Select Global Label)" screen, and click the [OK] button.

☞ Page 66 "Import Global Label (Select Global Label)" screen

5. Select a global label to import in the "Import Global Label (Select Data)" screen, and click the [OK] button.

☞ Page 67 "Import Global Label (Select Data)" screen
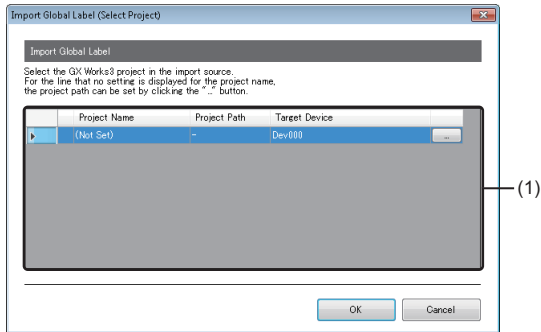
> **Point**
>
> - Regardless of an item (▊ or ▣) selected under "Address Space" in the tree view, global labels are imported immediately under an access target device selected in the "Import Global Label (Select Project)" screen.
> - If an imported global label is a structure, the data structure of the structure is imported into the structure definition. (☞ Page 53 Structure Definition Setting)
> - A tag with a global label imported is displayed as related data as shown below.
>
>
>
> - For related data, the following items cannot be edited:
>   Name, device type, digit specification, bit specification, extended number (network number or start I/O number), PLC device number (I/O address), data type (☞ Page 36 [Basic] tab)
>   Extended data type (☞ Page 38 [Details] tab)
> - When importing module labels, their details are applied to "Description."
>
>

■"Import Global Label (Select Project)" screen

Item	Description
(1) Import source list	An engineering tool project and access target device that are set as import sources of global labels are displayed. If no project is set in an access target device, "(Not Set)" is displayed. Select a project in the "Address Space(Target Device)" screen displayed by clicking the [...] button. ⤷ Page 32 Access target device
[OK] button	Click this to apply the setting and open the screen for selecting a global label to be imported. • When there is only one unit of setting data for a global label in an import source project: ⤷ Page 67 "Import Global Label (Select Data)" screen • When there are multiple units of setting data for a global label in an import source project: ⤷ Page 66 "Import Global Label (Select Global Label)" screen

■"Import Global Label (Select Global Label)" screen
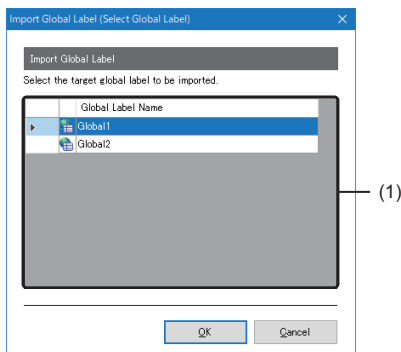
Item		Description
(1) Global label list	—	Setting data for a global label in an import source project is displayed in a list. Select setting data used as an import source.
	Global Label Name	The name of setting data for a global label is displayed.
[OK] button		Click this to open the screen for selecting a global label to be imported from selected setting data. ⤷ Page 67 "Import Global Label (Select Data)" screen

■"Import Global Label (Select Data)" screen
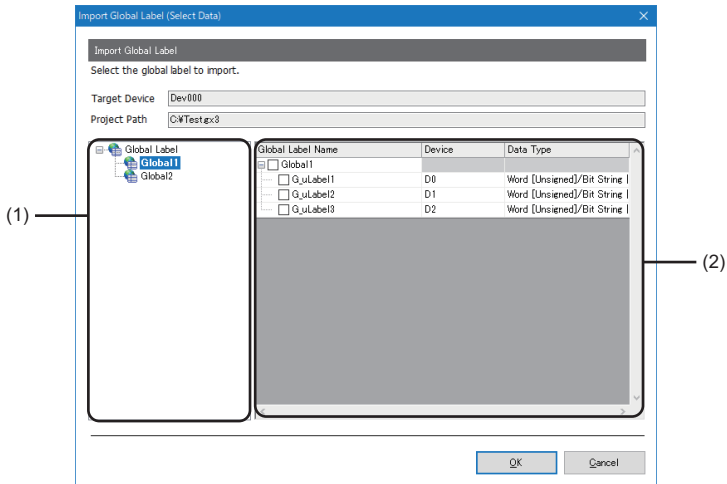
Item		Description
Target Device		An access target device selected in the "Import Global Label (Select Project)" screen is displayed.
Project Path		The path of a project selected in the "Import Global Label (Select Project)" screen is displayed.
(1) Global label list		Setting data for a global label in an import source project is displayed in a list. Select setting data used as an import source.
(2) Global label import list	—	The content of setting data selected in the global label list is displayed.
	Global Label Name	A global label name (set in an engineering tool) is displayed.[1] Select the checkbox of a global label to be imported.
	Device	The device of a global label is displayed.
	Data Type	The data type of a global label is displayed.
[OK] button		Click this to import a selected global label and close the screen.

[1] For a module label, the name is displayed in either of the following formats. If a name includes 257 or more characters, those exceeding the number are deleted to display.
- (instance name)_(module number)_(label name)
- (instance name)_(module number)_(label name)_D
For the instance name, module number, label name, or _D, refer to each of the following:
□☞ Page 112 Instance name, Page 112 Module number, Page 112 Label name, Page 112 _D

Precautions

- If the number of tags[1] exceeds 10000 after importing a global label, the global label cannot be imported. Reduce the number of global labels to be imported in the configuration tool, then import it again.

[1] When using a structure label, a member of a structure is also treated as a tag.

- A global label cannot be imported if it applies to any of the following conditions:

| Item	Condition
Label name	• A character other than one shown in the following section is used. ☞ Page 131 Available ASCII characters • The checkbox of a global label with the same name is already selected. • The total number of characters in a structure label name and member name (including a member of a structure) exceeds 800 after importing a global label.
Device	• A device type or representation that is not supported by an OPC UA server module is used.
Class	• 'VAR_GLOBAL_CONSTANT' is used.
Data type	• A data type that is not supported by an OPC UA server module is used. (☞ Page 71 Data types) • A combination of a device and data type that is not supported by an OPC UA server module is used. (☞ Page 37 Setting availability of data types for each device) • When the data type is a string, the number of characters exceeds 255.
Array	• The first element number of each dimension of an array is set to a number other than '0.' • The product of the numbers of elements in each dimension of an array exceeds the upper limit.[1] • For a bit device, the product of the numbers of elements in each dimension of an array is set to a number other than a multiple of 16. • A data type that is not supported by an OPC UA server module is used. (☞ Page 71 Data types)
Structure	• The number of members of a structure exceeds the upper limit.[1]
Project	• A project file is not converted.
All items	• The total of the number of units of basic data (tags) and that of structures (groups) exceeds 204800. For each calculation method, refer to the following: 📖 MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

[1] For the upper limit, refer to the following:
  📖 MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

■Global label name

- Basic data

A display example when a global label is basic data and one of a tag name after import are as follows:
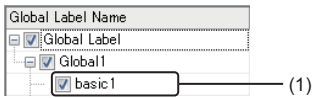
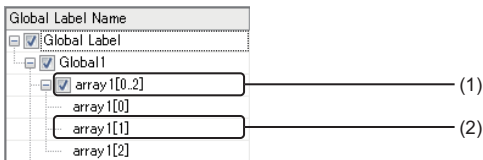| Type	Display example of a global label name	Display example of a tag name after import
(1) Basic data	basic1	basic1

- Array

A display example when a global label is an array and one of a tag name after import are as follows:

Type	Display example of a global label name	Display example of a tag name after import
(1) Array data	array1[0..2]	array1
(2) Array element	array1[1]	—

- Structure

A display example when a global label is a structure and one of a structure label name and tag name after import are as follows:
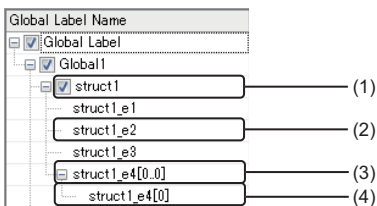
Type	Display example of a global label name	Display example of a structure label name after import	Display example of a tag name after import
(1) Structure data	struct1	struct1	—
(2) Structure element	struct1_e2	—	struct1_e2
(3) Structure element [array]	struct1_e4[0..0]	—	—
(4) Array element	struct1_e4[0]	—	struct1_e4

• Structure array

A display example when a global label is a structure array and one of a structure label name and tag name after import are as follows:

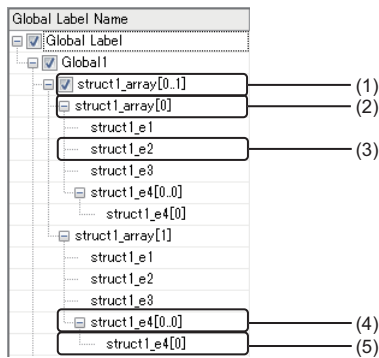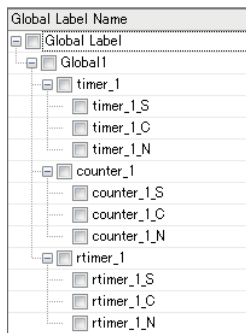| Type	Display example of a global label name	Display example of a structure label name after import	Display example of a tag name after import
(1) Structure array data	struct1_array[0..1]	struct1_array	—
(2) Structure array element	struct1_array[0]	—	—
(3) Structure element	struct1_e2	—	struct1_e2
(4) Structure element [array]	struct1_e4[0..0]	—	—
(5) Array element	struct1_e4[0]	—	struct1_e4

• Timer/counter/retentive timer

A display example when a global label is a timer, counter, or retentive timer and one of a tag name after import are as follows:

Type		Display example of a global label name[*1][*2]	Display example of a tag name after import
Timer	Contact	timer_1_S	timer_1_S
	Coil	timer_1_C	timer_1_C
	Current value	timer_1_N	timer_1_N
Counter	Contact	counter_1_S	counter_1_S
	Coil	counter_1_C	counter_1_C
	Current value	counter_1_N	counter_1_N
Retentive timer	Contact	rtimer_1_S	rtimer_1_S
	Coil	rtimer_1_C	rtimer_1_C
	Current value	rtimer_1_N	rtimer_1_N

*1 A contact, coil, and current value are displayed as follows:
   - Contact: (label name)_S
   - Coil: (label name)_C
   - Current value: (label name)_N
*2 When setting the timer, counter, or retentive timer as an array, they are displayed as arrays of a contact, coil, and current value.

■Data types

The following table shows the data types of global labels and those of tags after import.

○: Available, ×: Not available

Data type of a global label	Import			Data type of a tag
	Without array	With array[*1]	Structure	
Bit	○	○	○	BOOL
Word [signed]	○	○	○	INT
Double word [signed]	○	○	○	DINT
Word [unsigned]/bit string [16-bit]	○	○	○	UINT
Double word [unsigned]/bit string [32-bit]	○	○	○	UDINT
Float (single precision)	○	○	○	REAL
Float (double precision)	○	○	○	LREAL
String (n)[*2]	○	×	○	STRING
String [Unicode] (n)[*2]	○	×	○	WSTRING
Timer	○	○[*3]	×	Contact: BOOL Coil: BOOL Current value: INT
Counter	○	○[*3]	×	
Retentive timer	○	○[*3]	×	
Long timer	○	○[*3*4]	×	Contact: BOOL Coil: BOOL Current value: DINT
Long counter	○	○[*3]	×	
Long retentive timer	○	○[*3*4]	×	
Time	○	○	○	TIME
Pointer	×	×	×	—

*1 Global labels with bit-specified or digit-specified devices assigned cannot be imported.

*2 'n' indicates the number of characters. Import to a project of the configuration tool is available only when 'n' is 1 to 255.

*3 Only device-assigned global labels can be imported.

*4 Only the current values (LTN, LSTN) can be imported.

Releasing relation to global labels

The following shows the procedure for releasing the relation between a global label of an engineering tool and related data.

Operating procedure

Select and right-click an item (📊 or 📁) under "Address Space" in the tree view or related data in the list view, then select [Release Relation to Global Label] from the shortcut menu.

> **Point**
>
> - When selecting an item (📊 or 📁), all related data under the item is the target.
> - The relation can also be released when unselecting the checkbox of "Use the global label/common device comment" in the "Address Space(Target Device)" screen. (☞ Page 32 Access target device)

Precautions

To link the data whose relation was once released, import the global label again.

Updating data related to global labels

The following shows the procedure for updating data related to a global label of an engineering tool to the latest value.
If it cannot be updated, the relation will be released.

> **Point**
>
> If there are multiple labels with a same name set in an engineering tool project, global labels are updated to the content set in the first label.

Operating procedure

1. Select an item (▊▊ or 🟡) under "Address Space" in the tree view.

2. Select [Edit] ⇨ [Update Data Related to Global Label].

3. Select a project to be updated in the "Update Data Related to Global Label (Select Project)" screen, and click the [OK] button.
   ☞ Page 73 "Update Data Related to Global Label (Select Project)" screen

4. Select a global label to be updated in the "Update Data Related to Global Label (Select Data)" screen, and click the [OK] button.
   ☞ Page 74 "Update Data Related to Global Label" screen

■"Update Data Related to Global Label (Select Project)" screen

Item		Description
Import Target[1]	All Projects	Select this to update related data of all projects.
	Specified Project	Select this to update related data of a specified project.
(1) Import source list		An engineering tool project and access target device that are set as import sources of global labels are displayed. If no project is set in an access target device, "(Not Set)" is displayed. Select a project in the "Address Space(Target Device)" screen displayed by clicking the [...] button. ☞ Page 32 Access target device
[OK] button		Click this to apply the setting and open the screen for selecting a global label to be updated. ☞ Page 74 "Update Data Related to Global Label" screen

*1 Does not appear when displaying this screen by either of the following operations:
- Importing a CSV file
- Writing a setting to an OPC UA server module

■"Update Data Related to Global Label" screen

Item	Description
Tag Name	The name of a tag is displayed.
Target Device	An access target device is displayed.
Type	Either of the following items is displayed. • Update: When related data, devices, or data types are different from the previous data, the values are updated. • Relation Release: The relation is released when related data is not found or there is an inconsistency due to update.[1]
Device	A device after update is displayed. If a device is changed after update, the device name is displayed in red.
Data Type	A data type after update is displayed. If a data type is changed after update, it is displayed in red.
[OK] button	Click this to update related data or release the relation.

[1]   Applies to the following cases:
    - The global label name does not exist in an import source project.
    - A device, class, data type, or character string size that cannot be used for an OPC UA server module is specified.
    - A device that cannot be combined with a data type is used.
    - The total number of characters per structure label or structure definition exceeds the upper limit. (📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup))

Importing common device comments

The following shows the procedure for importing common device comments set in an engineering tool as data.

Operating procedure

1. Select an item (▦ or ▨) under "Address Space" in the tree view.

2. Select [Edit] ⇨ [Import Common Device Comment].

3. Select an import source project of common device comments in the "Import Common Device Comment (Select Project)" screen, and click the [OK] button.
☞ Page 75 "Import Common Device Comment (Select Project)" screen

4. Select common device comments to import in the "Import Common Device Comment (Select Data)" screen, and click the [OK] button.
☞ Page 76 "Import Common Device Comment (Select Data)" screen

> **Point**
>
> Regardless of an item (▦ or ▨) selected under "Address Space" in the tree view, common device comments are imported immediately under an access target device selected in the "Import Common Device Comment (Select Project)" screen.

■"Import Common Device Comment (Select Project)" screen

Item	Description
(1) Import source list	An engineering tool project and access target device that are set as import sources of common device comments are displayed. If no project is set in an access target device, "(Not Set)" is displayed. Select a project in the "Address Space(Target Device)" screen displayed by clicking the [...] button. ☞ Page 32 Access target device
[OK] button	Click this to apply the setting and open the screen for selecting a common device comment to be imported. ☞ Page 76 "Import Common Device Comment (Select Data)" screen

■"Import Common Device Comment (Select Data)" screen
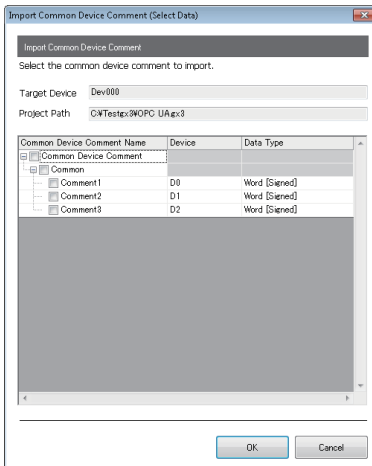
Item	Description
Target Device	An access target device selected in the "Import Common Device Comment (Select Project)" screen is displayed.
Project Path	The path of a project selected in the "Import Common Device Comment (Select Project)" screen is displayed.
Common Device Comment	A common device comment (set in an engineering tool) is displayed. Select the checkbox of a common device comment to import.
Device	A device with a common device comment is displayed.
Data Type	The data type of a device is displayed.
[OK] button	Click this to import a selected common device comment and close the screen.

Precautions

- If the number of tags[*1] exceeds 10000 after importing a common device comment, the common device comment cannot be imported. Reduce the number of common device comments to be imported in the configuration tool, then import it again.

*1   When using a structure label, a member of a structure is also treated as a tag.

- A common device comment cannot be imported if it applies to any of the following conditions:

Item	Condition
Comment	• A character other than one shown in the following section is used. ⧉ Page 131 Available ASCII characters • It exceeds 256 characters. • The checkbox of a common device comment with the same name is already selected. • The total number of characters in a structure label name and member name (including a member of a structure) exceeds 800 after importing a common device comment.
Device	• No device is assigned. • A device type or representation that is not supported by an OPC UA server module is used.
Data type	• A data type that is not supported by an OPC UA server module is used. (⧉ Page 71 Data types) • A combination of a device and data type that is not supported by an OPC UA server module is used. (⧉ Page 37 Setting availability of data types for each device) • When the data type is a string, the number of characters exceeds 255.
Project	• A project file is not converted.

■Data type

The correspondence between the data types of devices for which common device comments are set and those of tags after import is same as that shown in the following section.

⧉ Page 71 Data types

2.11 Online

This section shows the online operations performed to an OPC UA server module connected on a network.

Connection destination setting

The following shows the screen for setting and editing connection destination information.
Perform the user authentication when connecting actually.

Window

Select [Online] ⇨ [Target Setting].
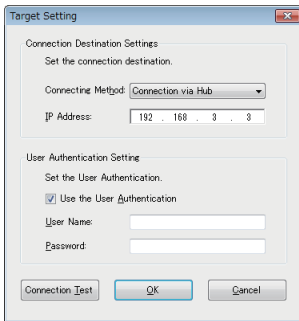
Displayed items

Item		Description
Connection Destination Settings	Connecting Method	Select a connection method.
	IP Address	Set the IP address for connection destination.
User Authentication Setting	Use the User Authentication	Select the checkbox to perform user authentication.
	User Name	Specify a user name for user authentication.
	Password	Specify a password for user authentication.
[Connection Test] button		Click this to perform a connection test with a set connection destination.

Online data operations

The following shows the operations for reading, writing, verifying, and updating a setting (project) in an OPC UA server module.

Reading from an OPC UA server module

A setting in an OPC UA server module specified in the "Target Setting" screen can be read.

Precautions

 • When reading a project in the information model mode
Reading takes time according to the number of Nodes due to decoding information models and mapping information.
(Example) If the number of Nodes included in an information model file exceeds 10000, it may take one minute or more.

Operating procedure

Select [Online] ⇨ [Read from OPC UA Server Module].

> *Restriction*
>
> If writing a setting to a module in a configuration tool with software version '1.07H' or later, the security policy setting may be changed when reading the setting in software version '1.06G' or earlier. (☞ Page 60 Security policy compatibility)
> Update the configuration tool to the latest software version before reading.

■Reading availability list

The following table shows the reading availability for each combination of the firmware version of an OPC UA server module and the software version of the configuration tool.
Note that even if it is 'available,' a setting may not be read depending on the combination of a function used in a project and the software version of the configuration tool.

○: Available, ─: Not available

Firmware version and operation mode of a module		Software version and operation mode of the configuration tool			
		'1.08J' or earlier	'1.09K' to '1.10L'	'1.11M' or later	
				Tag mode	Information model mode
'9' or earlier		○	○	○	○[*1]
'10' to '11'		─	○	○	○[*1]
'12' or later	Tag mode	─	○	○	○[*1]
	Information model mode	─	─	○[*1]	○

*1   The configuration tool in a mode supporting a project to be read must be started.

Writing to an OPC UA server module

A setting can be written to an SD memory card inserted in an OPC UA server module specified in the "Target Setting" screen.

Operating procedure

1. Select [Online] ⇨ [Write to OPC UA Server Module].

2. Update data related to global labels as necessary. (☞ Page 73 Updating data related to global labels)

Restriction

• If writing a setting to a module in a configuration tool with software version '1.07H' or later, the security policy setting may be changed when writing the setting in software version '1.06G' or earlier. (☞ Page 60 Security policy compatibility)
Update the configuration tool to the latest software version before writing.

• A setting cannot be written to a module with firmware version '09' or earlier in a configuration tool with software version '1.09K' or later. Update the module to the latest firmware version before writing.

■Writing availability list

The following table shows the writing availability for each combination of the firmware version of an OPC UA server module and the software version of the configuration tool, and the operation mode after updating the setting.
Note that even if it is 'available,' a setting may not be written or operations may not be performed on the module depending on the combination of a function used in a project and the firmware version of the module.

○: Available (after setting update: tag mode), ●: Available (after setting update: information model mode), ―: Not available

Firmware version and operation mode of a module		Software version and operation mode of the configuration tool			
		'1.08J' or earlier	'1.09K' to '1.10L'	'1.11M' or later	
				Tag mode	Information model mode
'9' or earlier		○	―	―	―
'10' to '11'		―*1	○	○	―
'12' or later	Tag mode	―*1	○	○	―
	Information model mode	―*1	○	―	●

*1 Available but a setting file error (error code: 1C10H) occurs after updating the setting.

Verification with an OPC UA server module

A setting in an OPC UA server module specified in the "Target Setting" screen can be verified with the setting of a project being edited.

Operating procedure

Select [Online] ⇨ [Verify with OPC UA Server Module].

> **Restriction** 🖐
>
> - If writing a setting to a module in a configuration tool with software version '1.01B' or later, the setting cannot be verified correctly in software version '1.00A.' Update the configuration tool to the latest software version before verification.
> - If writing a setting to a module in a configuration tool with software version '1.07H' or later, the setting may not be verified correctly in software version '1.06G' or earlier due to the change in the security policy setting method. (☞ Page 60 Security policy compatibility)
>   Update the configuration tool to the latest software version before verification.
> - Even if the setting contents of a project created in the configuration tool are the same as those of one created by importing a CSV file, the verification result may be different.
> - If writing a setting to a module in a configuration tool with software version '1.08J' or earlier, the setting cannot be verified correctly in software version '1.09K' or later.
>   Check the following to solve the problem.
>   - For the firmware version '10' or later:
>   Read a setting from the OPC UA server module and write (read/write) it to the module again before verification.
>   - For the firmware version '04' to '09':
>   Update the OPC UA server module to the latest version and read/write a setting before verification.
>   - For the firmware version '03' or earlier:
>   Please contact your local Mitsubishi Electric sales office or representative.

■Verification availability list

The following table shows the verification availability for each combination of the firmware version of an OPC UA server module and the software version of the configuration tool. Note that even if it is available, some combinations always result in a mismatch.

○: Available, △: Available (always mismatch), ─: Not available

Firmware version and operation mode of a module		Software version and operation mode of the configuration tool			
		'1.08J' or earlier	'1.09K' to '1.10L'	'1.11M' or later	
				Tag mode	Information model mode
'9' or earlier		○	△	△	△
'10' to '11'		─	○	○	△
'12' or later	Tag mode	─	○	○	△
	Information model mode	─	─	△	○

Setting update of an OPC UA server module

A setting in an OPC UA server module specified in the "Target Setting" screen can be updated.

Operating procedure

Select [Online] ⇨ [Update setting of OPC UA Server Module].

Server operation

The following shows the operations for restarting and stopping a server operation of an OPC UA server module.

Restart of an OPC UA server module

A server operation of an OPC UA server module specified in the "Target Setting" screen can be restarted.

Operating procedure

Select [Online] ⇨ [Restart the OPC UA Server Module].

Stop of an OPC UA server module

A server operation of an OPC UA server module specified in the "Target Setting" screen can be stopped.

Operating procedure

Select [Online] ⇨ [Stop the OPC UA Server Module].

■Start of an operation

After stopping an OPC UA server module, its operation can be started by the following operations. Whether the setting is updated differs for each operation.

Operation	Setting update
Restarting an OPC UA server module	Not updated
Updating the setting of an OPC UA server module	Updated
Powering OFF and ON	

Information on an OPC UA server module

The following shows the screen for displaying the operating status of an OPC UA server module.

Window

Select [Online] ⇨ [OPC UA Server Module Information].
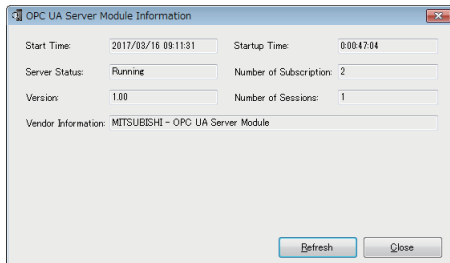
Displayed items

Item	Description
Start Time	The date and time when a server started is displayed.
Startup Time	The elapsed time since a server started is displayed.
Server Status	The status of a server is displayed.
Number of Subscription	The number of accumulated subscriptions since a server started is displayed.[1]
Version	The software version of a server is displayed.
Number of Sessions	The number of sessions of OPC UA clients connected to a server is displayed.[1]
Vendor Information	The vendor information is displayed.
[Refresh] button	Click this to update the operating status of a server to the latest information.

[1] "0" is always displayed when the module is in the information model mode and no information model file is imported in the project.

SD memory card diagnostic

The following shows the screen for displaying the current use status of an SD memory card inserted in an OPC UA server module and formatting the SD memory card.

Window

Select [Online] ⇨ [SD Memory Card Diagnosis].
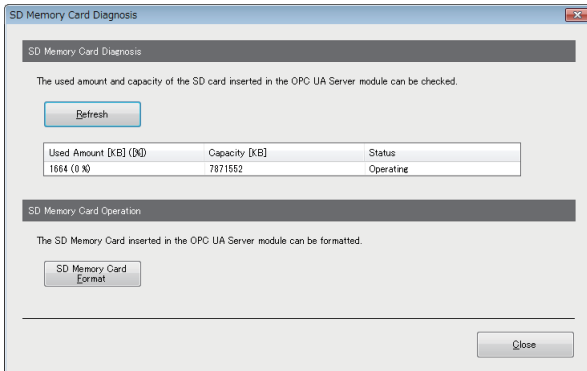
Displayed items

Item		Description
SD Memory Card Diagnosis	[Refresh] button	Click this to update the status of an SD memory card to the latest information.
	Used Amount [KB] ([%])	The used amount and use rate of an SD memory card are displayed.
	Capacity [KB]	The capacity of an SD memory card is displayed.
	Status	The status of an SD memory card is displayed.
SD Memory Card Operation	[SD Memory Card Format] button	Click this to format an SD memory card.

Precautions

All the settings of OPC UA server module will be lost if the SD memory card is formatted since the settings are saved in the SD memory card.

Read the current setting as necessary, and write the setting after formatting the card.

If the power is turned OFF to ON or the CPU module is reset without writing the setting in the SD memory card, the IP address of the OPC UA server module returns to the initial state (192.168.3.3).

Application certificate management

The following shows the screen for managing application certificates in an OPC UA server module.

When certificates are exchanged automatically, a client certificate is not displayed. (☞ Page 55 Security Setting)

The [Trusted] tab is used for communicating with an OPC UA client by using a normal authentication method, and the [Issuers] tab for the communication by using Issuers authentication.

For managing certificates certified by a certificate authority, refer to the following:

☞ Page 136 Handling Certificates Certified by a Certificate Authority

> **Point**
>
> Issuers authentication is an authentication method using an electronic certificate issued by a certificate authority. It allows communication more secure than a normal authentication method.
>
> For Issuers authentication, upload an electronic certificate issued by a certificate authority to "Trust List" in the [Issuers] tab, and a client certificate to trust to "Trust List" in the [Trusted] tab.

Window

Select [Online] ⇨ [Manage Application Certificate].

Displayed items

■[Trusted] tab/[Issuers] tab

Item		Description
Trust list	—	A list to register the certificate of a client (der) which is allowed to connect. When trusting an OPC UA client which requests to connect and allowing the connection, click the [Upload] button to upload a client certificate (der) to trust to the trust list. ■When communicating by using a certificate certified by a certificate authority Upload an electronic certificate issued by a certificate authority. The connection only from an OPC UA client using the certificate listed on the electronic certificate is allowed.
	[Upload] button	Click this to transfer an arbitrary certificate from a configuration personal computer to the SD memory card inserted in an OPC UA server module.
	[Download] button	Click this to transfer an arbitrary certificate from the SD memory card inserted in an OPC UA server module to a configuration personal computer.
	[Delete] button	Click this to delete an arbitrary certificate in the SD memory card inserted in an OPC UA server module.

Item		Description
Revocation List	—	A client certificate (der_NG) is automatically stored when the trust of the certificate stored in "Trust List" is lost (such as expiration). ■When communicating by using a certificate certified by a certificate authority Upload the certificate revocation list (crl) issued by a certificate authority. The connection from an OPC UA client using the certificate listed on the certificate revocation list is denied.
	[Upload] button	Click this to transfer an arbitrary certificate from a configuration personal computer to the SD memory card inserted in an OPC UA server module.
	[Download] button	Click this to transfer an arbitrary certificate from the SD memory card inserted in an OPC UA server module to a configuration personal computer.
	[Delete] button	Click this to delete an arbitrary certificate in the SD memory card inserted in an OPC UA server module.
Denied Certificate List	—	A client certificate denied when connecting is automatically stored. To allow the connection, click the [Download] button to download the certificate and upload it to "Trust List."
	[Download] button	Click this to transfer an arbitrary certificate from the SD memory card inserted in an OPC UA server module to a configuration personal computer.
	[Delete] button	Click this to delete an arbitrary certificate in the SD memory card inserted in an OPC UA server module.
	[Refresh] button	Click this to update the denied certificate list to the latest information.
[Server Certificate Upload] button		Click this to transfer a server certificate from a configuration personal computer to the SD memory card inserted in an OPC UA server module. Use this button to upload a certificate (such as one issued by a certificate authority) other than one with the contents set in the following section. ☞ Page 61 [Certificate] tab
[Server Certificate Download] button		Click this to transfer a server certificate from the SD memory card inserted in an OPC UA server module to a configuration personal computer. A downloaded certificate is used for issuing an electronic certificate and others.
[Server Certificate Delete] button		Click this to delete a server certificate in the SD memory card inserted in an OPC UA server module. When a certificate is deleted, a certificate with the contents set in the following section is created once the power is turned OFF to ON or the CPU module is reset. ☞ Page 61 [Certificate] tab
[Server Private Key Upload] button		Click this to transfer the server private key of an OPC UA server module from a configuration personal computer to the SD memory card inserted in an OPC UA server module. The server private key paired with a certificate uploaded by clicking the [Server Certificate Upload] button is uploaded.
[Server Private Key Download] button		Click this to transfer the server private key of an OPC UA server module from the SD memory card inserted in an OPC UA server module to a configuration personal computer. A downloaded server private key is used for issuing an electronic certificate and others.
[Server Private Key Delete] button		Click this to delete the server private key of an OPC UA server module in the SD memory card inserted in an OPC UA server module. If the server private key is deleted, a server private key paired with a certificate set in the following section is created once the power is turned OFF and ON or the CPU module is reset. ☞ Page 61 [Certificate] tab

Restriction🖑

Certificates cannot be uploaded in the following cases:
- A file name contains a double-byte character.
- A file name contains a single-byte katakana.
- A file name exceeds 80 characters.
- A file path exceeds 126 characters.

User certificate management

The following shows the screen for managing user certificates in an OPC UA server module.

The [Trusted] tab is used for communicating with an OPC UA client by using a normal authentication method, and the [Issuers] tab for the communication by using Issuers authentication.

For managing certificates certified by a certificate authority, refer to the following:

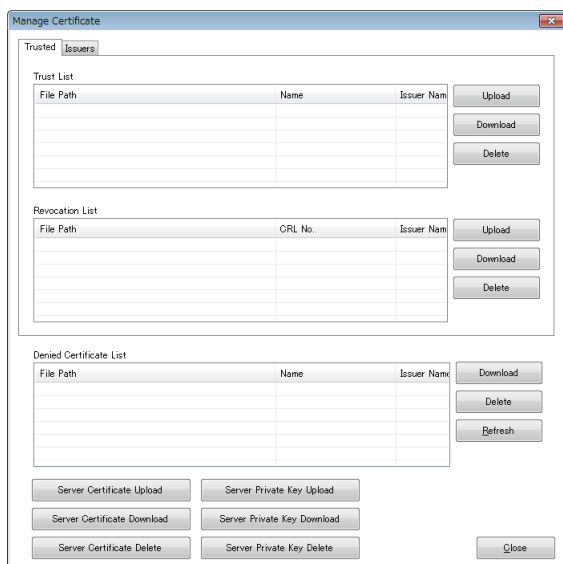☞ Page 136 Handling Certificates Certified by a Certificate Authority

> **Point**
>
> Issuers authentication is an authentication method using an electronic certificate issued by a certificate authority. It allows communication more secure than a normal authentication method.
>
> For Issuers authentication, upload an electronic certificate issued by a certificate authority to "Trust List" in the [Issuers] tab, and a client certificate to trust to "Trust List" in the [Trusted] tab.

Window

Select [Online] ⇨ [Manage User Certificate].
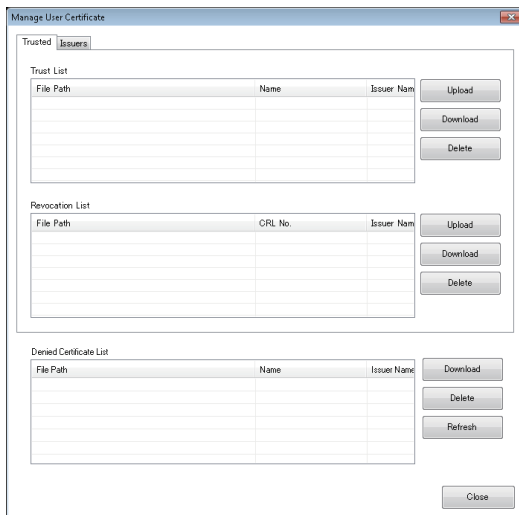
Displayed items

The screen items are same as those described in the following section.

☞ Page 84 [Trusted] tab/[Issuers] tab

Note that the following items are not displayed.

- [Server Certificate Upload] button
- [Server Certificate Download] button
- [Server Certificate Delete] button
- [Server Private Key Upload] button
- [Server Private Key Download] button
- [Server Private Key Delete] button

OPC UA server module management

Information in an OPC UA server module can be displayed and operations can be performed to it.

Firmware update management

The following shows the screen and procedure for displaying and changing the prohibition state of the firmware update set in an OPC UA server module.

Window

Select [Online] ⇨ [OPC UA Server Module Management].
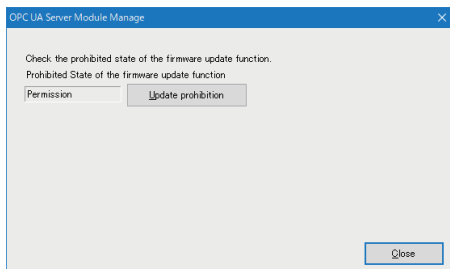
Displayed items

Item	Description
Prohibited State of the firmware update function*1	The prohibition state of the firmware update is displayed.
[Update prohibition] button*2	Click this to display the "Firmware Update Function Prohibition Operation" screen.
[Update prohibition release] button*3	☞ Page 87 Changing the prohibition state of the firmware update

*1 "-" is displayed if acquiring the prohibition state fails in communication with an OPC UA server module.
*2 Appears when "Permission" or "-" is displayed for "Prohibited State of the firmware update function"; however, it cannot be clicked when "-" is displayed.
*3 Appears when "Prohibition" is displayed for "Prohibited State of the firmware update function."

■Changing the prohibition state of the firmware update

Operating procedure

• For setting it to "Prohibition"

1. Set a password for "Prohibition release password" and "Prohibition release password (Confirm Password)" (8 to 16 characters).

2. Click the [OK] button.

• For setting it to "Permission"

1. Enter a password set for "Prohibition release password."

2. Click the [OK] button.

> *Point*
>
> If a prohibition release password is forgotten, initialize an OPC UA server module. "Prohibited State of the firmware update function" is set to "Permission."
> ☞ Page 22 Initialization function

2.12 Help

This section shows the help function for the following operations.

- Opening the user's manual
- Version information

Opening the user's manual

The user's manual (operation help) can be opened by the following operation.

Operating procedure

Select [Help] ⇨ [Help].

Version information

The version information of the configuration tool can be checked by the following operation.

Operating procedure

Select [Help] ⇨ [Version Information].

3 PARAMETER SETTING

This chapter explains each setting that can be set in the parameter setting of an engineering tool.

3.1 Parameter Setting Procedure

1. Add an OPC UA server module to an engineering tool.

🖱 [Navigation window] ➪ [Parameter] ➪ [Module Information] ➪ right-click ➪ [Add New Module] in the shortcut menu

2. Set two types of parameter settings, basic settings and refresh settings, by selecting in the tree in the screen displayed by the following operation:

🖱 [Navigation window] ➪ [Parameter] ➪ [Module Information] ➪ [RD81OPC96]

3. Write the settings to a CPU module in the engineering tool.

🖱 [Online] ➪ [Write to PLC]

4. The settings are applied by resetting the CPU module or turning the power OFF and ON.

3.2 Basic Setting

This section shows the various operation settings of an OPC UA server module.
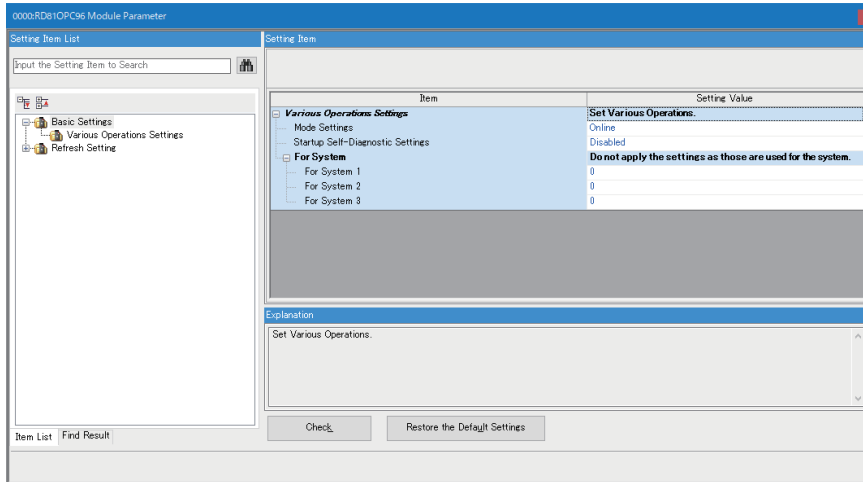
Various operation settings

The mode setting and the response monitoring time setting of an access target device for an OPC UA server module can be configured.

Item name		Description	Setting range
Mode Settings[1]		Set the operation mode of an OPC UA server module. • Online: Normal operation mode • Online (Asynchronous Mode): An OPC UA server module and a CPU module start without synchronization. • Firmware update: To update the firmware of an OPC UA server module. • Module initialization setting: To initialize information retained in an OPC UA server module. • Automatic hardware test: Hardware such as ROM/RAM/Ethernet of an OPC UA server module is tested. • Hardware test for LED check: LED of an OPC UA server module is tested.	• Online • Online (Asynchronous Mode)[2] • Firmware update • Module initialization setting • Automatic hardware test • Hardware test for LED check (Default: Online)
Startup Self-Diagnostic Settings[3][4]		Set whether or not to test the hardware (ROM) at startup. When "Enabled", hardware (ROM) related failures can be detected before operation. The startup time of OPC UA Server module will be longer than when it is "Disabled". Please verify it well before operating the system. Regardless of whether it is "Enabled" or "Disabled", if a hardware (ROM) related failure is detected during operation, it will be notified with an error code or watchdog timer error.	• Disabled • Enabled (Default: Disabled)
For System	For System 1 to 3	Do not use these since they are used only for the system.	—

*1 For the difference between 'online' and 'online (asynchronous mode),' refer to the following:
    ☞ Page 91 Online and online (asynchronous mode)
*2 Available for the following combinations:
    - OPC UA server module: Firmware version '02' or later
    - GX Works3: Software version '1.055H' or later
*3 When "Enabled," the time until an OPC UA server module starts will be longer, but this does not affect the startup time of a programmable controller CPU module (start of a sequence program).
*4 Available for the following combinations:
    - OPC UA server module: Firmware version '12' or later
    - GX Works3: Software version '1.105K' or later

Online and online (asynchronous mode)

The following explains the difference between 'online' and 'online (asynchronous mode).'

■Online

A CPU module and an OPC UA server module synchronize each other and complete their start processing, then start at the same time. (A CPU module stands by until an OPC UA server module completes its start processing.)

■Online (asynchronous mode)

A CPU module and an OPC UA server module start individually when their start processing is completed without waiting for the completion of the processing of the other module.

Precautions

The following shows the considerations for using 'online (asynchronous mode).'

• Do not access the buffer memory of an OPC UA server module until the module starts after a CPU module starts.

Otherwise, an indefinite value may be acquired and a sequence program may not run as intended.

When accessing the buffer memory, make sure that 'Module READY' (X0) is turned ON.

3.3 Refresh Setting

This section shows the setting of the refresh timing of the specified target.
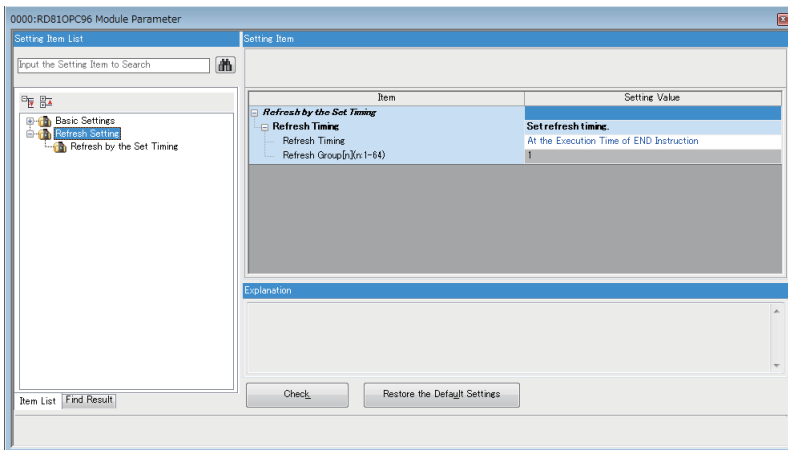
Setting value	Description
At the Execution Time of END Instruction	To refresh at the END processing in a CPU module.
At the Execution Time of Specified Program	To refresh when executing a program specified in "Refresh Group [n]."

4 TROUBLESHOOTING

This chapter explains the errors which may occur when using an OPC UA server module and the troubleshooting.

4.1 Checking Method for Error Descriptions

The following are the methods for checking error descriptions.

Checking method	Details
"Module Diagnostics" screen of an engineering tool	Error codes[1] can be checked in the "Module Diagnostics" screen of an engineering tool. The "Module Diagnostics" screen can be displayed from the system monitor. ☞ Page 93 Checking the Module Status
Buffer memory	Error codes[1] can be checked in the following buffer memory. ☞ Page 124 Error code (Un\G7168) ☞ Page 127 Error log 1 to 16 (Un\G13058 to 13217)
Dot matrix LED	Error codes[1] can be checked with the dot matrix LED on the front of an OPC UA server module.

*1 Error code
  If the same error occurs repeatedly, the error is output only for the first time. (Detailed information is also output only for the first occurrence of the error.)
  When the same error occurs several times in different causes, take action to correct the error in the order of occurrence based on the error code and detailed information that were outputted at the first occurrence of the error.
  By clearing the error (or resetting and turning the power OFF and ON) after taking the corrective action, error information is output when the same error occurs again.

Error type

There are two types of errors of an OPC UA server module as follows:

Error type	ERR LED	Module status	Corrective action
Module stop error	Flashing	An OPC UA server function of a module stops.	Take action for the error according to the error code, and turn the 'ERR LED' OFF by any of the following operations: • Error clear request (Y10) • Turn the power OFF and ON. • Reset the CPU module. • Update the setting in the configuration tool.
Module continuation error	ON	An OPC UA server function of a module continues.	

4.2 Checking the Module Status

The module status can be checked in the "Module Diagnostics" screen of an engineering tool.

Function	Purpose	Reference
Error Information	To display the description of an error currently occurred. The history of errors detected and operations performed in an OPC UA server module can be checked by clicking the [Event History] button.	Page 93 Error information
Module Information List	To display the information on each status of an OPC UA server module.	Page 94 Module information list

In addition, the self-diagnostic tests that check the hardware of an OPC UA server module can be performed in an engineering tool. (☞ Page 95 Self-diagnostic test)

Error information

The description of an error occurring and its corrective action can be checked in the [Error Information] tab.

Window
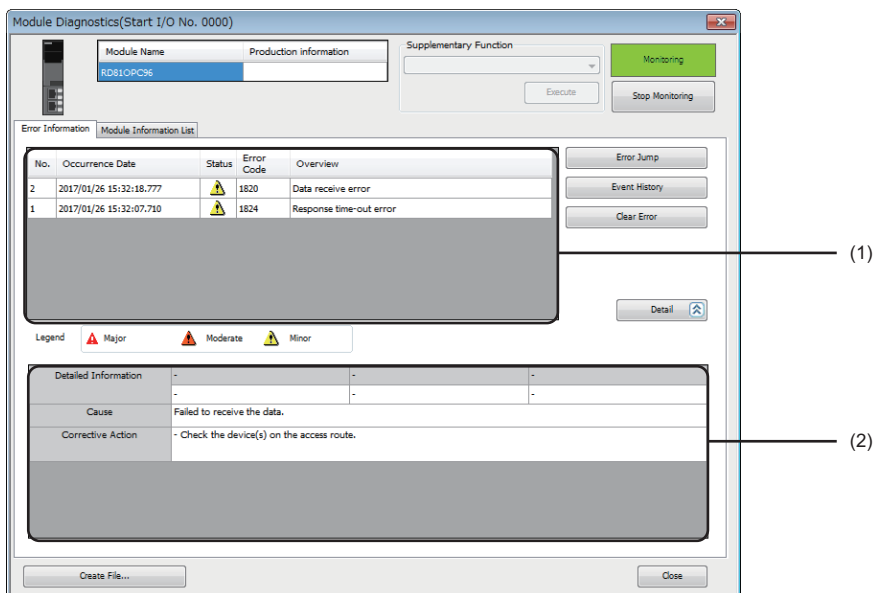
Displayed items

Item		Description
(1) Error information list		Errors occurring are listed.
(2) Error detailed information	—	Detailed information on an error selected in the error information list is displayed.
	Detailed Information	Detailed information of an error is displayed (up to three).
	Cause	An error cause is displayed.
	Corrective Action	A corrective action for an error is displayed.

Restriction

An error in an OPC UA server module cannot be cleared with the [Clear Error] button.
To clear an error, update the setting in the configuration tool. (☞ Page 80 Setting update of an OPC UA server module)

Module information list

The LED information and switch information can be checked in the [Module Information List] tab.

During a self-diagnostic test, "Automatic hardware is being tested" or "Hardware test for LED check is being executed" is displayed in all the LED information and switch information.

If an error occurs, refer to the following section to take corrective action.

☞ Page 98 Troubleshooting by Symptom

Window
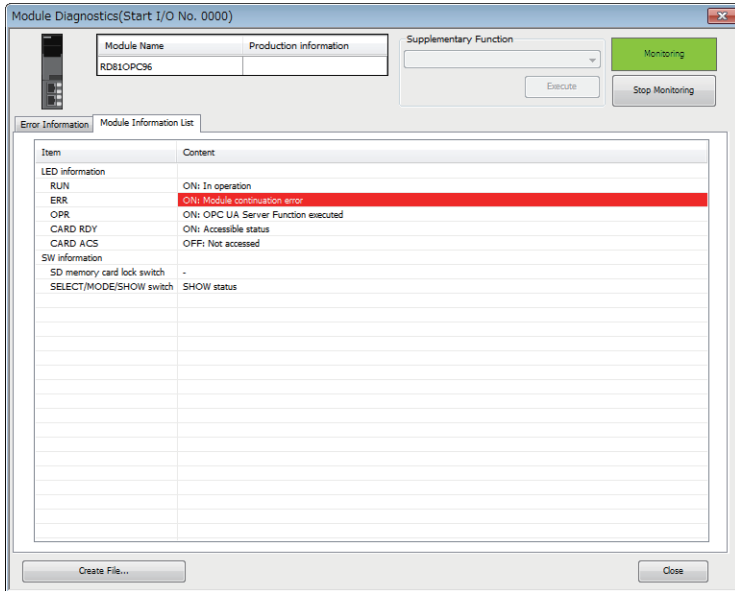
Displayed items

Item		Description
LED information	RUN	The running status of a module is displayed.
	ERR	The error status of a module is displayed.
	OPR	The operating status of a module is displayed.
	CARD RDY	The status of an SD memory card is displayed.
	CARD ACS	The access status of an SD memory card is displayed.
SW information	SD memory card lock switch	Information on the SD memory card lock switch is displayed.
	SELECT/MODE/SHOW switch	Information on the dot matrix LED display mode switch is displayed.

Self-diagnostic test

Automatic hardware test

The following explains the test on hardware such as ROM/RAM/Ethernet of an OPC UA server module.

> **Restriction** ✋
>
> The values in the buffer memory cannot be referenced in an engineering tool during the automatic hardware test.

Operating procedure

1. Select "Automatic hardware test" in "Basic Settings" ⇨ "Various Operations Settings" ⇨ "Mode Settings" for an OPC UA server module in an engineering tool.

2. Disconnect a cable if it is connected to a 1000BASE-T/100BASE-TX/10BASE-T interface.

3. Remove an SD memory card if it is inserted.

4. Set the CPU module to the STOP state, and write the parameters.

5. Reset the CPU module.
After it is reset, the automatic hardware test is performed automatically. The LED display for diagnosis is as follows:

Status		RUN LED status	ERR LED status	Dot matrix LED status
Diagnosing		ON	OFF	"H.T." (Flashing)
Complete diagnosing	Normal completion	ON	OFF	"OK" (ON)
	Abnormal completion	ON	ON	"ERR" (ON)

6. When the test is completed normally, return the mode setting changed in step 1 to "Online" and reset the CPU module.

7. When the test is completed abnormally, check if measures are taken to reduce noise of the system, and perform the test again. If it is completed abnormally again, a hardware failure may occur in the OPC UA server module. Please contact your local Mitsubishi Electric sales office or representative.
Do not use an electric screwdriver when removing the module. Loose the module fixing screws completely to remove the module.

Hardware test for LED check

The following explains the LED hardware diagnostic of an OPC UA server module. For the diagnostic, the LED of an OPC UA server module needs to be turned ON.

> **Restriction** ✋
>
> The values in the buffer memory cannot be referenced in an engineering tool during the hardware test for LED check.

Operating procedure

1. Select "Hardware test for LED check" in "Basic Settings" ⇨ "Various Operations Settings" ⇨ "Mode Settings" for an OPC UA server module in an engineering tool.

2. Set the CPU module to the STOP state, and write the parameters.

3. Reset the CPU module.

After it is reset, the hardware test for LED check is performed automatically. When the following contents are displayed, check them visually for any errors.

LED name	Display color	Display status
RUN	Green	ON
ERR	Red	ON
OPR	Green	ON
CARD RDY	Green	ON
CARD ACS	Green	ON
Dot matrix LED	Orange	☞ Page 97 Patterns for dot matrix LED check

Since the LED under the OPR LED is used for the system, the test is performed as well as other LEDs. (Display color: green, display status: ON)

4. When the test is completed normally, change the mode set in the step 1 back to "Online," and reset the CPU module.

5. When the test is completed abnormally (when any color or status is different from the one shown in the table above), check if measures are taken to reduce noise of the system, and perform the test again. If it is completed abnormally again, a hardware failure may occur in the OPC UA server module. Please contact your local Mitsubishi Electric sales office or representative.

Do not use an electric screwdriver when removing the module. Loose the module fixing screws completely to remove the module.

■Patterns for dot matrix LED check

Test patterns are turned ON in turn on the dot matrix LED.

The pattern switches every one second.

□: ON, ▣: OFF
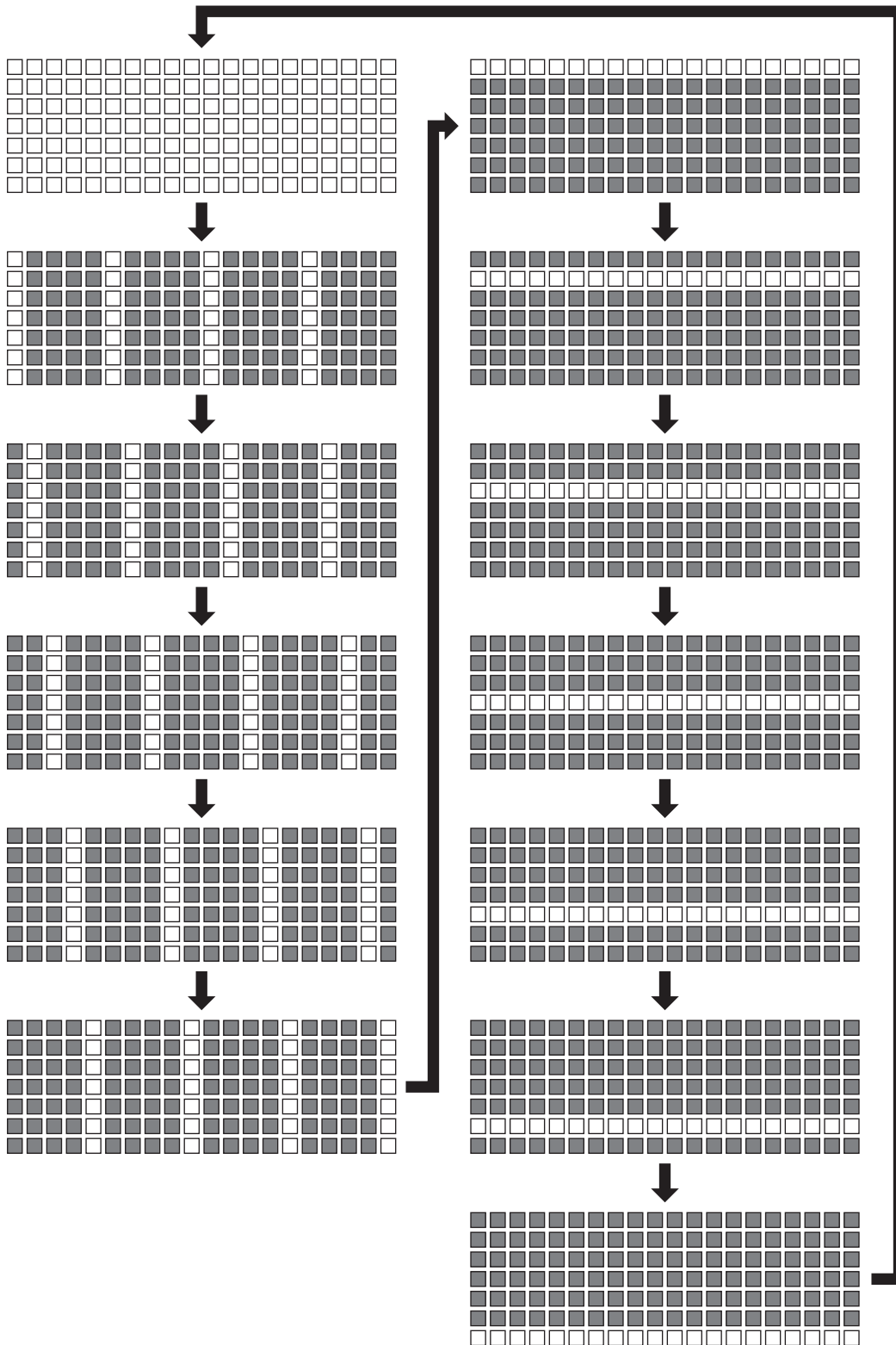
4.3   Troubleshooting by Symptom

Troubleshooting on the configuration tool

| Symptom	Check point	Corrective action
Unable to connect the configuration tool to the OPC UA server module.	Is there any disconnection in the connection route?	• Connect the cables properly.
	Is the IP address specified in the connection destination setting correct?	• Review the IP address setting.
	Are the following correct: the user authentication, user name, and password specified in the connection destination setting?	• Review the user authentication setting, the user name, and the password.
	Is the IP address duplicated?	• Review the IP address setting.
	Is there a firewall and/or a proxy server in the connection route?	• Consult your network administrator about the firewall setting and/or the setting contents of the proxy server.
	Is the direct connection set in the connection destination setting?	Software with a firewall function that restricts communication of the configuration tool may be installed on a personal computer. For using security software with a firewall function, take either of the following corrective actions: • Refer to the manual for the software to allow the communication of the configuration tool. • Set the connection method to the connection via a hub in the connection destination setting.
	Is the "Online" is selected for the mode setting of RD81OPC96?	• Select "Online" for the mode setting in an engineering tool.
	Is there any problem on the personal computer?	• Replace it with another computer.
	Is it connected directly using the Ethernet (CH2)?	• Connect it directly using the Ethernet (CH1). • When using the Ethernet (CH2), connect it via a hub.
	Is it connected to the Ethernet port which is not selected to use in the network setting?	• Connect to the Ethernet port which is selected to use in the network setting. • Enable the setting of the connected Ethernet port.
	Are multiple IP addresses enabled on the personal computer side at the same time?	• When using direct connection, review the network setting so that multiple IP addresses are not enabled on the personal computer. • Disable the wireless LAN.
	Was an attempt made to connect directly via a hub?	• When using direct connection, connect the OPC UA server module (CH1) to the personal computer on a 1:1 basis.
	Is the checkbox of "Use the User Authentication" unselected in the connection destination setting at the first startup of an OPC UA server module?	• At the first startup of an OPC UA server module, select the checkbox of "Use the User Authentication" in the connection destination setting, and enter the default user name and password to connect. For details, refer to 'PROCEDURE FOR OPERATION' in the following: (MELSEC iQ-R OPC UA Server Module User's Manual (Startup))
	Is any one of the following input signals OFF? • Module READY (X0) • OPC UA server status (X1) • Ethernet port status (X5)	• Wait for the input signal to turn ON.
	Has a setting file error (error code: 1C10H) occurred?	❶ Use the latest version of the configuration tool. ❷ Access the OPC UA server module as the default user. ❸ Delete the settings of the functions that are not supported by the firmware version of the OPC UA server module, and write the settings again. (☞ Page 169 Added and Changed Functions)
	Has a setting file error (error code: 1C12H) occurred?	❶ Use the latest version of the configuration tool. ❷ Access the OPC UA server module as the default user. ❸ Review the security setting, and write the setting again. (☞ Page 55 Security Setting)

Symptom	Check point	Corrective action
Unable to open the project file.	Is an old version of the configuration tool used?	• Use the latest version of the configuration tool.
	Is a file which has the extension other than '.mxcfg' specified?	• Specify a file which has the '.mxcfg' extension.
	Is the specified project file corrupted?	• Specify another project file.
Unable to read the data from the OPC UA server module or display the information of the OPC UA server module.	Is a project file in the module corrupted?	• Replace the SD memory card with another one. • Format the SD memory card in the SD memory card diagnostic of the configuration tool.
The verification result is mismatched between the configuration tool and an OPC UA server module to which the same setting as one set in the configuration tool is written.	Is the setting verified in a configuration tool with version '1.00A'?	• Update the configuration tool to the latest version before verification.
	Is the setting verified by using a project file for which the following operation was performed? • Opening and saving a project file, which was saved in a configuration tool with version '1.07H' or later, in version '1.06G' or earlier	• The security policy setting may have been changed. Review them. (☞ Page 60 Security policy compatibility)
	Is the setting verified in a configuration tool with software version '1.09K' or later for a module to which the setting is written in software version '1.08J' or earlier?	■For the firmware version '10' or later • Read the setting from the OPC UA server module and write (read/write) it to the module again before verification. ■For the firmware version '04' to '09' • Update the OPC UA server module to the latest version and read/write the setting before verification. ■For the firmware version '03' or earlier • Please contact your local Mitsubishi Electric sales office or representative.
An error or warning occurs when importing a CSV file.	Is there a log file in the folder storing the CSV file to be imported?	• Check the log file and take corrective action. (☞ Page 157 Warning/error log file when importing a CSV file)

Troubleshooting on LED indication and I/O signals

Symptom	Check point	Corrective action
The RUN LED does not turn ON.	Is the module in preparation?	• Wait for the startup of the OPC UA server module to complete. (It may take several minutes for the RUN LED to turn ON depending on the system configuration.)
	Is 'Module READY' (X0) OFF?	• There may be a watchdog timer error. Please contact your local Mitsubishi Electric sales office or representative.
	Is "Online(Asynchronous Mode)" selected for the mode setting of an OPC UA server module with firmware version '01'?	• Change the mode setting to "Online." (☞ Page 90 Various operation settings) • Use an OPC UA server module with firmware version '02' or later.
	Does the system configuration satisfy both of the following conditions? • The module is used with a recorder module (RD81RC96), camera recorder module (RD81RC96-CA), MES interface module (RD81MES96N), or C intelligent function module (RD55UP12-V) in the system. • "Online (Asynchronous Mode)" is selected for the mode setting.	• Change the mode setting to "Online." (☞ Page 90 Various operation settings)
The RUN LED is flashing.	Is the module selected as the target for online module change?	• Turn ON the module selection cancel request flag (SM1615).
The RUN LED is OFF.	Is the module ready to be exchanged in the process of online module change?	• Perform the online module change function. For details, refer to the following: (📖MELSEC iQ-R Online Module Change Manual)
The ERR LED is ON or flashing.	Is any of the input signals (X10 to X14) ON?	• According to the error code stored by the error detection shown on the left side, check the error description and take a corrective action. (☞ Page 104 Error Code List)
	Check the error code in the system monitor of an engineering tool.	• By the error code, check the error description and take a corrective action. (☞ Page 104 Error Code List)
'Module READY' (X0) does not turn ON, or it takes time to turn ON.	Is the module in preparation?	• Wait for the startup of the OPC UA server module to complete. (It may take several minutes for 'Module READY' (X0) to turn ON depending on the number of access target device settings.)
	Is an SD memory card containing unnecessary files used?	• Format the SD memory card in the SD memory card diagnostic of the configuration tool, and write the setting to use.
	Is the RUN LED turned OFF?	• There may be a watchdog timer error. Please contact your local Mitsubishi Electric sales office or representative.
'OPC UA server status' (X1) does not turn ON or takes time to turn ON.	Does a related data updating start (event code: 24000) occur in the system monitor ⇨ [Event History] of an engineering tool?	• Open the setting used for the OPC UA server module in the configuration tool, specify a GX Works3 project used for the CPU module, and update data related to global labels. (☞ Page 73 Updating data related to global labels) Then, write the setting to the OPC UA server module and update the setting. (It takes time to update related data every time the OPC UA server module starts and the setting is updated because global labels written to the CPU module differ from those in the setting of the OPC UA server module.)
The contents of the dot matrix LED display cannot be switched even though the dot matrix LED display mode switch (SELECT/MODE/SHOW switch) is operated.	Is the contents of SELECT/MODE/SHOW switch item blank in [Module Diagnostics] ⇨ [Module Information List] of the engineering tool?	• The dot matrix LED display mode switch (SELECT/MODE/SHOW switch) may have a failure. Please contact your local Mitsubishi Electric sales office or representative.

Troubleshooting on network connection

Symptom	Check point	Corrective action
Unable to access the OPC UA server module.	Is an Ethernet cable connected to CH1 or CH2?	• Connect an Ethernet cable to CH1 or CH2.
	Is there any disconnection in the connection route?	• Connect the cables properly.
	Is the IP address duplicated in other devices on the network?	• Review the IP address setting.
	Is there any problem in the network setting of the personal computer?	• Check the network setting of the personal computer.
	Is it connected directly using the Ethernet (CH2)?	• Connect it directly using the Ethernet (CH1). • When using the Ethernet (CH2), connect it via a hub.
	Is it connected to the Ethernet port which is not selected to use in the network setting?	• Connect to the Ethernet port which is selected to use in the network setting. • Enable the setting of the connected Ethernet port.
	Are multiple IP addresses enabled on the personal computer side at the same time?	• When using direct connection, review the network setting so that multiple IP addresses are not enabled on the personal computer. • Disable the wireless LAN.
	Was an attempt made to connect directly via a hub?	• When using direct connection, connect the OPC UA server module (CH1) to the personal computer on a 1:1 basis.
	Is any one of the following input signals OFF? • Module READY (X0) • OPC UA server status (X1) • Ethernet port status (X5)	• Wait for the input signal to turn ON.

Troubleshooting on access target device communication

Symptom	Check point	Corrective action
Unable to communicate with a specified access target device.	Is there any device for which the remote password setting is enabled on the communication route with an access target device if a response timeout error (error code: 1824H) is notified?	• Disable the remote password setting. • Unlock the remote password.
	Is there any device for which the same IP address is set on the same network when communicating with an access target device via the Ethernet route?	• Do not use the device to which the same IP address is set on the same network. • Set the IP address to devices without duplication.

Troubleshooting on connection with an OPC UA client

Symptom	Check point	Corrective action
Unable to connect from an OPC UA client to an OPC UA server module.	Has an error occurred in the OPC UA client?	• If an error occurs, check the error and take a corrective action.
	Is the setting of the connection destination OPC UA server of the OPC UA client correct?	• Review the setting of the connection destination OPC UA server of the OPC UA client.
	Is there any device to which the same IP address is set on the same network?	• Do not use the device to which the same IP address is set on the same network. • Set the IP address to devices without duplication.
	Are the security settings of the OPC UA server module and the OPC UA client correct?	• Review the security settings of the OPC UA server module and the OPC UA client.
	Are the following security policies set in the OPC UA server setting? • Basic128Rsa15 • Basic256	For the firmware version '06' or '07,' an OPC UA server operates as if "Basic256Sha256" were selected for the security policy (☞ Page 59 OPC UA Server Setting). Perform either of the following operations: • Select "Basic256Sha256" for the security policy for the OPC UA client. • Use an OPC UA server module with firmware version '05' or earlier, or '08' or later.
	Are the expiration dates of the server certificate and the client certificate correct?	• Download the server certificate and the client certificate, then check their expiration dates and take corrective action. For details on the expiration date, refer to the following: (📖 MELSEC iQ-R OPC UA Server Module User's Manual (Startup))
	Is it connected using the Ethernet (CH2)?	• Connect it using the Ethernet (CH1).
	Is any one of the following input signals OFF? • Module READY (X0) • OPC UA server status (X1) • Ethernet port status (X5)	• Wait for the input signal to turn ON.
It takes time or a timeout occurs when connecting from an OPC UA client to an OPC UA server module.	Is the number of certificates uploaded to "Trust List" in the "Manage Application Certificate" screen 100 or less[1]?	• Delete an unnecessary certificate from "Trust List."
	Is the number of certificates uploaded to "Trust List" in the "Manage User Certificate" screen 100 or less[1] when authenticating a user with a certificate?	• Delete an unnecessary certificate from "Trust List."
The list of denied certificates is not updated when connecting from an OPC UA client to an OPC UA server module.	• Is the number of certificates stored in "Denied Certificate List" in the "Manage User Certificate" screen 100 or less? • Is the number of certificates stored in "Denied Certificate List" in the "Manage Application Certificate" screen 100 or less?	• Delete an unnecessary certificate from "Denied Certificate List." • Perform the following procedure. ❶ Download a certificate to trust from "Denied Certificate List." ❷ Upload it to "Trust List." ❸ Delete the certificate from "Denied Certificate List."
A tag value in the address space is not updated.	Has an error occurred in the module of the target tag?	• If an error occurs, check the error and take a corrective action.
	Is the polling cycle setting of the OPC UA server module correct?	• Review the polling cycle setting of the OPC UA server module.
A value of the OPC UA client is not applied to a tag of the address space.	Has an error occurred in the module of the target tag?	• If an error occurs, check the error and take a corrective action.
	Was the relevant device value manipulated in the CPU module?	• Do not manipulate the device value in the CPU module at the timing of operating from the OPC UA client.
Some tags cannot be accessed from an OPC UA client.	Are the data types of these tags 'Not Assigned'?	• Specify their data types. (☞ Page 35 Tag) (A CSV file may have been imported without specifying their data types.)

Symptom	Check point	Corrective action
• Multidimensional array elements cannot be accessed. • A value written to a multidimensional array element is not applied to a device or global label. • A value read from a multidimensional array element differs from one in a device or global label.	Is the firmware version of an OPC UA server module '08' or earlier, or the software version of the configuration tool '1.07H' or earlier?	■For the firmware version '04' to '08' or the software version '1.07H' or earlier Update the firmware version to '09' or later and the software version to '1.08J' or later. Then, unselect the checkbox of "Reverse the dimensional order of multidimensional arrays" in [Tool] ⇨ [OPC UA Server Setting] ⇨ the [Operation Setting] tab of the configuration tool. (☞ Page 62 [Operation Setting] tab) ■For the firmware version '03' or earlier Reverse the dimensional order of multidimensional arrays and specify an element. (Example: Two-dimensional array) When accessing an element with "3" in the first dimension and "5" in the second dimension, specify "5" for the first dimension and "3" for the second dimension in an OPC UA client. (Example: Three-dimensional array) When accessing an element with "3" in the first dimension, "5" in the second dimension, and "7" in the third dimension, specify "7" for the first dimension, "5" for the second dimension, and "3" for the third dimension in an OPC UA client.
	Is the checkbox of "Reverse the dimensional order of multidimensional arrays" selected in [Tool] ⇨ [OPC UA Server Setting] ⇨ the [Operation Setting] tab of the configuration tool?[2]	• Unselect the checkbox. (☞ Page 62 [Operation Setting] tab)
	Is the firmware version of an OPC UA server module '09' or later, and the software version of the configuration tool '1.08J' or later?	• The dimensional order of multidimensional arrays for an OPC UA server module differs for each firmware version. To set the same order as a firmware version '08' or earlier, select the checkbox of "Reverse the dimensional order of multidimensional arrays" in [Tool] ⇨ [OPC UA Server Setting] ⇨ the [Operation Setting] tab of the configuration tool. (☞ Page 62 [Operation Setting] tab) For details on the dimensional order specifications, refer to the following: (☐MELSEC iQ-R OPC UA Server Module User's Manual (Startup))

*1 A reference for reducing the connection time
*2 This setting is unavailable for an OPC UA server module with firmware version '08' or earlier or the configuration tool with software version '1.07H' or earlier.

Troubleshooting on an SD memory card

Symptom	Check point	Corrective action
Settings were erased while the power was OFF	Is there a problem with the type of SD memory card?	• Replace the SD memory card with an available one. ☐MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
	Was the power turned OFF or the control CPU reset during writing to the SD memory card?	• Do not turn the power OFF or reset the control CPU during writing to the SD memory card.
Unable to recognize the SD memory card.	Is the SD memory card inserted correctly?	• Remove the SD memory card once, and insert it again.
	Was the power turned OFF or the control CPU reset during writing to the SD memory card?	• Do not turn the power OFF or reset the control CPU during writing to the SD memory card. • Format the SD memory card in the configuration tool.

4.4 Error Code List

This section shows the error code list.

If a system error occurs, please contact your local Mitsubishi Electric sales office or representative.

Error code	Error name	Error description	Corrective action
1800H	Unsupported device error	A device unsupported by OPC UA Server module exists on the access route.	• Review the device on the access route.
1801H to 1802H	Incorrect access target error	Incorrect setting values in the [Communication Settings].	• Review the settings in the [Communication Settings].
1803H	Incorrect access target error	A device/access route unsupported by OPC UA Server module is set in the [Communication Settings].	• Review the settings in the [Communication Settings]. • Check if there is any problem on the route to the target device.
1804H	Incorrect access target error	A device unsupported by OPC UA Server module is set in the [Communication Settings].	• Review the settings in the [Communication Settings].
1805H	Incorrect access target error	A non-accessible device is set in the [Communication Settings].	• Review the settings in the [Communication Settings].
1806H	Device memory type error	A non-existent device memory type is specified. (Or the size of device memory exceeds the applicable range.)	• Review the device memory type entered in the [Address space(Tag)].
1807H	Device memory No. error	A non-existent device memory No. is specified.	• Review the device memory number entered in the [Address space(Tag)].
1808H	Target device communication error	An error has occurred when accessing the target device.	• Check if the settings in the [Communication Settings] are correct. • Check the status of the target device. • Check if the route to the target device is correct. • Check if there is any problem on the route to the target device.
1809H	Data receive error	Failed to receive the data.	• Review the device on the access route.
180AH	Size error	The device size exceeded the device range.	• Review the device memory number entered in the [Address space(Tag)].
180BH	Block error	The block No. of the specified extension file register is invalid.	• Check the block No. of the extension file register (device type).
180CH	Data receive error	Failed to receive the data.	• Review the device on the access route.
180DH	Write protect error	The block No. of the specified extension file register has been allocated to the write-protect area of the memory cassette.	• Check the block No. of the extension file register (device type). • Check the write-protect DIP switch on the memory cassette of the target device.
180EH	Incorrect access target device error	The device type set in the [Communication Settings] is different from the one of the actual target device.	• Review the settings in the [Communication Settings].
180FH	Incorrect access target error	Incorrect station No. is specified in the [Communication Settings].	• Review the settings in the [Communication Settings].
1810H	ROM operation error	Writing a TC setting value was attempted to the programmable controller CPU that was running the ROM.	• Change the TC setting value during RAM operation.
1811H	Incorrect target device settings error (Start I/O No.)	Incorrect start I/O No. is specified in the [Communication Settings].	• Review the settings (start I/O No.) of the [Communication Settings]. • Check the configuration of the target device (start I/O No.).
1812H to 1813H	Data receive error	Failed to receive the data.	• Review the device on the access route.
1814H	Incorrect target device settings error (IP address)	Incorrect IP address is specified in the [Communication Settings].	• Review the settings (IP address) in the [Communication Settings]. • Check the configuration of the target device (IP address).
1815H to 1816H	Target device communication reception data error	Incorrect data received from the target device.	• Review the settings in the [Communication Settings]. • Check the communication cable status and Access target device status.
1817H	Unsupported device error	A device unsupported by OPC UA Server module exists on the access route.	• Review the device on the access route.

Error code	Error name	Error description	Corrective action
1818H	Data receive error	Multiple responses were received at Ethernet direct communication.	• Check if the direct connection with the module is configured on a 1:1 basis.
1819H	Incorrect target device status error	Unable to set. The OPC UA Server module is communicating with other devices at Ethernet direct communication.	• Check if the direct connection with the module is configured on a 1:1 basis.
181AH	Incorrect target device settings error (Station No./Network No.)	Incorrect Station No./Network No. are specified in the [Communication Settings].	• Review the settings (Station No./Network No.) in the [Communication Settings]. • Check the configuration of the target device (Station No./Network No.).
181BH	Target device communication connection error (IP address)	Incorrect IP address is specified in the [Communication Settings].	• Review the settings (IP address) in the [Communication Settings]. • Check the configuration of the target device (IP address).
181CH	Target device communication time-out error	No response from the target device.	• Check the status of the target device. • Review the settings in the [Communication Settings]. • Adjust the time-out setting.
181DH to 181FH	Data send error	Failed to send the data.	• Review the device on the access route.
1820H to 1823H	Data receive error	Failed to receive the data.	• Review the device on the access route.
1824H	Response time-out error	No response has been received from the other station.	• Check the communication cable status and Access target device status. • Review the time-out setting. • Review the routing parameter set for the CPU(s) on the access route. • Review the control CPU(s) of the network module(s) on the access route to the Access target device module. • Review if the access target PLC series is supported. • Check the configuration of the target device.
18FEH	Target device communication error	An error has occurred when accessing the target device.	• Check if the settings in the [Communication Settings] are correct. • Check the status of the target device. • Check if the route to the target device is correct. • Check if there is any problem on the route to the target device.
18FFH to 1900H	System error	—	—
1904H	Errors detected in the CPU module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of the CPU module. • Check the global label-related data update function in the user's manual of OPC UA Server module when the device-unassigned global labels are in use.
1907H	Errors detected in the serial communication module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of the serial communication module.
190BH	Errors detected in the CC-Link module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of CC-Link module.
190CH	Errors detected in the Ethernet-equipped module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and refer to the user's manual of the Ethernet-equipped module and check the errors displayed in the source error code.
190DH	Errors detected in the CC-Link IE Field Network module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of CC-Link IE Field Network module.
190EH	Errors detected in the CC-Link IE Controller Network module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of CC-Link IE Controller Network module.

4

Error code	Error name	Error description	Corrective action
190FH	Errors detected in the MELSECNET/H network module	—	• Check the source error code displayed on the error detailed information of the engineering tool, and check it in the user's manual of MELSECNET/H network module.
1920H	Global label mismatch error	The global label written to the CPU module is different from the OPC UA Server module setting.	• Open the setting running in OPC UA Server module with the configuration tool and update data related to global label after specifying the GX Works3 project running in CPU module. After that, write the setting to OPC UA Server module and update setting.
1921H	Global label unavailable error	Attempted to access a global label that is not written to the CPU module or is not available.	• Check "Access from External Device" in the global label setting of GX Works3. • Change "Class" to other than "VAR_GLOBAL_CONSTANT" in the global label setting of GX Works3. • Write "Global Label Setting" and "Global Label Assignment Information" to the CPU module. • Update data related to global label with the configuration tool. After that, write the setting to OPC UA Server module and update setting. • If a device is allocated to a structure-type global label has structure-type member, unselect "Update data related global label from the OPC UA server module" in the configuration tool.
1990H	System error	—	—
19E0H	CH1/CH2 address specified in the fourth octet setting error	The value set in the CH1/CH2 address specified in the fourth octet is out of range.	• Check if the value of 1-254 is set to the CH1/CH2 address specified in the fourth octet.
1A00H	Data type unavailable error	Data type of label and the DataType of Variable are mapped in a combination that cannot be used.	• Review mapped labels using the configuration tool and write/update setting to the OPC UA Server module. • Review data type of label using the GX Works3, write to the CPU module and update setting to the OPC UA Server module using the configuration tool.
1A01H	Data conversion error	The label value read from the CPU module is outside the range of the mapped Variable.	• Review the mapped labels using the configuration tool and write/update setting to the OPC UA Server module. • Review data type of label using the GX Works3 and write to the CPU module. • Write a value in the range from the GX Works3 to the target label. • Write a valid value to the target Variable from OPC UA client.
1A10H	Project file (not supported version)	The project file version is not supported.	• Upgrade to the latest version of OPC UA Server module.
1A11H	Project file (load error)	Failed to load the project file written to the module. The following are possible causes. • The file is incorrect. • The file is corrupted. • SD memory card hardware error.	• Retry writing to the OPC UA Server module from the configuration tool. • Replace the SD memory card.
1A20H	Information model file (not supported version)	The information model file version is not supported.	• Upgrade to the latest version of OPC UA Server module.
1A21H	Information model file (load error)	Failed to load the information model file written to the module. The following are possible causes. • The file is incorrect. • The file is corrupted. • SD memory card hardware error.	• Retry writing to the OPC UA Server module from the configuration tool. • Replace the SD memory card.
1A22H	Information model file (No file)	The required information model file cannot be found.	• Retry writing to the OPC UA Server module from the configuration tool.
1A30H	Information model file (extension load error)	Failed to load the information model file written to the module. The following are possible causes. • The extension format is incorrect. • The extension format version is not supported. • The file is incorrect. • The file is corrupted. • SD memory card hardware error.	• Retry writing to the OPC UA Server module from the configuration tool. • Upgrade to the latest version of OPC UA Server module. • Replace the SD memory card.

Error code	Error name	Error description	Corrective action
1C00H	OPC UA Server function starting error	Failed to startup OPC UA Server function.	• Please review the OPC UA server setting with configuration tool and refresh the configuration file.
1C01H	Plug-in file error	Failed to find Plug-in file.	• Please consult your local Mitsubishi representative.
1C02H	Setting file error	Failed to find setting file.	• Please consult your local Mitsubishi representative.
1C10H	Setting file error	Failed to load file information in setting file.	• Check the version of the configuration tool matches the version of the module. • Check the matching version in Added and Changed Functions of the user's manual of OPC UA Server module. ■Also check the following when the OPC UA server module version is "10" or later. • Please upgrade to the latest version of configuration tool and read from OPC UA server module, and then write again. ■Also check the following when the OPC UA server module version is "04" to "09". • Upgrade to the latest version of OPC UA Server module. ■Also check the following when the OPC UA server module version is "03" or earlier. • Please consult your local Mitsubishi representative.
1C11H	Setting file error	Failed to find system setting in setting file.	• Please consult your local Mitsubishi representative.
1C12H	Setting file error	Failed to load security setting in setting file.	• Please review the security setting with configuration tool and refresh the configuration file.
1C13H	Setting file error	Failed to load network setting in setting file.	• Please review the Network setting with configuration tool and refresh the configuration file.
1C14H	Setting file error	Failed to load OPC UA Server setting in setting file.	• Please review the OPC UA server setting with configuration tool and refresh the configuration file.
1C16H	Setting file error	Failed to find target device setting in setting file.	• Please consult your local Mitsubishi representative.
1C17H	Setting file error	Failed to load target device setting in setting file.	• Please review the Address space setting with configuration tool and refresh the configuration file. • Please confirm the number of groups did not exceed the upper limit (10000).
1C1AH	Setting file error	Failed to find definition setting in setting file.	• Please consult your local Mitsubishi representative.
1C1BH	Setting file error	Failed to load polling method definition in setting file.	• Please review the Polling Method Definitions with configuration tool and refresh the configuration file.
1C1CH	Setting file error	Failed to load conversion definition in setting file.	• Please review the Conversion definitions with configuration tool and refresh the configuration file.
1F20H	Error log output error	No SD memory card has been installed or failed to write the log file.	• Install the SD memory card. • Replace the SD memory card. • Slide the write protect switch to unlock the SD memory card (remove the write-protect) when the switch is in the lock position (protecting data writing).
1F21H	Log information error	The log information is corrupted. Restored by deleting the previous information.	• Check the SD memory card.
1F43H	Setting file writing error	Failed to write the setting file.	• Retry the writing of the settings with configuration tool.
2121H	SD Memory card error	An error has been detected in the SD memory card.	• Format the SD memory card. • Reinsert the SD memory card. • Check the SD memory card. • Replace the SD memory card if it is damaged.

Error code	Error name	Error description	Corrective action
2440H	Module major error	In the multiple CPU system, the control CPU setting in the system parameters is different from that of other numbered CPU modules. An error has been detected in the I/O module or intelligent function module during the initial processing.	• Review the system parameters of the second or higher numbered CPU modules and match them with those of the smallest numbered CPU module. • The possible cause is a hardware failure of the error module. Please consult your local Mitsubishi representative.
2450H	Module major error	A major error has been detected from the I/O module or intelligent function module.	• Check the connection status of the extension cable. • Check if the I/O module or intelligent function module is mounted correctly. • Reset the CPU module and switch it to RUN. If the same error is displayed again, a hardware failure may occur in the module. Please consult your local Mitsubishi representative.
24C0H to 24C1H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the CPU module, base unit, extension cable, or module (I/O module or intelligent function module) connected. Please consult your local Mitsubishi representative.
24C2H	System bus error	An error was detected on the system bus.	• Check the connection status of the extension cable. • Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the CPU module, base unit, extension cable, or module (I/O module or intelligent function module) connected. Please consult your local Mitsubishi representative.
24C3H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the CPU module, base unit, extension cable, or module (I/O module or intelligent function module) connected. Please consult your local Mitsubishi representative.
24C4H to 24C5H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the base unit, extension cable, or module (I/O module or intelligent function module) connected. Please consult your local Mitsubishi representative.
24C6H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the CPU module or extension cable. Please consult your local Mitsubishi representative.
24C8H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the extension cable, or module (I/O module or intelligent function module) connected. Please consult your local Mitsubishi representative.
24E0H	System bus error	An error was detected on the system bus.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the CPU module or base unit. Please consult your local Mitsubishi representative.
2701H to 270AH	System error	—	—

Error code	Error name	Error description	Corrective action
3030H	Access target device setting error	Incorrect settings in the [Communication Settings]	• Review the settings in the [Communication Settings].
3060H	System error	—	—
3061H	Global label access error	Failed to access to global labels.	• Reset the CPU module and switch it to RUN after writing "Global Label Setting" and "Global Label Assignment Information" to the CPU module. If the same error is displayed again, please consult your local Mitsubishi representative.
30A1H	System error	—	—
30B0H	SD memory card eject error	SD memory card has been ejected without stopping file access.	• Install the SD memory card and update setting.
30B1H	SD memory card format error	Failed to format the SD memory card.	• Check if the SD memory card is inserted firmly. • Check if an error has occurred in the SD memory card. • Slide the write protect switch to unlock the SD memory card (remove the write-protect) when the switch is in the lock position (protecting data writing).
30B2H	SD memory card mount error	Failed to install the SD memory card.	• Check if the SD memory card is inserted firmly. • Replace the SD memory card. • Slide the write protect switch to unlock the SD memory card (remove the write-protect) when the switch is in the lock position (protecting data writing).
30B3H	No SD memory card installed	OPC UA Server module has been started without installing the SD memory card.	• Check if the SD memory card is inserted firmly. • Install the SD memory card.
30B4H	System error	—	—
30C0H	System error	—	—
30D1H to 30D2H	System error	—	—
30D3H	Target device communication error	An error has occurred when accessing the target device.	• Check if the settings in the [Communication Settings] are correct. • Check the status of the target device. • Check if the route to the target device is correct. • Check if there is any problem on the route to the target device.
30E0H	System error	—	—
3100H	System error	—	—
3110H	System error	—	—
3120H	System error	—	—
3130H	System error	—	—
3880H	System error	—	—
3881H	SD memory card access error	Failed to access the SD memory card.	• Check the SD memory card. • Replace the SD memory card if it is damaged. • Check if the SD memory card had been used in other applications. • Slide the write protect switch to unlock the SD memory card (remove the write-protect) when the switch is in the lock position (protecting data writing). • Check if the connectable SD memory card is used.
3882H	SD memory card error	Unable to operate in this module. The settings for a new version of OPC UA Server module is written in the SD memory card.	• Format the SD memory card and retry the writing of the settings with configuration tool.
3920H	System error	—	—
3921H	SD memory card access error	Failed to access the SD memory card.	• Check the SD memory card. • Replace the SD memory card if it is damaged. • Check if the SD memory card had been used in other applications. • Slide the write protect switch to unlock the SD memory card (remove the write-protect) when the switch is in the lock position (protecting data writing).

Error code	Error name	Error description	Corrective action
3940H	System error	—	—
3944H to 3948H	System error	—	—
3980H	System error	—	—
3C00H to 3C03H	Hardware failure	A hardware failure has been detected.	• Take measures to reduce noise. • Reset the CPU module and switch it to RUN. If the same error is displayed again, a hardware failure may occur in OPC UA Server module. Please consult your local Mitsubishi representative.
3C0FH	Hardware failure	A hardware failure has been detected.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the OPC UA Server module. Please consult your local Mitsubishi representative.
3C22H	Memory error	An error has been detected in the memory.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the OPC UA Server module. Please consult your local Mitsubishi representative.
3C2FH	Memory error	An error has been detected in the memory.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the OPC UA Server module. Please consult your local Mitsubishi representative.
3C32H	Memory error	An error has been detected in the memory.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the OPC UA Server module. Please consult your local Mitsubishi representative.
3F01H to 3F05H	Memory error	An error has been detected in the memory.	• Take measures to reduce noise. • Reset the CPU module, and run it again. If the same error code is displayed again, the possible cause is a hardware failure of the OPC UA Server module. Please consult your local Mitsubishi representative.

4.5 Event Code List

This section shows the event code list.

Event code	Event type	Overview	Cause
20400	Operation	Firmware update completed successfully (intelligent function module)	The firmware of the Intelligent Function Module was successfully updated.
20401	Operation	Firmware update failed (Intelligent Function Module)	The firmware update of the Intelligent Function Module failed.
24000	Operation	Related data updating start	Started to update data related to global label.
24001	Operation	Related data updating finish	Finished to update data related to global label.
24002	Operation	Label CRC matched	Data related to global labels matched between the CPU module and the OPC UA Server module.
24003	Operation	Related data updating failure	Failed to update data related to global label.

4

APPENDIX

Appendix 1 Module Labels

This section shows the module labels used to set the input/output signals and buffer memory of an OPC UA server module.

Module label configuration

The name of a module label is defined in the following configurations:

"Instance name"_"Module number"."Label name"

"Instance name"_"Module number"."Label name"_D

> **Ex.**
> OPC96_1.bSts_ModuleREADY

■Instance name

The instance name of an OPC UA server module (RD81OPC96) is 'OPC96.'

■Module number

A module number is a number starting from 1, which is added to identify a module that has the same instance name.

■Label name

This is a module unique label name.

■_D

This indicates that the module label is for direct access. Without this symbol, it means a label for refresh. There are some differences between refresh and direct access as shown below.

Type	Description	Access timing
Refresh	Values written to/read from a module label are applied to a module in a batch at the time of refresh. This shortens the program execution time.	At the time of refresh
Direct access	Values written to/read from a module label are immediately applied to a module. Although the program execution time is longer than refresh, the responsiveness will be increased.	At the time of writing to/reading from a module label

Appendix 2 Input/Output Signals

This section explains the input/output signals of an OPC UA server module.

The following shows an example of assigning input/output signals when the start input/output number of an OPC UA server module is '0.'

A device X indicates an input signal from an OPC UA server module to a CPU module.

A device Y indicates an output signal from a CPU module to an OPC UA server module.

Precautions

As for input/output signals to a CPU module, do not output (turn ON) 'Use prohibited' signals.

Doing so may cause malfunction of a programmable controller system.

Input/output signal list

The following shows the input/output signal list of an OPC UA server module.

For details on the input/output signals, refer to the following:

Input signals

Device No.	Signal name
X0	Module READY
X1	OPC UA server status
X2	Use prohibited
X3	File access status
X4	Use prohibited
X5	Ethernet port status
X6	Use prohibited
X7	Connection status
X8 to XF	Use prohibited
X10	Module stop error status
X11	Module continuation error status
X12 to X13	Use prohibited
X14	Target device error
X15 to X1F	Use prohibited

Output signals

Device No.	Signal name
Y0	Use prohibited
Y1	OPC UA server resume request
Y2	OPC UA server pause request
Y3	File access stop request
Y4	File access stop cancellation request
Y5 to YF	Use prohibited
Y10	Error clear request
Y11 to Y1F	Use prohibited

Input signal details

The following shows the details on the input signals from an OPC UA server module to a CPU module.

Module READY (X0)

This signal turns ON when OPC UA server module becomes ready after the programmable controller is powered ON from OFF or the CPU module is reset.

It turns OFF when a watchdog timer error occurs.

Do not access the buffer memory and perform online operations from configuration tool until the OPC UA server module is in READY status.

OPC UA server status (X1)

● This signal turns ON when an OPC UA server module is in operation.

It indicates that the processing of an OPC UA server module is executable.

● This signal turns OFF when an OPC UA server module is stopped.

An OPC UA server module stops in the following cases:

- The period after a programmable controller is powered OFF and ON or a CPU module is reset until an OPC UA server module is started
- A server operation is stopped in the configuration tool. (☞ Page 81 Stop of an OPC UA server module)
- A module stop error occurs in an OPC UA server module.
- While updating the settings
- While file access is stopped (☐MELSEC iQ-R OPC UA Server Module User's Manual (Startup))
- While updating data related to global labels (☞ Page 23 Global label-related data update function)

*1 If an SD memory card is reinserted (if it is unmounted once or more than once), the operation does not start.
   Restart the operation after updating a setting of the OPC UA server module.

File access status (X3)

● This signal turns ON while file access is stopped.

An SD memory card can be inserted or removed while file access is stopped. The file access will be in operation after inserting or removing an SD memory card, and this signal will turn OFF.

While file access is stopped, operations are as follows:

- Reading from/writing to an SD memory card are disabled.
- The operation of an OPC UA server module is stopped.
- Operations (reading/writing/verification/setting update/each diagnostic except the SD memory card diagnostic) cannot be performed in the configuration tool.

● This signal turns OFF during file access operation.

By turning the power OFF and ON or resetting a CPU module, the file access will be in operation.

However, this signal turns OFF during initialization upon powering ON from OFF.
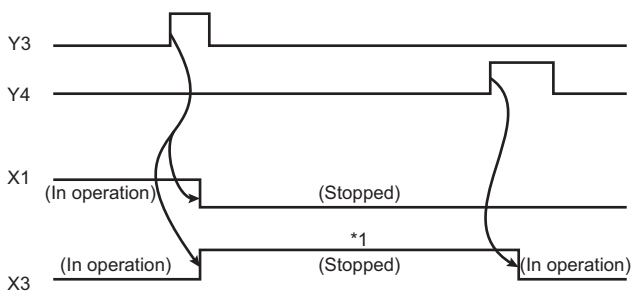
*1 The following operations are available.
   - Replacement of an SD memory card
   - Power OFF of a programmable controller

For the considerations when handling an SD memory card while file access is stopped, refer to the following:

📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

Ethernet port status (X5)

This signal turns ON when either Ethernet port is available.

It turns OFF when neither Ethernet port is available.

Connection status (X7)

This signal turns ON when a connection is established between an OPC UA server module and an OPC UA client (even one session is established).

Module stop error status (X10)

This signal turns ON while a module stop error occurs (ERR LED is flashing).

If an access target device error occurs when 'Module stop error status' (X10) or 'Module continuation error status' (X11) turns ON, 'Target device error' (X14) turns ON.

Module continuation error status (X11)

This signal turns ON while a module continuation error occurs (ERR LED is ON).

It turns OFF when 'Error clear request' (Y10) is turned ON.

Target device error (X14)

This signal turns ON when a communication error or access error with an access target device occurs.

When this signal is ON, an error code is stored in the access target status (device) area (Un\G8448 to 8703).

The signal turns OFF in the following cases:

- 'Error clear request' (Y10) is turned ON.
- The setting is updated in the configuration tool.
- A communication error or an access error has been cleared in all the access target devices.

Output signal details

The following shows the details on the output signals from an OPC UA server module to a CPU module.

OPC UA server resume request (Y1)

This signal starts the operation of an OPC UA server module according to the setting currently stored.

If an SD memory card is reinserted (if it is unmounted once or more than once), the operation does not start.

Restart the operation after updating a setting of the OPC UA server module.

When 'OPC UA server status' (X1) is ON, 'OPC UA server pause request' (Y2) needs to be executed first.

A request is not received in the following cases at the timing when an OPC UA server module monitors the output signals.

 • 'OPC UA server module operation stop request' (Y2) is being executed (Y2 is ON).
 • This signal turns ON simultaneously with 'OPC UA server module operation stop request' (Y2).

A request is not received before an OPC UA server module operates (it is not received if 'OPC UA server status' (X1) has never turned ON after turning the power ON).

OPC UA server pause request (Y2)

This signal sets the OPC UA server module operation to a stop state.

A request is not received in the following cases at the timing when an OPC UA server module monitors the output signals.

 • 'OPC UA server module operation restart request' (Y1) is being executed (Y1 is ON).
 • This signal turns ON simultaneously with 'OPC UA server module operation restart request' (Y1).

File access stop request (Y3)

This signal sets the file access to a stop state.

For ON/OFF timing, refer to the following:

☞ Page 115 File access status (X3)

For the considerations when handling an SD memory card while file access is stopped, refer to the following:

📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

File access stop cancellation request (Y4)

This signal cancels the stop state of the file access.

For ON/OFF timing, refer to the following:

☞ Page 115 File access status (X3)

> **Point**
>
> Even if file access is stopped by 'File access stop request' (Y3), it can be restarted by this signal.

Error clear request (Y10)

This signal turns the ERR LED, 'Module continuation error status' (X11), and 'Target device error' (X14) OFF by turning ON while a module continuation error occurs (ERR LED is ON).

It clears the latest error area (Un\G7168 to 7199).

The latest error code displayed on the system monitor of the engineering tool is cleared.

Appendix 3 Buffer Memory

This section explains the buffer memory of an OPC UA server module.

Precautions

Do not write any data to the "system area" of the buffer memory. Doing so may cause malfunction of the programmable controller system.

Buffer memory list

The following table shows the buffer memory list of an OPC UA server module.

R: Read-only, W: Write-only, R/W: Readable/Writable

Address Dec (Hex)	Purpose	Name and description		Initial value	R/W
0 (0H)	Module information	LED information	RUN LED status 0: OFF, 1: ON, 2: Flashing	0	R
1 (1H)			ERR LED status 0: OFF, 1: ON, 2: Flashing	0	R
2 (2H)			OPR LED status 0: OFF, 1: ON, 2: Flashing	0	R
3 (3H)			System area	—	—
4 (4H)			CARD RDY LED status 0: OFF, 1: ON, 2: Flashing	0	R
5 (5H)			CARD ACS LED status 0: OFF, 1: ON	0	R
6 to 7 (6H to 7H)			System area	—	—
8 (8H)			Dot matrix LED display mode 1: Error code 2: CH1 IP address 3: CH2 IP address	0	R
9 to 24 (9H to 18H)			Dot matrix LED display character string[1]	0	R
25 to 29 (19H to 1DH)		Parameter information	System area	—	—
30 (1EH)			OPC UA server function operating status 0: Initializing, 1: Running, 2: Stopping, 3: Stop	0	R
31 (1FH)			Module error status 0: No error, 1: Continuation error, 2: Stop error	0	R
32 (20H)			Operation mode 0: Tag mode, 1: Information model mode	0	R
33 to 85 (21H to 55H)			System area	—	—
86 to 511 (56H to 1FFH)	System area			—	—
512 (200H)	Network information	Ethernet port CH1 current value	Valid flag 0: Not use, 1: Use	0	R
513 (201H)		Ethernet port CH2 current value	Valid flag 0: Not use, 1: Use	0	R
514 (202H)		Ethernet port CH1 setting value	Valid flag 0: Not use, 1: Use	0	R
515 (203H)		Ethernet port CH2 setting value	Valid flag 0: Not use, 1: Use	0	R
516 to 525 (204H to 20DH)		System area		—	—

A

Address Dec (Hex)	Purpose	Name and description		Initial value	R/W
526 to 533 (20EH to 215H)	Network information	Ethernet port CH1 current value	IP address (character string)	0	R
534 to 535 (216H to 217H)			IP address	0	R
536 to 537 (218H to 219H)			Subnet mask	0	R
538 to 539 (21AH to 21BH)			Default gateway	0	R
540 to 557 (21CH to 22DH)			System area	—	—
558 to 589 (22EH to 24DH)		Ethernet port CH2 current value	Same as CH1		
590 to 653 (24EH to 28DH)		System area		—	—
654 to 661 (28EH to 295H)		Ethernet port CH1 setting value	IP address (character string)	0	R
662 to 663 (296H to 297H)			IP address	0	R
664 to 665 (298H to 299H)			Subnet mask	0	R
666 to 667 (29AH to 29BH)			Default gateway	0	R
668 to 685 (29CH to 2ADH)			System area	—	—
686 to 717 (2AEH to 2CDH)		Ethernet port CH2 setting value	Same as CH1		
718 to 1037 (2CEH to 40DH)		System area		—	—
1038 to 7167 (40EH to 1BFFH)	System area			—	—
7168 (1C00H)	Module information	Module error information	Error code	0	R
7169 (1C01H)			System area	—	—
7170 to 7177 (1C02H to 1C09H)			Error occurrence date and time	0	R
7178 to 7199 (1C0AH to 1C1FH)			System area	—	—
7200 to 7935 (1C20H to 1EFFH)	System area			—	—
7936 (1F00H)	SD memory card information	Mounting status 0: Initializing SD memory card status 1: Normal SD memory card mounting 2: Stopped file access 3: Invalid SD card mounting 4: Formatting SD memory card 5: Not inserted		0	R
7937 to 7939 (1F01H to 1F03H)		System area		—	—
7940 to 7941 (1F04H to 1F05H)		Capacity Unit: KB		0	R
7942 to 7943 (1F06H to 1F07H)		Free space Unit: KB		0	R
7944 to 7945 (1F08H to 1F09H)		Used amount Unit: KB		0	R
7946 (1F0AH)		Use rate Unit: %		0	R
7947 to 7999 (1F0BH to 1F3FH)		System area		—	—

Address Dec (Hex)	Purpose	Name and description			Initial value	R/W
8000 to 8447 (1F40H to 20FFH)	System area				—	—
8448 (2100H)	Target device information	Target device (1 to 16) information	Valid flag 0: Not set, 1: Set		0	R
8449 to 8455 (2101H to 2107H)			System area		—	—
8456 to 8457 (2108H to 2109H)			Connection status 0: Not connected, 1: Connecting, 2: Disconnecting		0	R
8458 to 8471 (210AH to 2117H)			System area		—	—
8472 (2118H)			Error information 0: No error, 1: Error		0	R
8473 to 8479 (2119H to 211FH)			System area		—	—
8480 to 8495 (2120H to 212FH)			Error code		0	R
8496 to 8607 (2130H to 219FH)			System area		—	—
8608 (21A0H)		System area			—	—
8609 (21A1H)		Label update information	Label update valid flag (target device 1 to 16) 0: Not set, 1: Set		0	R
8610 to 8616 (21A2H to 21A8H)			System area		—	—
8617 (21A9H)			Label update running status (target device 1 to 16) 0: Stopping, 1: Running		0	R
8618 to 8624 (21AAH to 21B0H)			System area		—	—
8625 to 8703 (21B1H to 21FFH)		System area			—	—
8704 to 8705 (2200H to 2201H)	Access OPC UA client information	Access OPC UA client information	System area		—	—
8706 to 8707 (2202H to 2203H)			Number of connected clients		0	R
8708 to 8743 (2204H to 2227H)			System area		—	—
8744 (2228H)		Session information (available only for the information model mode)	Session 1 information	Session status 0: Ready 1: Session free, available to create a new session 2: Session created, but not activated yet 4: Session active	0	R
8745 to 8746 (2229H to 222AH)				Session ID	0	R
8747 to 8748 (222BH to 222CH)				IP address	0	R
8749 to 8764 (222DH to 223CH)				System area	0	R
8765 to 9058 (223DH to 2362H)			Session 2 information to session 15 information	Same as session 1 information		
9059 to 9211 (2363H to 23FBH)		System area			—	—
9212 to 12418 (23FCH to 3082H)	System area				—	—

Address Dec (Hex)	Purpose	Name and description		Initial value	R/W
12419 to 12420 (3083H to 3084H)	Data processing information (available only for the information model mode)	Reading data	RevisedSamplingInterval (minimum) [ms]	0	R
12421 to 12422 (3085H to 3086H)			Actual SamplingInterval (minimum) [ms]	0	R
12423 to 12670 (3087H to 317EH)		System area		—	—
12671 to 13055 (317FH to 32FFH)	System area			—	—
13056 (3300H)	Error log information	Error count		0	R
13057 (3301H)		Latest error log number		0	R
13058 (3302H)		Error log 1	Error code	0	R
13059 (3303H)			System area	—	—
13060 to 13067 (3304H to 330BH)			Error occurrence date and time	0	R
13068 to 13217 (330CH to 33A1H)		Error log 2 to 16	Same as error log 1		
13218 to 13391 (33A2H to 344FH)		System area		—	—

Address Dec (Hex)	Purpose	Name and description			Initial value	R/W
13392 (3450H)	Firmware update history information	Firmware update completion with/without an error			0	R
13393 to 13401 (3451H to 3459H)		System area			—	—
13402 (345AH)		Latest firmware update information	History information	Execution time (year)	0	R
13403 (345BH)				Execution time (month)	0	R
13404 (345CH)				Execution time (day)	0	R
13405 (345DH)				Execution time (hour)	0	R
13406 (345EH)				Execution time (minute)	0	R
13407 (345FH)				Execution time (second)	0	R
13408 (3460H)				Execution time (day of the week)	0	R
13409 (3461H)				Firmware version after update	0	R
13410 (3462H)				Firmware version before update	0	R
13411 (3463H)		Latest firmware update result		Firmware update target	0	R
13412 (3464H)				Firmware update result	0	R
13413 (3465H)		Previous firmware update information	History information	Execution time (year)	0	R
13414 (3466H)				Execution time (month)	0	R
13415 (3467H)				Execution time (day)	0	R
13416 (3468H)				Execution time (hour)	0	R
13417 (3469H)				Execution time (minute)	0	R
13418 (346AH)				Execution time (second)	0	R
13419 (346BH)				Execution time (day of the week)	0	R
13420 (346CH)				Firmware version after update	0	R
13421 (346DH)				Firmware version before update	0	R
13422 (346EH)	Firmware update history information	Previous firmware update result		Firmware update target	0	R
13423 (346FH)				Firmware update result	0	R
13424 to 13427 (3470H to 3473H)		System area			—	—
13428 to 40959 (3474H to 9FFFH)	System area				—	—

*1 The displayed characters are updated when switched. (Scrolling the displayed characters will not be considered as switching display characters.)

Buffer memory details

The following explains the buffer memory details of an OPC UA server module.

Module information (Un\G0 to 85)

The LED information, OPC UA server function operating status, and module error status of an OPC UA server module are stored in this area.

For the stored values, refer to the following:

For the specifications, refer to the following:

Item	Reference
LED information	📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

■LED information (Un\G0 to 24)

The LED status, dot matrix LED display mode, and dot matrix LED display character string (ASCII format (within the range from 0x0020 to 0x007E)) are stored.

■OPC UA server function operating status (Un\G30)

The operating status of an OPC UA server function is stored.

■Module error status (Un\G31)

The error status of an OPC UA server module is stored.

■Operation mode (Un\G32)

The operation mode of an OPC UA server module is stored.

0: Tag mode

1: Information model mode

Network information (Un\G512 to 1037)

The connection status of an OPC UA server module to a network is stored in this area.

■Common setting (Un\G512 to 517)

Common settings for Ethernet port are stored.

Buffer memory name	Address	Description
Ethernet port CH1 current value valid flag	Un\G512	The setting status (use/ not use) of current Ethernet port (CH1) is stored. 0: Not use 1: Use
Ethernet port CH2 current value valid flag	Un\G513	The setting status (use/ not use) of current Ethernet port (CH2) is stored. The setting value is same as 'Ethernet port CH1 current value valid flag' (Un\G512).
Ethernet port CH1 setting value valid flag	Un\G514	The setting status (value set by the configuration tool) of Ethernet port (CH1) is stored. 0: Not use 1: Use
Ethernet port CH2 setting value valid flag	Un\G515	The setting status (value set by the configuration tool) of Ethernet port (CH2) is stored. The setting value is same as 'Ethernet port CH1 setting value valid flag' (Un\G514).

■Ethernet port CH1 current value (Un\G526 to 557)

The current IP address information of Ethernet port (CH1) is stored.

Buffer memory name	Address	Description
IP address (character string)	Un\G526 to 533	IP address is stored in character string. The character string to be stored is set by left justifying. (Example) "192.168.3.3"
IP address	Un\G534 to 535	The IP address is stored as a double word (32-bit value).
Subnet mask	Un\G536 to 537	The subnet mask is stored as a double word (32-bit value).
Default gateway	Un\G538 to 539	The default gateway address is stored as a double word (32-bit value). When the default gateway is not set, 0 is stored.

■Ethernet port CH2 current value (Un\G558 to 589)

The current IP address information of Ethernet port (CH2) is stored.

Each item is same as 'Ethernet port CH1 current value' (Un\G526 to 557).

■Ethernet port CH1 setting value (Un\G654 to 685)

The IP address information of the setting value of Ethernet port (CH1) (value set by the configuration tool) is stored.

Each item is same as 'Ethernet port CH1 current value' (Un\G526 to 557).

■Ethernet port CH2 setting value (Un\G686 to 717)

The IP address information of the setting value of Ethernet port (CH2) (value set by the configuration tool) is stored.

Each item is same as 'Ethernet port CH1 current value' (Un\G526 to 557).

Module information (Un\G7168 to 7199)

The latest error information of an OPC UA server module is stored in this area.

■Error code (Un\G7168)

An error code which indicates the error contents is stored. (☞ Page 104 Error Code List)

■Error occurrence date and time (Un\G7170 to 7177)

The time when the error occurred is stored in BCD code.

	b15 ⋯ b8	b7 ⋯ b0
Un\G7170	Unused	UTC offset*1
Un\G7171	Month (01H to 12H)	Year (00H to 99H) first 2 digits
Un\G7172	Hour (00H to 23H)	Day (01H to 31H)
Un\G7173	Second (00H to 59H)	Minute (00H to 59H)
Un\G7174	Year (00H to 99H) first 2 digits	Day of the week (00H to 06H)*2
Un\G7175	Lower milliseconds (00H to 99H)*3	Upper milliseconds (00H to 09H)*4
Un\G7176	System area	System area
Un\G7177	System area	System area

*1 UTC offset
    -48 to 52: -12 hours to +13 hours (Unit: 15 minutes)
*2 0: Sunday, 1: Monday, 2: Tuesday, 3: Wednesday, 4: Thursday, 5: Friday, 6: Saturday
*3 Lower milliseconds: Tens digit, ones digit
*4 Upper milliseconds: Hundreds digit

SD memory card information (Un\G7936 to 7999)

The status of the SD memory card inserted in an OPC UA server module is stored in this area.

■Mounting status (Un\G7936)

The status of SD memory card is stored.

0: Initializing SD memory card status

1: Normal SD memory card mounting

2: Stopped file access

3: Invalid SD card mounting

4: Formatting SD memory card

5: Not inserted

■Capacity (Un\G7940 to 7941)

The capacity of an SD memory card is stored. (Unit: KB)

■Free space (Un\G7942 to 7943)

The free space of an SD memory card is stored. (Unit: KB)

■Used amount (Un\G7944 to 7945)

The used amount of an SD memory card is stored. (Unit: KB)

■Use rate (Un\G7946)

The use rate of an SD memory card is stored. (Unit: %)

Target device information (Un\G8448 to 8703)

The setting status of a target device is stored in this area.
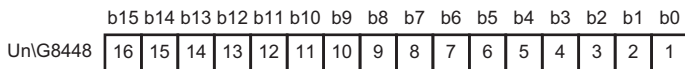
■Valid flag (Un\G8448)

The setting status of the target device setting is stored.

The corresponding bit of the setting number of a set access target device turns ON.

0: Not set

1: Set

	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
Un\G8448	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

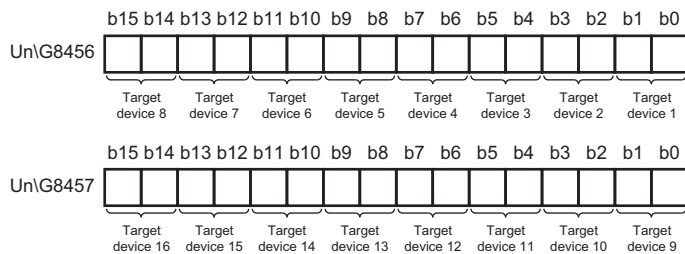### ■Connection status (Un\G8456 to 8457)

The connection status of the target device is stored.

Depending on the connection status, values are stored in the corresponding bit of the setting number for the target device as follows:

00b: Not connected (including the case in which 'Valid flag' (Un\G8448) is 'Not set' (0).)

01b: Connecting

10b: Disconnecting

■Error information (Un\G8472)

The error information of the target device is stored.

The corresponding bit of the setting number of an access target device in which an error has occurred turns ON.

0: No error

1: Error

	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
Un\G8472	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
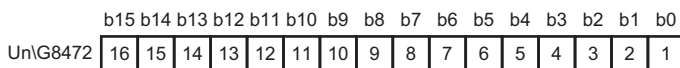
■Error code (Un\G8480 to 8495)

An error code which indicates the error contents is stored to the corresponding area of the setting number for the target device in which an error occurs.

Ex.

When an error occurs in the target device set in the target device setting No.16

· Bit 15 of 'Error information' (Un\G8472) turns ON.

· An error code is stored in 'Error code 16' (Un\G8495).

A

■Label update information (Un\G8609 to 8624)

The label update information of an access target device is stored.

Buffer memory name	Address	Description
Label update valid flag	Un\G8609	Whether the global label-related data update function is set is stored. The corresponding bit of the setting number of a set access target device turns ON. 0: Not set 1: Set | Label update running status	Un\G8617	Whether the global label-related data update function is running or stopped is stored. If it is running, the corresponding bit of the setting number of an access target device turns ON. 0: Stopping 1: Running

For Un\G8609:

	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
Un\G8609	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

For Un\G8617:

	b15	b14	b13	b12	b11	b10	b9	b8	b7	b6	b5	b4	b3	b2	b1	b0
Un\G8617	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Access OPC UA client information (Un\G8704 to 9211)

The setting status of an access OPC UA client is stored in this area.

■Number of connected clients (Un\G8706 to 8707)

The number of connected access OPC UA clients is stored.

■Session 1 information to session 15 information (Un\G8744 to 9058) (information model mode only)

When using the information model mode, session information is stored.

Note that session information is not stored if no information model file is imported in a project.

Buffer memory name	Description
Session status	The status of a session is stored. • 0: Ready • 1: Session free, available to create a new session • 2: Session created, but not activated yet • 4: Session active
Session ID	The ID of a session is stored. The session ID is stored when the session is open.
IP address	The IP address is stored as a double word (32-bit value). The IP address is stored when the session is activated.

Data processing information (Un\G12419 to 12670) (information model mode only)

When using the information model mode, the status of data processing of an OPC UA server module is stored in this area.

■Reading data (Un\G12419 to 12422)

The status of data reading processing is stored.

Buffer memory name	Address	Description
RevisedSamplingInterval (minimum)	Un\G12419 to 12420	Among RevisedSamplingIntervals for MonitoredItems, the minimum one is stored. (Unit: ms)
Actual SamplingInterval (minimum)	Un\G12421 to 12422	An actually executed SamplingInterval for the RevisedSamplingInterval (minimum) is stored. (Unit: ms)

Error log information (Un\G13056 to 13391)

The error history occurred in an OPC UA server module is stored in this area.

■Error count (Un\G13056)

The accumulated count registered in the error log area is stored.

If the count exceeds the maximum value, the maximum value (65535) is stored.

■Latest error log number (Un\G13057)

The error log number in which the latest error log is registered is stored.[*1]

0: No error (No error log registered)

1 or more: Error log number in which the latest error log is registered

*1 The pointer value of "16" indicates that the latest error log has been registered in the error log area of 16.

■Error log 1 to 16 (Un\G13058 to 13217)

The error history is stored.

Error log area is comprised of 16 error logs with the same data configuration. (continuation error: up to 15, stop error: up to 1)

When a new stop error occurs in the state where a stop error is stored, the information of the stop error is updated.

An error log is not stored in the following cases.

- When an error that has already been stored in the error log area occurs again
- When a new continuation error occurs after a stop error occurs
- When a new continuation error occurs in the state where 15 continuation errors are stored

Buffer memory name	Description
Error code	An error code which indicates the error contents is stored. (☞ Page 104 Error Code List)
Error occurrence date and time	The time when the error occurred is stored in BCD code. (☞ Page 124 Error occurrence date and time (Un\G7170 to 7177))

Firmware update history information (Un\G13392 to 13427)

The firmware update history of an OPC UA server module is stored in this area.

Buffer memory name			Address	Description
Firmware update completion with/without an error			Un\G13392	The error occurrence state on the firmware update function is stored. • 0: Update completed without an error (including successful completion) • 1: Update completed with an error '1' is stored when a value of 'Firmware update result' (Un\G13412) is within 100 to 300H.
System area			Un\G13393 to 13401	Use prohibited
Latest firmware update information	History information	Execution time (year)	Un\G13402	The value of the year (four digits) when the firmware update was executed is stored as a BIN code.
		Execution time (month)	Un\G13403	The value of the month when the firmware update was executed is stored as a BIN code.
		Execution time (day)	Un\G13404	The value of the day when the firmware update was executed is stored as a BIN code.
		Execution time (hour)	Un\G13405	The value of the hour when the firmware update was executed is stored as a BIN code.
		Execution time (minute)	Un\G13406	The value of the minutes when the firmware update was executed is stored as a BIN code.
		Execution time (second)	Un\G13407	The value of the seconds when the firmware update was executed is stored as a BIN code.
		Execution time (day of the week)	Un\G13408	The value of the day of the week when the firmware update was executed is stored as a BIN code. (0: Sunday, 1: Monday, 2: Tuesday, 3: Wednesday, 4: Thursday, 5: Friday, 6: Saturday)
		Firmware version after update	Un\G13409	The firmware version after update is stored. (When the update is completed with an error, '0' is stored.)
		Firmware version before update	Un\G13410	The firmware version before update is stored.

A

Buffer memory name			Address	Description
Latest firmware update result		Firmware update target	Un\G13411	The start input/output number of the module where the firmware update was executed is stored.
		Firmware update result	Un\G13412	The execution result of the firmware update is stored. • 1H: Normal end • 100H: Flash ROM error • 200H: Model mismatched • 201H: File invalid • 203H: Firmware update prohibited state • 300H: Firmware data error
Previous firmware update information	History information	Execution time (year)	Un\G13413	The value of the year (four digits) when the firmware update was executed is stored as a BIN code.
		Execution time (month)	Un\G13414	The value of the month when the firmware update was executed is stored as a BIN code.
		Execution time (day)	Un\G13415	The value of the day when the firmware update was executed is stored as a BIN code.
		Execution time (hour)	Un\G13416	The value of the hour when the firmware update was executed is stored as a BIN code.
		Execution time (minute)	Un\G13417	The value of the minutes when the firmware update was executed is stored as a BIN code.
		Execution time (second)	Un\G13418	The value of the seconds when the firmware update was executed is stored as a BIN code.
		Execution time (day of the week)	Un\G13419	The value of the day of the week when the firmware update was executed is stored as a BIN code. (0: Sunday, 1: Monday, 2: Tuesday, 3: Wednesday, 4: Thursday, 5: Friday, 6: Saturday)
		Firmware version after update	Un\G13420	The firmware version after update is stored. (When the update is completed with an error, '0' is stored.)
		Firmware version before update	Un\G13421	The firmware version before update is stored.
Previous firmware update result		Firmware update target	Un\G13422	The start input/output number of the module where the firmware update was executed is stored.
		Firmware update result	Un\G13423	The execution result of the firmware update is stored. • 1H: Normal end • 100H: Flash ROM error • 200H: Model mismatched • 201H: File invalid • 203H: Firmware update prohibited state • 300H: Firmware data error

Appendix 4 Available Characters

This section shows the characters that can be used for each setting item.

Screen	Item	Available character	Reference
Address Space(Target Device)	Name	☞ Page 131 Available ASCII characters	Page 32 Access target device
	Description	Characters that can be represented in Unicode®	
Communication Setting	Station No.	Numerals (decimal)	Page 33 Communication setting
	Start I/O No.	Numerals (hexadecimal)	
	Time Out	Numerals (decimal)	
	Network No.	Numerals (decimal)	
	IP Address	Numerals (decimal)	
Address Space(Data Tag) ([Basic] tab)	Name	☞ Page 131 Available ASCII characters	Page 36 [Basic] tab
	Description	Characters that can be represented in Unicode	
	Remark		
	Extended number (Network No./Start I/O No.)	Numerals (decimal/hexadecimal)[*1]	
	PLC Device No. (I/O Address)		
Address Space(Data Tag) ([Details] tab)	Number of elements	Numerals (decimal)	Page 38 [Details] tab
	Length		
Address Space(Data Tag) ([Multiply] tab)	Start No.		Page 41 [Multiply] tab
	Numeric Places		
	Number of items		
	Name	☞ Page 131 Available ASCII characters	
Structure Label Definitions	Label Name	☞ Page 131 Available ASCII characters	Page 43 Label
	Comment	Characters that can be represented in Unicode	
	Remark		
	Number of elements	Numerals (decimal)	
	Address	• Available ASCII characters[*2] ☞ Page 131 Available ASCII characters • \, . (period)	Page 44 Address
	Structure Array offset Value	Numerals (decimal)	
	Extended number (Network No./Start I/O No.)	Numerals (decimal/hexadecimal)[*1]	
	PLC Device No. (I/O Address)		
Address Space(Group)	Name	☞ Page 131 Available ASCII characters	Page 49 Group
	Description	Characters that can be represented in Unicode	
Conversion Definitions	Name	☞ Page 131 Available ASCII characters	Page 50 Conversion Definition Setting
	Engineering Unit	• Numerals (decimal) • +, - (minus), . (decimal point), E (exponent notation)	
	Instrument Range		
	Range		
Polling Method Definitions	Name	☞ Page 131 Available ASCII characters	Page 52 Polling Definition Setting
	Rate	Numerals (decimal)	

A

Screen	Item	Available character	Reference
Structure Type Declarations	Name	☞ Page 131 Available ASCII characters	Page 53 Structure Definition Setting
	Description	Characters that can be represented in Unicode	
	Comment		
	Remark		
	Number of elements	Numerals (decimal)	Page 54 Adding a member
	Length		
User Account Setting	User Name	☞ Page 131 Available ASCII characters	Page 57 User account setting
	Password		
Network Setting	IP Address	Numerals (decimal)	Page 58 Network Setting
	Subnet Mask		
	Default Gateway		
	Host Name	Available ASCII characters[*3] ☞ Page 131 Available ASCII characters	
OPC UA Server Setting ([Connection Setting] tab)	Port No.	Numerals (decimal)	Page 59 [Connection Setting] tab
OPC UA Server Setting ([Certificate] tab)	OPC UA Server Name	☞ Page 131 Available ASCII characters	Page 61 [Certificate] tab
	Organization name		
	Organization Unit		
	Locality		
	State		
	Country	Available ASCII characters[*3] ☞ Page 131 Available ASCII characters	
OPC UA Server Setting ([Discovery Server] tab)	Discovery Server URL	• Available ASCII characters[*2] ☞ Page 131 Available ASCII characters • :, /, . (period)	Page 61 [Discovery Server] tab
	Registration Interval	Numerals (decimal)	
OPC UA Server Setting ([Operation Setting] tab)	Waiting time		Page 62 [Operation Setting] tab
Target Setting	IP Address		Page 77 Connection destination setting
	User Name	☞ Page 131 Available ASCII characters	
	Password		
OPC UA Server Module Manage	Prohibition release password	U+0020 to U+007E (ASCII characters excluding control characters and DEL)	Page 87 Firmware update management

*1   Whether it is decimal or hexadecimal notation differs depending on a specified device type.

*2   Excluding underscores (_).

*3   Excluding lower-case characters.

Available ASCII characters

Characters in the shaded area can be used.

	0	1	2	3	4	5	6	7
0	NUL		(SP)	0	@	P	`	p
1			!	1	A	Q	a	q
2			"	2	B	R	b	r
3			#	3	C	S	c	s
4			$	4	D	T	d	t
5			%	5	E	U	e	u
6			&	6	F	V	f	v
7			'	7	G	W	g	w
8			(	8	H	X	h	x
9			)	9	I	Y	i	y
A			*	:	J	Z	j	z
B			+	;	K	[	k	{
C			,	<	L	\	l	|
D			-	=	M	]	m	}
E			.	>	N	^	n	~
F			/	?	O	_	o	

Appendix 5 Uploading Certificates to the Trust List

This section shows the procedures for uploading certificates to "Trust List" before connecting with an OPC UA client.

When uploading a certificate certified by a certificate authority, refer to the following:

☞ Page 136 Handling Certificates Certified by a Certificate Authority

User authentication with a certificate

For user authentication with a certificate when connecting with an OPC UA client, upload a certificate by the following procedure.
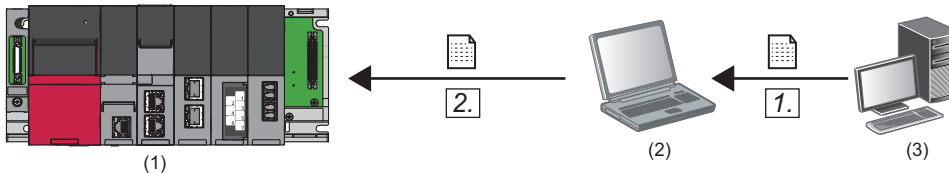
(1) OPC UA server module
(2) Configuration personal computer (configuration tool)
(3) OPC UA client

1. Store a client certificate in a personal computer on which the configuration tool is installed.
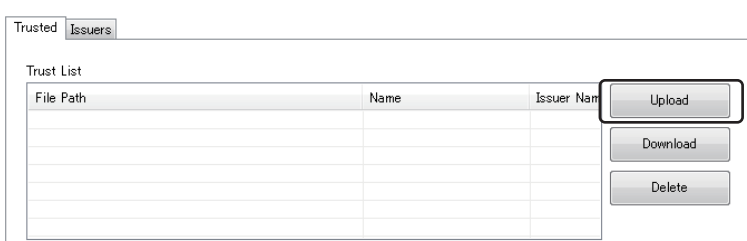
For the operation methods of an OPC UA client, refer to the manual for the OPC UA client used.

> **Point**
>
> If a folder in which a client certificate is stored is unclear, perform the procedure shown in the following section.
>
> ☞ Page 133 Uploading a denied certificate to the trust list
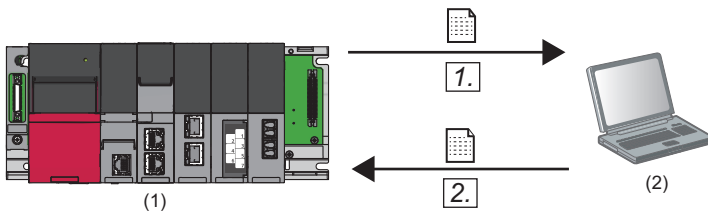
2. Click the [Upload] button in the "Manage User Certificate" screen to upload the client certificate to "Trust List."

Uploading a denied certificate to the trust list

If a client certificate is not uploaded to "Trust List," it is stored in "Denied Certificate List" when connecting from an OPC UA client to an OPC UA server module, and the connection is not established.
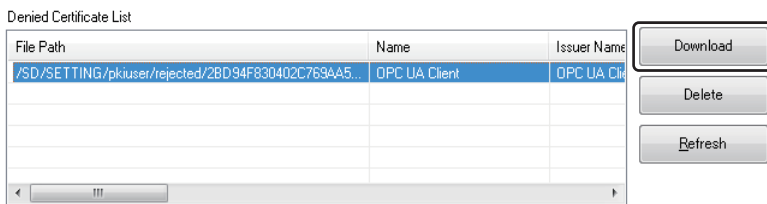
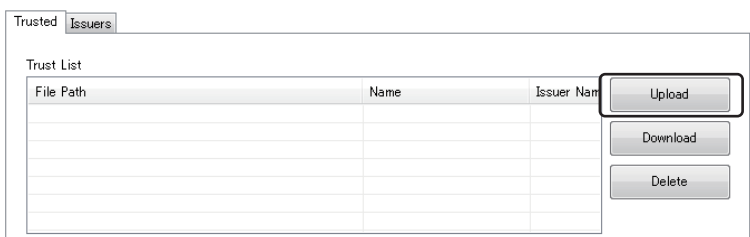Upload a stored certificate by the following procedure.

(1) OPC UA server module
(2) Configuration personal computer (configuration tool)

1. Click the [Download] button in the "Manage User Certificate" screen to download a client certificate to a personal computer.

Denied Certificate List

File Path	Name	Issuer Name	
/SD/SETTING/pkiuser/rejected/2BD94F830402C769AA5...	OPC UA Client	OPC UA Clie	Download
			Delete
			Refresh

2. Click the [Upload] button in the "Manage User Certificate" screen to upload the client certificate to "Trust List."

Trusted   Issuers

Trust List

File Path	Name	Issuer Nam	
			Upload
			Download
			Delete

A

Application authentication with a certificate

If not exchanging certificates automatically when performing application authentication with a certificate, upload a certificate by the following procedure.
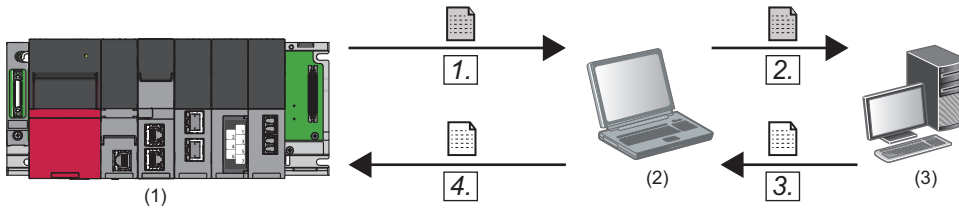
(1) OPC UA server module
(2) Configuration personal computer (configuration tool)
(3) OPC UA client

1. Click the [Server Certificate Download] button in the "Manage Application Certificate" screen to download a server certificate.

> **Point**
>
> This step can be skipped depending on an OPC UA client to use.

2. Register the server certificate in the trust list of an OPC UA client.

For the registration method, refer to the manual for an OPC UA client used.

> **Point**
>
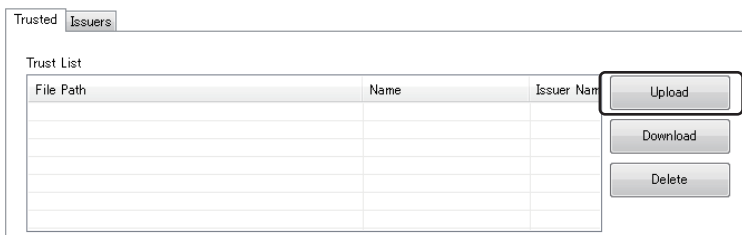> This step can be skipped depending on an OPC UA client to use.

3. Store a client certificate in a personal computer on which the configuration tool is installed.

For the operation methods of an OPC UA client, refer to the manual for the OPC UA client used.

> **Point**
>
> If a folder in which a client certificate is stored is unclear, perform the procedure shown in the following section.
>
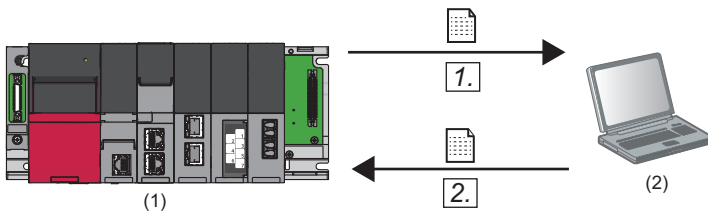> ☞ Page 135 Uploading a denied certificate to the trust list

4. Click the [Upload] button in the "Manage Application Certificate" screen to upload the client certificate to "Trust List."

Uploading a denied certificate to the trust list

If a client certificate is not uploaded to "Trust List," it is stored in "Denied Certificate List" when connecting from an OPC UA client to an OPC UA server module, and the connection is not established.
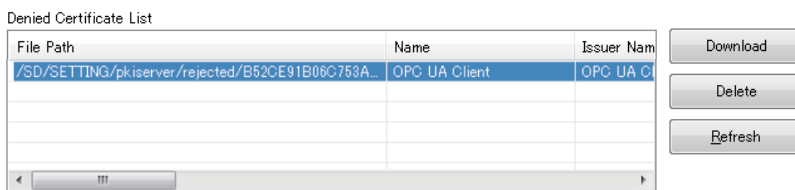
Upload a stored certificate by the following procedure.

(1) OPC UA server module
(2) Configuration personal computer (configuration tool)

1. Click the [Download] button in the "Manage Application Certificate" screen to download a client certificate to a personal computer.

2. Click the [Upload] button in the "Manage Application Certificate" screen to upload the client certificate to "Trust List."
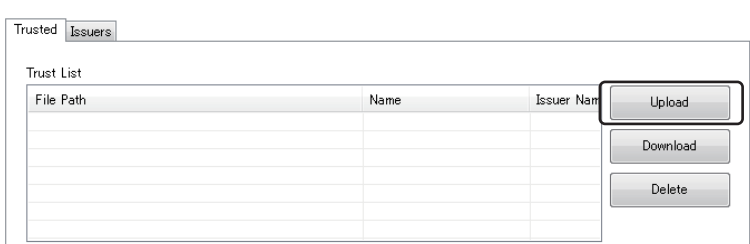
# Appendix 6 Handling Certificates Certified by a Certificate Authority

This section describes the handling of certificates certified by a certificate authority.

Certificates and revocation lists that must be uploaded

When using a certificate certified by a certificate authority, all electronic certificates issued by certificate authorities in the tree (files with the extension 'der') must be uploaded to "Trust List" in the [Trusted] or [Issuers] tab.
In addition, all certificate revocation lists issued by certificate authorities in the tree (files with the extension 'crl') must be uploaded to "Revocation List" in the tab in which electronic certificates issued by certificate authorities are uploaded. Otherwise, the electronic certificates cannot be authenticated.
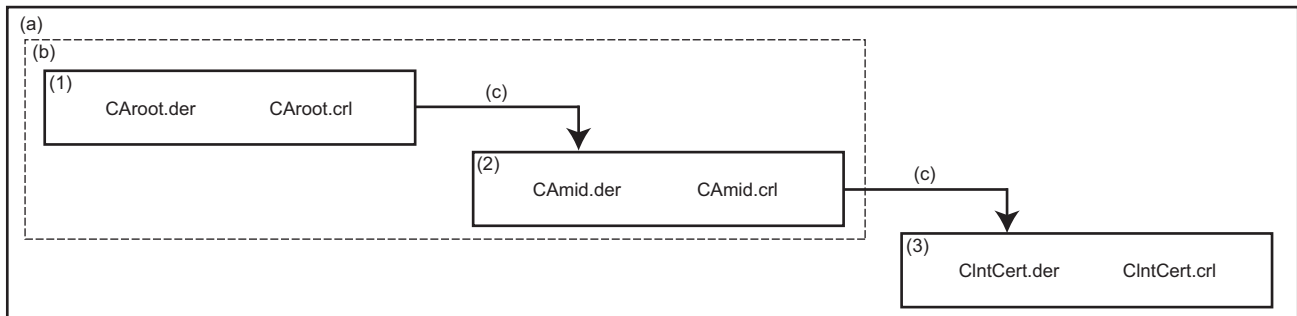
(a) Certificate tree
(b) Electronic certificate issued by a certificate authority
(c) Certification
(1) Root certificate (CA_root)
(2) Intermediate certificate (CA_mid)
(3) Client certificate (ClientCert)

When uploading an electronic certificate issued by a certificate authority to "Trust List" in the [Trusted] tab, all certificates certified by the certificate authority are authenticated. In this case, a client certificate does not need to be uploaded to "Trust List" in the [Trusted] tab.

When uploading an electronic certificate issued by a certificate authority to "Trust List" in the [Issures] tab, client certificates that can be authenticated can be limited.

The following table shows the client certificates that can be authenticated for each combination of certificates uploaded to "Trust List" in the [Trusted] and [Issuers] tab.

Certificate uploaded to "Trust List" in the [Trusted] tab	Certificate uploaded to "Trust List" in the [Issures] tab	Client certificate that can be authenticated
• (1) Root certificate (CA_root) • (2) Intermediate certificate (CA_mid) • (3) Client certificate (ClientCert)[1]	N/A	All client certificates authenticated by (1) root certificate or (2) intermediate certificate (including (3) client certificate (ClientCert))
• (2) Intermediate certificate (CA_mid) • (3) Client certificate (ClientCert)[1]	(1) Root certificate (CA_root)	All client certificates certified by (2) intermediate certificate (including (3) client certificate (ClientCert))
(3) Client certificate (ClientCert)	• (1) Root certificate (CA_root) • (2) Intermediate certificate (CA_mid)	(3) Client certificate (ClientCert) only

*1   Not always required.

Appendix 7　Processing Time

This section shows the measurement results for the processing time of the Data Access function.

Note that the processing time may increase depending on any of the following factors:

- Usage environment (personal computer, network, and SD memory card)
- Sequence scan time
- Access status from a personal computer, HMI, or another intelligent function module to a CPU module
- Settings of an OPC UA server module

Use the measurement results as a reference for processing time.

Measurement conditions

- In measuring the processing times of the Read and Write, the time is measured from when an OPC UA client sends a ReadRequest or WriteRequest to an OPC UA server module to when a response is returned.
- For a Subscription, the interval at which an OPC UA client receives the Publish of a subscription target tag is measured.

Item		Description
Access target device	CPU module	R08CPU
	Scan time	20 ms (A program with a specified scan time is used.)
	Device/label access service processing setting	10% (default value)
	Program content	A program for incrementing 50% of devices assigned to the address space (tag) of RD81OPC96 every scan
	Network	Own station (control CPU), another station (via Ethernet)
OPC UA server module	Access type	• Read • Write • Subscription
	Number of access target tags	• Non-array: 100, 1000, 5000, 10000 • Array[1]: 1000 (10), 5000 (50), 10000 (100), 20000 (200), 50000 (500)
	Number of tag settings	Same as 'Number of access target tags'
	Polling cycle	• Subscription: 200 ms (minimum settable value) • Read/Write: 1000 ms
	Device data type	• Non-array: WORD • Array: ARRAY [0..99] OF INT
	Data type	• Non-array: INT • Array: Array of INT
	Security policy	Basic256Sha256
	Security mode	Sign & Encrypt
OPC UA client	CPU	Intel® Core™ i5-8500 3.00 GHz
	Memory	16 GB
	OS	Windows® 10 Enterprise
	SDK	UA-.NETStandard-1.4.367.41 of OPC Foundation
Other	Number of measurements	An average calculated by measuring for 100 times

*1　The numbers in the parentheses indicate the numbers of tags in an array. 100 elements can be set per array tag.

Measurement results

■Non-array tag

Access target	Access type	Number of access target tags			
		100	1000	5000	10000
Own station (control CPU)	Read	20 ms	110 ms	520 ms	1000 ms
	Write	80 ms	550 ms	2720 ms	5430 ms
	Subscription	210 ms	210 ms	1400 ms	6500 ms
Another station (via Ethernet)	Read	20 ms	120 ms	540 ms	1070 ms
	Write	90 ms	790 ms	3850 ms	7640 ms
	Subscription	210 ms	220 ms	1600 ms	7100 ms

■Array tag

Access target	Access type	Number of access target tags (number of tags in an array)				
		1000 (10)	5000 (50)	10000 (100)	20000 (200)	50000 (500)
Own station (control CPU)	Read	10 ms	20 ms	30 ms	60 ms	130 ms
	Write	350 ms	2110 ms	4130 ms	8150 ms	20150 ms
	Subscription	220 ms	1090 ms	2100 ms	4190 ms	10500 ms
Another station (via Ethernet)	Read	10 ms	20 ms	30 ms	60 ms	140 ms
	Write	380 ms	2120 ms	4130 ms	8150 ms	20150 ms
	Subscription	220 ms	1090 ms	2110 ms	4220 ms	10650 ms

Appendix 8 CSV File Format

This section shows the format specifications of a file used for the import or export function for CSV files.

CSV file format

■Format specifications

Item name		Description
Delimiter		Comma (,) The number of commas must be the same in each row, excluding setting values.
Character code		UTF-8 (with BOM)
Line feed code		CRLF (0x0D, 0x0A)
Upper/lower-case character		• Column name row: Not case-sensitive • Setting row: Case-sensitive[*1]
Special character	Line feed	If a line feed is included in a setting value, the entire data is enclosed in double quotes.
	Comma	If a comma is included in a setting value, the entire setting value is enclosed in double quotes.
	Double quote	A double quote (") is used in pairs ("") as a setting value, and the entire setting value is enclosed in double quotes (").
Column order		It can be described freely.
Column name		All items are described.
Line feed		A row with a line feed only is ignored.

*1   The related data object name (OBJECT_NAME with LABEL_RELATION of "RELATED") is not case-sensitive.

■Format overview

	TARGET_DEVICE	OBJECT_PATH	OBJECT_NAME	OBJECT_TYPE	···
(1)	Dev000		Group0	GROUP	···
(2)	Dev000	Group0	Tag000	TAG	···
	:	:	:	:	···

```
(1)   TARGET_DEVICE,OBJECT_PATH,OBJECT_NAME,OBJECT_TYPE,…
      Dev000,,Group0,GROUP,…
(2)   Dev000,Group0,Tag000,TAG,…
      :
```

Element	Description
(1) Column name row	The name of a setting item. The first row excluding a row with a line feed only.
(2) Setting row	A setting value. A row excluding one with a line feed only and the column name row.

File list

Nine types of CSV files and two types of text files are used for the import or export function for CSV files.

Files are stored in any specified folders.

○: Used, ×: Not used, —: N/A

File name	Description	Max. No. of rows	Import	Export
ADDRESS_SPACE.CSV	Address space setting (tag, structure label, structure label member, group)	21000	○	○
STRUCTURE.CSV	Structure definition setting	12000	○	○
TARGET_DEVICE.CSV	Address space setting (access target device)	8	○	○
CONVERSION.CSV	Conversion definition setting	256	○	○
POLLING.CSV	Polling definition setting	8	○	○
SECURITY.CSV	Security setting	1	○	○
USER_SETTING.CSV	User setting	16	○	○[*1]
NETWORK.CSV	Network setting	1	○	○
OPCUA_SERVER.CSV	OPC UA server setting	1	○	○
export_info.txt	Supplementary information (project name, export date and time, configuration tool version)	—	×	○
csv_import_yyyymmdd_hhmmssfff.log	Warning/error log file when importing a CSV file	—	○[*2]	×

*1   A password is not output.

*2   A log file output if a warning or error occurs when importing a CSV file
       For details on a log file, refer to the following:
       ☞ Page 157 Warning/error log file when importing a CSV file

File details

Each item in a CSV file is to be imported or exported unless otherwise specified.

For details on the characters that can be used as setting values, refer to the following:

☞ Page 129 Available Characters

■ADDRESS_SPACE.CSV

Column name	Overview	Description	Setting value
TARGET_DEVICE	Access target device name	The name of an access target device to which an object[1] belongs	• ASCII character • 1 to 256 characters
OBJECT_PATH	Path to an object	The path to an object[1]. The path is a character string consisting of objects connected with a period (.), excluding an access target device. (Example) For the following settings • OBJECT_PATH of an object with OBJECT_NAME of 'Group000': Blank • OBJECT_PATH of an object with OBJECT_NAME of 'Group001': Group000 • OBJECT_PATH of an object with OBJECT_NAME of 'Tag002': Group000.Group001	• ASCII character and period (.) • 0 to 1826 characters
OBJECT_NAME	Object name	The name of an object[1]	• ASCII character • 1 to 256 characters
OBJECT_TYPE	Object type	The type of an object[1]. Any of the following is specified: a tag, group, structure label, or member of a structure label. For details on the description rules for using structure labels, refer to the following: ☞ Description rules for structure labels	• TAG: Tag • GROUP: Group • STRUCT: Structure label • MEMBER: Member of a structure label
STRUCTURE	Structure definition name	The name of a structure definition that is a source of a structure label. This column is used in the following cases: • OBJECT_TYPE is "STRUCT" • OBJECT_TYPE is "MEMBER" and DATA_TYPE is "STRUCT" On import, any structure not defined in a STRUCTURE.CSV file or the setting of an import destination cannot be specified. In addition, when OBJECT_TYPE is "MEMBER" and DATA_TYPE is "STRUCT," this item must match the structure definition name (STRUCTURE of STRUCTURE.CSV) specified for the member of the corresponding structure definition.	• ASCII character • 1 to 256 characters
DESCRIPTION	Description or comment	The description or comment for an object[1]. This column is used when OBJECT_TYPE is "TAG," "GROUP," or "STRUCT."	• Unicode character • 0 to 128 characters
REMARK	Remarks	The remarks for an object[1]. This column is used when OBJECT_TYPE is "TAG" or "STRUCT."	• Unicode character • 0 to 128 characters
ADDRESS	Device memory	A device assigned to a tag or a member of a structure label.[2] This column is used when OBJECT_TYPE is "TAG" or "MEMBER." For "MEMBER," this setting value is ignored on import under the following conditions: • A structure to which a member belongs is an array and the member is neither bit nor word device defined first in the structure member. This item includes the following settings of the configuration tool. • Device type, digit specification, bit specification, extended number, and PLC device number in the address space (tag) setting • Device type, bit specification, extended number, and PLC device number in the address setting in the structure label definition setting The description methods of bit specification and digit specification are as follows: • Bit specification: '.n' (n = 0 to F) is added to the end. (Example) D100.0, J1\W0.F • Digit specification: 'Kn' (n = 1 to 8) is added to the start. (Example) K8M0, J1\K4X0 If this column is blank, a device is unassigned (Not Assigned) on import.	• Character that can be used in device representation

A

| Column name	Overview	Description	Setting value
LABEL_RELATION	Global label-related data specification	Whether a global label is related to an object[1]. This column is used when OBJECT_TYPE is "TAG" or "STRUCT." The setting contents of this column, OBJECT_PATH, and OBJECT_NAME differ depending on the contents of a global label. ■For a global label not using a structure • This column: RELATED • OBJECT_PATH: Blank • OBJECT_NAME: Label name of a global label ■For a global label using a structure The settings for a structure are as follows: • This column: RELATED • OBJECT_PATH: Blank • OBJECT_NAME: Label name of a global label The settings for a member are as follows: • This column: Blank • OBJECT_PATH: Structure label name of a definition source • OBJECT_NAME: Label name of a member Note the following points to set OBJECT_PATH and OBJECT_NAME.[3] ■OBJECT_NAME of a timer/counter/retentive timer/long timer/long counter/long retentive timer type label • Contact: Add '_S' to a label name. [Label name]_S • Coil: Add '_C' to a label name. [Label name]_C • Current value: Add '_N' to a label name. [Label name]_N (Example) When setting the timer type global label 'tdLabel,' the contact is 'tdLabel_S,' the coil is 'tdLabel_C,' and the current value is 'tdLabel_N.' ■For a structure global label OBJECT_PATH of a structure member is the structure label name. (Example) When representing the member 'bLabel' of the structure 'stLabel,' OBJECT_PATH is 'stLabel' and OBJECT_NAME is 'bLabel.' ■For a global label with a structure as a member of a structure OBJECT_PATH of a structure member is a character string consisting of structure label names connected with a period (.). (Example) When representing the member 'bLabel' of the structure 'stLabel' included as a member in the structure 'stLabel2,' OBJECT_PATH is 'stLabel2.stLabel' and OBJECT_NAME is 'bLabel.'	• RELATED: Data related to global labels exists. • Blank: No global labels are used.
ACCESS_RIGHTS	Access right	The access right for an object[1]. This column is used when OBJECT_TYPE is "TAG" or "MEMBER."	• READ: Reading • WRITE: Writing • READWRITE: Reading and writing • Blank: Reading and writing (on import only)
DATA_TYPE	Data type	The data type of an object[1]. This column is used when OBJECT_TYPE is "TAG" or "MEMBER." For "MEMBER," this item must match the data type (DATA_TYPE) of the member of the corresponding structure definition on import. Data types that can be specified differ depending on OBJECT_TYPE. ■When OBJECT_TYPE is "TAG" BOOL, INT, UINT, DINT, UDINT, REAL, LREAL, TIME, STRING, WSTRING, or blank ■When OBJECT_TYPE is "MEMBER" BOOL, INT, UINT, DINT, UDINT, REAL, LREAL, TIME, STRING, WSTRING, or STRUCT Also, data types that can be specified differ depending on a device specified for ADDRESS. For details, refer to the following: ☞ Page 37 Setting availability of data types for each device When using an array (Array of ~), store the number of elements in DIMENSION_1, DIMENSION_2, and DIMENSION_3.	• BOOL: Logical type • INT: Signed 16-bit integer type • UINT: Unsigned 16-bit integer type • DINT: Signed 32-bit integer type • UDINT: Unsigned 32-bit integer type • REAL: 32-bit floating point type • LREAL: 64-bit floating point type • TIME: Time type • STRING: ASCII string type • WSTRING: Unicode (UTF-16) string type • STRUCT: Structure • Blank: Not specified (Not Assigned)
POLLING_METHOD	Polling method	The name of a polling definition. This column is used when OBJECT_TYPE is "TAG" or "STRUCT."	• ASCII character • 1 to 50 characters • Blank: Polling definition with 'use as default polling rate' enabled (on import only)
ENABLE_TAG	Enabling a tag	Whether a tag is enabled or disabled. This column is used when OBJECT_TYPE is "TAG" or "STRUCT."	• ENABLE: Enabled • DISABLE: Disabled • Blank: Enabled (on import only)

Column name	Overview	Description	Setting value
SWAP_ORDER	Byte order swap	Whether the byte order swap is enabled or disabled. This column is used when OBJECT_TYPE is "TAG" or "MEMBER."	• ENABLE: Enabled • DISABLE: Disabled • Blank: Disabled (on import only)
CONVERT_TO_WORD	Conversion to the word size	Whether conversion to the word size is enabled or disabled. This column is used when OBJECT_TYPE is "TAG" or "MEMBER."	• ENABLE: Enabled • DISABLE: Disabled • Blank: Disabled (on import only)
CONVERSION	Conversion	The name of a conversion definition. This column is used when OBJECT_TYPE is "TAG" or "MEMBER."	• ASCII character • 1 to 50 characters (when using a conversion definition) • Blank: No conversion definitions are used.
DIMENSION_1	One dimension	The number of elements in the first dimension of an array.[*4] This column is used when OBJECT_TYPE is "TAG," "STRUCT," or "MEMBER." For "MEMBER," this item must match the number of one-dimensional elements (DIMENSION_1) of the member of the corresponding structure definition on import. ■When OBJECT_TYPE is "TAG" • A value is stored when DATA_TYPE is BOOL, INT, UINT, DINT, UDINT, REAL, LREAL, or TIME and an array is used. • The number of characters is stored when DATA_TYPE is STRING or WSTRING. ■When OBJECT_TYPE is "MEMBER" • A value is stored when DATA_TYPE is BOOL, INT, UINT, DINT, UDINT, REAL, LREAL, TIME, or STRUCT and an array is used. • The number of characters is stored when DATA_TYPE is STRING or WSTRING. ■When OBJECT_TYPE is "STRUCT" • A value is stored when an array is used. The value ranges in the right column also apply to the product of DIMENSION_1, DIMENSION_2, and DIMENSION_3 (excluding dimensions with '0').	• Numeral ■When OBJECT_TYPE is "TAG" or "MEMBER" • 1 to 40960 (when DATA_TYPE is BOOL, INT, or UINT)[*5] • 1 to 20480 (when DATA_TYPE is UDINT, DINT, TIME, or REAL) • 1 to 10240 (when DATA_TYPE is LREAL) • 1 to 5120 (when DATA_TYPE is STRUCT) • 1 to 255 (when DATA_TYPE is STRING or WSTRING) • Blank: No arrays are used. ■When OBJECT_TYPE is "STRUCT" • 1 to 5120 (when using an array) • Blank: No arrays are used.
DIMENSION_2	Two dimensions	The number of elements in the second dimension of an array.[*4] This column is used when OBJECT_TYPE is "TAG," "STRUCT," or "MEMBER." For "MEMBER," this item must match the number of two-dimensional elements (DIMENSION_2) of the member of the corresponding structure definition on import. A value is stored when a value for DIMENSION_1 is 1 or more and a two or more-dimensional array is used. The value ranges in the right column also apply to the product of DIMENSION_1, DIMENSION_2, and DIMENSION_3 (excluding dimensions with '0').	• Numeral ■When OBJECT_TYPE is "TAG" or "MEMBER" • 1 to 40960 (when DATA_TYPE is BOOL, INT, or UINT)[*5] • 1 to 20480 (when DATA_TYPE is UDINT, DINT, TIME, or REAL) • 1 to 10240 (when DATA_TYPE is LREAL) • 1 to 5120 (when DATA_TYPE is STRUCT) • Blank: Neither arrays nor two (three) or more-dimensional arrays are used, or DATA_TYPE is STRING or WSTRING. ■When OBJECT_TYPE is "STRUCT" • 1 to 5120 (when using an array) • Blank: No arrays are used.
DIMENSION_3	Three dimensions	The number of elements in the third dimension of an array.[*4] This column is used when OBJECT_TYPE is "TAG," "STRUCT," or "MEMBER." For "MEMBER," this item must match the number of three-dimensional elements (DIMENSION_3) of the member of the corresponding structure definition on import. A value is stored when a value for DIMENSION_2 is 1 or more and a three-dimensional array is used. The value ranges in the right column also apply to the product of DIMENSION_1, DIMENSION_2, and DIMENSION_3 (excluding dimensions with '0').	
WORD_OFFSET	Word device offset	A structure array offset value for a word device. This column is used when OBJECT_TYPE is "STRUCT" and a value for DIMENSION_1 is 1 or more. This item can be set when DATA_TYPE is INT, UINT, DINT, UDINT, REAL, LREAL, STRING, or WSTRING, or when a TIME type structure member is included.[*6]	• Numeral • 0 to 99999: Offset specification • Blank: Automatic
BIT_OFFSET	Bit device offset	A structure array offset value for a bit device. This column is used when OBJECT_TYPE is "STRUCT" and a value for DIMENSION_1 is 1 or more. This item can be set when a structure member with DATA_TYPE of BOOL is included.[*6]	• Numeral • 0 to 99999: Offset specification • Blank: Automatic

*1 A generic term for tags, groups, structure labels, and members of a structure label
*2 For the list of accessible devices, refer to the following:
　　MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

*3   These items can be imported even if the names are not the same, but related data is released when updating the data after the import.

*4   Whether this item can be set differs depending on the combinations of devices specified for ADDRESS and data types specified for DATA_TYPE. For details on the combinations, refer to the following:
    ☞ Page 37 Setting availability of data types for each device

*5   When DATA_TYPE is "BOOL," the product of DIMENSION_1, DIMENSION_2, and DIMENSION_3 (excluding dimensions with '0') must be a multiple of 16.

*6   The applicable members do not need to be immediately under a structure label.
    (Example) For the structure label 'Struct000' with the following hierarchies, even if the member 'VAR00' immediately under the structure label is not of the BOOL type, bit device offset can be set if the member 'VAR01' of the member 'Struct001' is of the BOOL type.

```
Struct000 (structure) ─┬─ VAR00 (member)
                       │
                       └─ Struct001 (structure) ─── VAR01 (member)
```
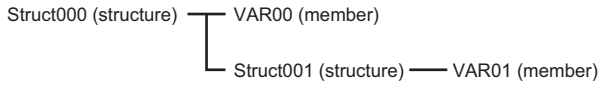
◇Description rules for structure labels

The following shows the description rules for structure labels in an ADDRESS_SPACE.CSV file.

• When a structure label is not an array
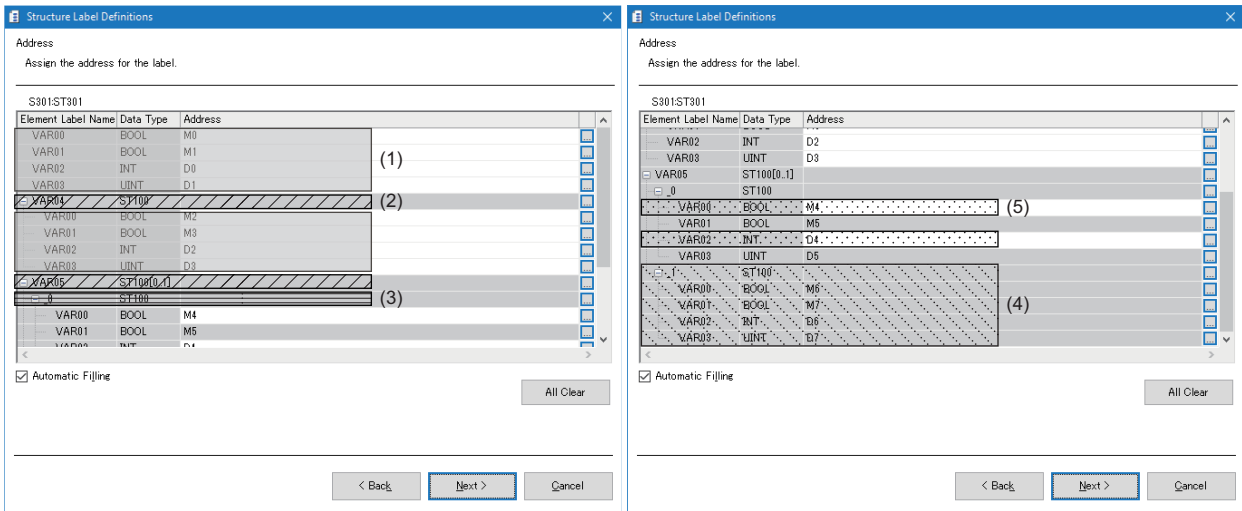
ADDRESS_SPACE.CSV (some columns excerpted)

OBJECT_PATH	OBJECT_NAME	OBJECT_TYPE	STRUCTURE	ADDRESS	DATA_TYPE	DIMENSION_1
	S301	STRUCT	ST301			
S301	VAR00	MEMBER		M0	BOOL	
S301	VAR01	MEMBER		M1	BOOL	
S301	VAR02	MEMBER		D0	INT	
S301	VAR03	MEMBER		D1	UINT	
S301	VAR04	MEMBER	ST100		STRUCT	
S301.VAR04	VAR00	MEMBER		M2	BOOL	
S301.VAR04	VAR01	MEMBER		M3	BOOL	
S301.VAR04	VAR02	MEMBER		D2	INT	
S301.VAR04	VAR03	MEMBER		D3	UINT	
S301	VAR05	MEMBER	ST100		STRUCT	2
S301.VAR05	VAR00	MEMBER		M4	BOOL	
S301.VAR05	VAR01	MEMBER		M5[1]	BOOL	
S301.VAR05	VAR02	MEMBER		D4	INT	
S301.VAR05	VAR03	MEMBER		D5[1]	UINT	

| No.	Description
(1)	Describe the addresses (ADDRESS) of all members other than structure arrays.[2]
(2)	For a member of a structure, describe "MEMBER" for OBJECT_TYPE, "STRUCT" for DATA_TYPE, and a structure name for STRUCTURE. For a structure array, describe a setting value for DIMENSION_1 and later.
(3)	Do not describe an index of a structure array.
(4)	Do not describe anything other than the first element (member under _0) of a structure array.[3]
(5)	For the address of a member of a structure array, describe the first bit device or word device only.[2]

[1] Output on export but not referenced on import. Note that a log file for a warning or error is output in cases such as when a value unavailable for device representation is set.

[2] When not assigning an address to a member, the description for ADDRESS of the member or the row itself can be omitted.

[3] The setting values for ACCESS_RIGHTS, SWAP_ORDER, CONVERT_TO_WORD, and CONVERSION of the first element also apply to other elements on import.

• When a structure label is an array
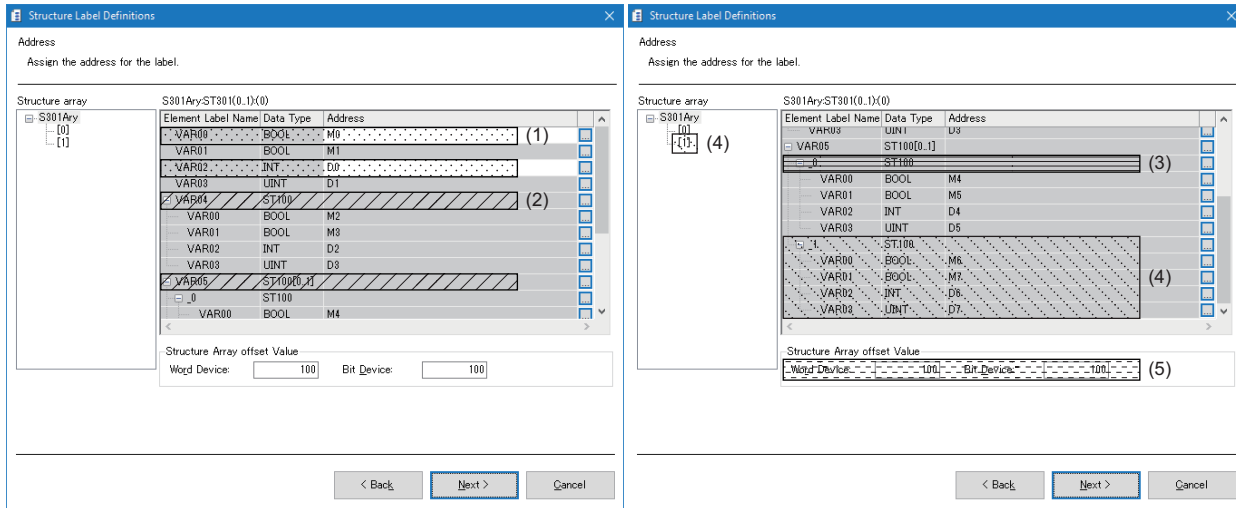
ADDRESS_SPACE.CSV (some columns excerpted)

OBJECT_PATH	OBJECT_NAME	OBJECT_TYPE	STRUCTURE	ADDRESS	DATA_TYPE	DIMENSION_1	WORD_OFFSET	BIT_OFFSET
	S301Ary	STRUCT	ST301			2	100	100
S301Ary	VAR00	MEMBER		M0	BOOL			
S301Ary	VAR01	MEMBER		M1[*1]	BOOL			
S301Ary	VAR02	MEMBER		D0	INT			
S301Ary	VAR03	MEMBER		D1[*1]	UINT			
S301Ary	VAR04	MEMBER	ST100		STRUCT			
S301Ary.VAR04	VAR00	MEMBER		M2[*1]	BOOL			
S301Ary.VAR04	VAR01	MEMBER		M3[*1]	BOOL			
S301Ary.VAR04	VAR02	MEMBER		D2[*1]	INT			
S301Ary.VAR04	VAR03	MEMBER		D3[*1]	UINT			
S301Ary	VAR05	MEMBER	ST100		STRUCT	2		
S301Ary.VAR05	VAR00	MEMBER		M4[*1]	BOOL			
S301Ary.VAR05	VAR01	MEMBER		M5[*1]	BOOL			
S301Ary.VAR05	VAR02	MEMBER		D4[*1]	INT			
S301Ary.VAR05	VAR03	MEMBER		D5[*1]	UINT			

No.	Description
(1)	For the address of a member of a structure label, describe the first bit device or word device only.[*2]
(2)	For a member of a structure, describe "MEMBER" for OBJECT_TYPE, "STRUCT" for DATA_TYPE, and a structure name for STRUCTURE. For a structure array, describe a setting value for DIMENSION_1 and later.
(3)	Do not describe an index of a structure array.
(4)	Do not describe anything other than the first element (member under _0) of a structure array.[*3]
(5)	A structure array offset value can be specified.

*1 Output on export but not referenced on import. Note that a log file for a warning or error is output in cases such as when a value unavailable for device representation is set.

*2 When not assigning an address to a member, the description for ADDRESS of the member or the row itself can be omitted.

*3 The setting values for ACCESS_RIGHTS, SWAP_ORDER, CONVERT_TO_WORD, and CONVERSION of the first element also apply to other elements on import.

■STRUCTURE.CSV

Column name	Overview	Description	Setting value
OBJECT_PATH	Path to an object	The path to an object[1]. This column is used when OBJECT_TYPE is "MEMBER." The path is OBJECT_NAME of the structure to which an object belongs. (Example) For the following structure definition 'Struct001' • OBJECT_PATH of an object with OBJECT_NAME of 'Struct001': Blank • OBJECT_PATH of an object with OBJECT_NAME of 'VAR01': Struct001 'VAR00' is a member of the structure definition 'Struct000'; therefore, it is not described as a member of the structure definition 'Struct001.'	• ASCII character • 0 to 256 characters
OBJECT_NAME	Object name	The name of an object[1]	• ASCII character • 1 to 256 characters
OBJECT_TYPE	Object type	The type of an object[1]. A structure or a member of the structure is specified.	• STRUCT: Structure • MEMBER: Member of a structure
DESCRIPTION	Description or comment	The description or comment for an object[1]	• Unicode character • 0 to 128 characters
REMARK	Remarks	The remarks for an object[1]	• Unicode character • 0 to 128 characters
DATA_TYPE	Data type	The data type of a member of a structure. This column is used when OBJECT_TYPE is "MEMBER." The number of elements is stored in DIMENSION_1, DIMENSION_2, and DIMENSION_3 when an array is used.	• BOOL: Logical type • INT: Signed 16-bit integer type • UINT: Unsigned 16-bit integer type • DINT: Signed 32-bit integer type • UDINT: Unsigned 32-bit integer type • REAL: 32-bit floating point type • LREAL: 64-bit floating point type • TIME: Time type • STRING: ASCII string type • WSTRING: Unicode (UTF-16) string type • STRUCT: Structure
STRUCTURE	Structure name	The name of a structure. This column is used when OBJECT_TYPE is "MEMBER" and DATA_TYPE is "STRUCT."	• ASCII character • 1 to 256 characters
DIMENSION_1	One dimension	The number of elements in the first dimension of an array. This column is used when OBJECT_TYPE is "MEMBER." A value is stored when an array is used or DATA_TYPE is "STRING" or "WSTRING." The value ranges in the right column also apply to the product of DIMENSION_1, DIMENSION_2, and DIMENSION_3 (excluding dimensions with '0').	• Numeral • 1 to 40960 (when DATA_TYPE is BOOL, INT, or UINT)[2] • 1 to 20480 (when DATA_TYPE is UDINT, DINT, TIME, or REAL) • 1 to 10240 (when DATA_TYPE is LREAL) • 1 to 5120 (when DATA_TYPE is STRUCT) • 1 to 255 (when DATA_TYPE is STRING or WSTRING) • Blank: No arrays are used.

Column name	Overview	Description	Setting value
DIMENSION_2	Two dimensions	The number of elements in the second dimension of an array. This column is used when OBJECT_TYPE is "MEMBER." A value is stored when a value for DIMENSION_1 is 1 or more and a two or more-dimensional array is used. The value ranges in the right column also apply to the product of DIMENSION_1, DIMENSION_2, and DIMENSION_3 (excluding dimensions with '0').	• Numeral • 1 to 40960 (when DATA_TYPE is BOOL, INT, or UINT)[2] • 1 to 20480 (when DATA_TYPE is UDINT, DINT, TIME, or REAL) • 1 to 10240 (when DATA_TYPE is LREAL) • 1 to 5120 (when DATA_TYPE is STRUCT) • Blank: Neither arrays nor two (three) or more-dimensional arrays are used, or DATA_TYPE is STRING or WSTRING.
DIMENSION_3	Three dimensions	The number of elements in the third dimension of an array. This column is used when OBJECT_TYPE is "MEMBER." A value is stored when a value for DIMENSION_2 is 1 or more and a three-dimensional array is used. The value ranges in the right column also apply to the product of DIMENSION_1, DIMENSION_2, and DIMENSION_3 (excluding dimensions with '0').	

*1 A generic term for structures and their members

*2 When DATA_TYPE is "BOOL," the product of DIMENSION_1, DIMENSION_2, and DIMENSION_3 (excluding dimensions with '0') must be a multiple of 16.

■TARGET_DEVICE.CSV

Column name	Overview	Description	Setting value
TARGET_DEVICE_NAME	Name	The name of an access target device	• ASCII character • 1 to 256 characters
DESCRIPTION	Description	The description for an access target device	• Unicode character • 0 to 128 characters
HOST_MODULE_TYPE	Module type of an access source system	The module type of an access source system. A blank cannot be set when CPU_SERIES is "QCPU" or "LCPU."	• DIRECT_ETHERNET: Built-in Ethernet port [CH2] (connect to an Ethernet module) • DIRECT_CPU: Built-in Ethernet port [CH2] (connect to a CPU module (Ethernet port)) • ETHERNET: Ethernet module • CCIECONT: CC-Link IE Control module • CCIEFIELD: CC-Link IE Field module • CCLINK: CC-Link module • Blank: Not set (own station)
HOST_STATION_NO	Station number of an access source system	The station number of an access source system. This column is used when HOST_MODULE_TYPE is "DIRECT_ETHERNET."	• Numeral • 0 to 120
HOST_START_IO_NO	Start I/O number of an access source system	The start I/O number of an access source system. This column is used when HOST_MODULE_TYPE is "CCLINK."	• Numeral (hexadecimal) • 0 to FE0 (in 10-point units)
HOST_TIME_OUT	Timeout of an access source system	The timeout time of communication with an access target device	• Numeral • 0 to 65535 • Blank: 3000 (on import only)
IP_ADDRESS	IP address of an access target (relay station) system	The IP address of a module in an access target (relay station) system. This column is used when HOST_MODULE_TYPE is "DIRECT_ETHERNET" or "DIRECT_CPU."	• IP address
RELAY_NETWORK_NO	Network number of an access target (relay station) system	The network number of an access target (relay station) system. This column is used when HOST_MODULE_TYPE is "DIRECT_ETHERNET," "ETHERNET," "CCIECONT," or "CCIEFIELD."	• Numeral • 1 to 239
RELAY_STATION_NO	Station number of an access target (relay station) system	The station number of an access target (relay station) system. This column is used when HOST_MODULE_TYPE is "DIRECT_ETHERNET," "ETHERNET," "CCIECONT," "CCIEFIELD," or "CCLINK."	• Numeral • 0 to 120 • 0 to 63 (when HOST_MODULE_TYPE is CCLINK)
RELAY_MODULE_TYPE	Module type of an access target (relay station) system	The type of a module routed when accessing another system. This column is used when HOST_MODULE_TYPE is "DIRECT_ETHERNET," "DIRECT_CPU," "ETHERNET," "CCIECONT," "CCIEFIELD," or "CCLINK." Module types that can be specified differ depending on HOST_MODULE_TYPE. ■For DIRECT_ETHERNET ETHERNET_CCLINK or blank ■For DIRECT_CPU and CCLINK ETHERNET, CCIECONT, CCIEFIELD, or blank ■For ETHERNET, CCIECONT, and CCIEFIELD CCLINK or blank	• ETHERNET_CCLINK: Ethernet/CC-Link IE Control/CC-Link IE Field • ETHERNET: Ethernet module • CCIECONT: CC-Link IE Control module • CCIEFIELD: CC-Link IE Field module • CCLINK: CC-Link module • Blank: No routed module
RELAY_START_IO_NO	Start I/O number of an access target (relay station) system	The start I/O number of a module routed when accessing another system. This column is used when RELAY_MODULE_TYPE is "CCLINK."	• Numeral (hexadecimal) • 0 to FE0 (in 10-point units)
CPU_SERIES	CPU series of an access target (target station) system	The series of a CPU module in an access target (target station) system. This column is used when HOST_MODULE_TYPE is "DIRECT_ETHERNET," "DIRECT_CPU," "ETHERNET," "CCIECONT," "CCIEFIELD," or "CCLINK."	• RCPU: iQ-R series • QCPU: Q series • LCPU: L series
MULTI_CPU	Multiple CPU specification in an access target (target station) system	The CPU number when an access target (target station) system is a multiple CPU system	• 1: CPU No.1 • 2: CPU No.2 • 3: CPU No.3 • 4: CPU No.4 • Blank: Not specified

Column name	Overview	Description	Setting value
TARGET_NETW ORK_NO	Network number of an access target (target station) system	The network number of an access target (target station) system. This column is used when RELAY_MODULE_TYPE is "ETHERNET_CCLINK," "ETHERNET," "CCIECONT," or "CCIEFIELD."	• Numeral • 1 to 239
TARGET_STATIO N_NO	Station number of an access target (target station) system	The station number of an access target (target station) system. This column is used when RELAY_MODULE_TYPE is "ETHERNET_CCLINK," "ETHERNET," "CCIECONT," "CCIEFIELD," or "CCLINK."	• Numeral • 0 to 120 • 0 to 63 (when RELAY_MODULE_TYPE is CCLINK)
ENABLE_DEVIC E	Enabling	Whether the connection to an access target device is enabled or disabled. If it is disabled, no connection is established from an OPC UA server module to an access target device, and no tag information is acquired either.	• ENABLE: Enabled • DISABLE: Disabled • Blank: Enabled (on import only)
LABEL_IMPORT_ SOURCE	Import source setting for global labels and common device comments	The absolute path to a GX Works3 project from which global labels and common device comments are imported	• Character available for file paths in Windows • 1 to 260 characters (when using global labels and common device comments) • Blank: No global labels or common device comments are used.
LABEL_UPDATE	Updating data related to global labels from a module	Whether the function for updating data related to global labels from a module is enabled or disabled. This column is used when LABEL_IMPORT_SOURCE is not blank.	• ENABLE: Enabled • DISABLE: Disabled • Blank: Enabled (on import only)
LABEL_CHANGE _DATE	Last update date and time of a global label	The last update date and time of a file specified for LABEL_IMPORT_SOURCE. This setting value is exported but not to be imported.	• yyyy/MM/dd hh:mm:ss.sss

■CONVERSION.CSV

Column name	Overview	Description	Setting value
CONVERSION_N AME	Name	The name of a conversion definition	• ASCII character • 1 to 50 characters
CONVERSION_T YPE	Conversion type	The type of conversion	• LINEAR: Linear • SQRT: Square root • Blank: None (double type)
ENGINEERING_ UNIT_L	Engineering unit (EU) minimum value	The minimum value of the engineering unit. This column is used when CONVERSION_TYPE is "LINEAR" or "SQRT." A value smaller than ENGINEERING_UNIT_H is stored.	• Numeral (including decimal and exponent notations) • $\pm1.79769313486231E+308$[*1] • Blank: 0 (on import only)
ENGINEERING_ UNIT_H	Engineering unit (EU) maximum value	The maximum value of the engineering unit. This column is used when CONVERSION_TYPE is "LINEAR" or "SQRT." A value larger than ENGINEERING_UNIT_L is stored.	• Numeral (including decimal and exponent notations) • $\pm1.79769313486231E+308$ [*1] • Blank: 100 (on import only)
INSTRUMENT_R ANGE_L	Instrument range (IR) minimum value	A device value equivalent to the minimum value of the engineering unit. This column is used when CONVERSION_TYPE is "LINEAR" or "SQRT." A value smaller than INSTRUMENT_RANGE_H is stored.	• Numeral (including decimal and exponent notations) • $\pm1.79769313486231E+308$[*1] • Blank: 0 (on import only)
INSTRUMENT_R ANGE_H	Instrument range (IR) maximum value	A device value equivalent to the maximum value of the engineering unit. This column is used when CONVERSION_TYPE is "LINEAR" or "SQRT." A value larger than INSTRUMENT_RANGE_L is stored.	• Numeral (including decimal and exponent notations) • $\pm1.79769313486231E+308$[*1] • Blank: 10000 (on import only)
CLAMPING_TYP E	Clamping type	The type of clamping. This column is used when CONVERSION_TYPE is "LINEAR" or "SQRT."	• ENGINEERING_UNIT: Engineering unit • DETAILS: Details • Blank: None
CLAMPING_RAN GE_L	Clamping range minimum value	The minimum value of clamping. This column is used when CONVERSION_TYPE is "LINEAR" or "SQRT" and CLAMPING_TYPE is "DETAILS." A value smaller than CLAMPING_RANGE_H is stored.	• Numeral (including decimal and exponent notations) • $\pm1.79769313486231E+308$[*1] • Blank: 0 (on import only)
CLAMPING_RAN GE_H	Clamping range maximum value	The maximum value of clamping. This column is used when CONVERSION_TYPE is "LINEAR" or "SQRT" and CLAMPING_TYPE is "DETAILS." A value larger than CLAMPING_RANGE_L is stored.	• Numeral (including decimal and exponent notations) • $\pm1.79769313486231E+308$[*1] • Blank: 100 (on import only)

*1 A value with an absolute value less than 4.94065645841247E-324 is rounded to $\pm$4.94065645841247E-324 or 0.

■POLLING.CSV

Column name	Overview	Description	Setting value
POLLING_NAME	Name	The name of a polling definition	• ASCII character • 1 to 50 characters
USE_AS_DEFAULT	Using this setting as the initial setting	Whether to use this setting as the initial setting. Only one of set polling definitions can be enabled.	• ENABLE: Enabled • DISABLE: Disabled • Blank: Disabled (on import only)
RATE	Cycle	A polling cycle. A value is stored in 100 milliseconds.	• Numeral • 200 to 86400000 (in 100 units) • Blank: 1000 (on import only)

If there is no longer any polling definition with 'use as default polling rate' enabled after import, the operation is as follows:

POLLING.CSV

Name	Use as default polling rate	Import target
PollMethod000		○
PollMethod001		
PollMethod002	ENABLE	
PollMethod003		

Polling definition for an import destination

Name	Use as default polling rate
PollMethod000	ENABLE
PollMethod001	
PollMethod002	
PollMethod003	
PollMethod004	

Polling definition after import

Name	Use as default polling rate
PollMethod000	ENABLE
PollMethod001	
PollMethod002	
PollMethod003	
PollMethod004	

A polling definition with the same name is overwritten.

If there is no longer any polling definition with 'use as default polling rate' enabled after import, the setting for 'use as default polling rate' before the import is retained.

If there are two or more polling definitions with 'use as default polling rate' enabled after import, the operation is as follows:

POLLING.CSV

Name	Use as default polling rate	Import target
PollMethodA	ENABLE	○
PollMethodB		
PollMethodC	ENABLE	○
PollMethodD		○

Polling definition for an import destination

Name	Use as default polling rate
PollMethod000	ENABLE
PollMethod001	
PollMethod002	
PollMethod003	
PollMethod004	

If there are multiple items to be imported for which 'use as default polling rate' is "ENABLE," an item with the lowest row number is applied as the initial setting (ENABLE).

Polling definition after import

Name	Use as default polling rate
PollMethod000	
PollMethod001	
PollMethod002	
PollMethod003	
PollMethod004	
PollMethodA	ENABLE
PollMethodC	
PollMethodD	

If there are two or more polling definitions with 'use as default polling rate' enabled after import, 'use as default polling rate' is enabled only for a polling definition to be imported and disabled for the others.

A

■SECURITY.CSV

Column name	Overview	Description	Setting value
TOOL_USER_AUTH	User authentication for connection from the configuration tool	Whether to perform authentication with a user name and password when accessing an OPC UA server module from the configuration tool	• ENABLE: Enabled • DISABLE: Disabled • Blank: Enabled (on import only)
USER_AUTH_USER_CERT	Allowing certificate authentication	Whether to allow user authentication with a certificate when accessing an OPC UA server module from an OPC UA client	• ENABLE: Enabled • DISABLE: Disabled • Blank: Disabled (on import only)
USER_AUTH_USERNAME	Allowing user name/password authentication	Whether to allow user authentication with a user name and password when accessing an OPC UA server module from an OPC UA client	• ENABLE: Enabled • DISABLE: Disabled • Blank: Enabled (on import only)
USER_AUTH_ANONYMOUS	Allowing authentication by Anonymous	Whether to allow authentication by Anonymous (access from anonymous users) when accessing an OPC UA server module from an OPC UA client	• ENABLE: Enabled • DISABLE: Disabled • Blank: Enabled (on import only)
APP_AUTH_AUTO_EXCHANGE	Exchanging a certificate automatically	Whether to automatically exchange an application certificate for the connection from an OPC UA client. When exchanging a certificate automatically, an application certificate passed from a client is automatically registered in the trust list and the connection is allowed (low security).	• ENABLE: Enabled • DISABLE: Disabled • Blank: Disabled (on import only)

■USER_SETTING.CSV

Column name	Overview	Description	Setting value
USER_NAME	User name	The user name of a user account	• ASCII character • 6 to 32 characters
PASSWORD	Password	The password for a user account. This setting value is to be imported but not exported.	• ASCII character • 6 to 32 characters • Blank: This user is not to be imported.
CONFIGURATION_TOOL	Accessibility from the configuration tool	Whether an OPC UA server module can be accessed from the configuration tool	• ENABLE: Enabled (accessible) • DISABLE: Disabled (inaccessible) • Blank: Disabled (inaccessible) (on import only)
OPC_UA_CLIENT	Accessibility from an OPC UA client	Whether an OPC UA server module can be accessed from an OPC UA client	• ENABLE: Enabled (accessible) • DISABLE: Disabled (inaccessible) • Blank: Disabled (inaccessible) (on import only)

■NETWORK.CSV

Column name	Overview	Description	Setting value
CH1_IP_ADDRESS	IP address of the Ethernet port (CH1)	The IP address of the Ethernet port (CH1) of an OPC UA server module	• IP address • Blank: 192.168.3.3 (on import only)
CH1_SUBNET_MASK	Subnet mask of the Ethernet port (CH1)	The subnet mask of the Ethernet port (CH1) of an OPC UA server module	• IP address • Blank: 255.255.255.0 (on import only)
CH2_IP_ADDRESS	IP address of the Ethernet port (CH2)	The IP address of the Ethernet port (CH2) of an OPC UA server module	• IP address (when using the Ethernet port (CH2)) • Blank: The Ethernet port (CH2) is not used.
CH2_SUBNET_MASK	Subnet mask of the Ethernet port (CH2)	The subnet mask of the Ethernet port (CH2) of an OPC UA server module	• IP address (when using the Ethernet port (CH2)) • Blank[1]: The Ethernet port (CH2) is not used.
DEFAULT_GATEWAY_TYPE	Default gateway	A target for which a default gateway is set	• CH1: CH1 • CH2: CH2 • Blank: Not set
DEFAULT_GATEWAY_IP_ADDRESS	IP address of a default gateway	The IP address of a default gateway	• IP address • Blank[2]: Not set
HOST_NAME	Host name	The host name	• ASCII character[3] • 0 to 24 characters

[1] No blank allowed when an IP address is set for CH2_IP_ADDRESS.

[2] No blank allowed when DEFAULT_GATEWAY_TYPE is "CH1" or "CH2."

[3] Excluding lower-case characters. (If any lower-case character is included on import, it is automatically converted to an upper-case character.)

A

■OPCUA_SERVER.CSV

Column name	Overview	Description	Setting value
PORT_NO	Port number	The port number of an OPC UA server	• Numeral • 1024 to 65535 • Blank: 4840 (on import only)
END_POINT	Endpoint URL	The endpoint URL of an OPC UA server module. When changing PORT_NO and the IP address of the Ethernet port (CH1), the endpoint URL is also changed. The display format is as follows: • opc.tcp://IP address:port number (Example) opc.tcp://192.168.3.3:4840 This setting value is exported but not to be imported.	• ASCII character, :, /, and . (period)
AES256_SHA256_RSAPSS	Aes256-Sha256-RsaPss	Whether the security policy 'Aes256-Sha256-RsaPss' is enabled or disabled	• ENABLE: Enabled • DISABLE: Disabled • Blank: Enabled (on import only)
AES128_SHA256_RSAOAEP	Aes128-Sha256-RsaOaep	Whether the security policy 'Aes128-Sha256-RsaOaep' is enabled or disabled	• ENABLE: Enabled • DISABLE: Disabled • Blank: Enabled (on import only)
BASIC256SHA256	Basic256Sha256	Whether the security policy 'Basic256Sha256' is enabled or disabled	• ENABLE: Enabled • DISABLE: Disabled • Blank: Enabled (on import only)
BASIC256	Basic256	Whether the security policy 'Basic256' is enabled or disabled	• ENABLE: Enabled • DISABLE: Disabled • Blank: Disabled (on import only)
BASIC128RSA15	Basic128Rsa15	Whether the security policy 'Basic128Rsa15' is enabled or disabled	• ENABLE: Enabled • DISABLE: Disabled • Blank: Disabled (on import only)
SECURITY_MODE	Security mode	A security mode. If all the security policies are disabled, NONE is specified. If at least one security policy is enabled, SIGN or SIGN_ENCRYPT is specified.	• NONE: None • SIGN: Sign • SIGN_ENCRYPT: Sign & Encrypt • Blank: None or Sign (on import only)
OPCUA_SERVER_NAME	OPC UA server name	An OPC UA server name listed on a server certificate	• ASCII character • 1 to 256 characters • Blank: RD81OPC96
ORGANIZATION_NAME	Organization name	An organization name listed on a server certificate	• ASCII character • 1 to 256 characters • Blank: Organization (on import only)
ORGANIZATION_UNIT	Organization unit	An organization unit listed on a server certificate	• ASCII character • 1 to 256 characters • Blank: Unit (on import only)
LOCALITY	Locality name	A locality name listed on a server certificate	• ASCII character • 1 to 256 characters • Blank: Location (on import only)
STATE	State	A state listed on a server certificate	• ASCII character • 1 to 256 characters • Blank: State (on import only)
COUNTRY	Country name	A country name listed on a server certificate	• ASCII character[1] • 2 characters • Blank: JP (on import only)
DISCOVERY_SERVER_URL	Discovery server URL	The URL of a discovery server in which endpoint information of an OPC UA server module is registered	• ASCII character, :, /, and . (period) • 0 to 256 characters
REGISTRATION_INTERVAL	Registration interval	An interval for registering endpoint information in a discovery server (unit: ms)	• Numeral • 10000 to 999999 • Blank: 10000 (on import only)
LOG_OUTPUT	Outputting logs	Whether to output operation logs of an OPC UA server module to an SD memory card	• ENABLE: Enabled (output) • DISABLE: Disabled (not output) • Blank: Enabled (output) (on import only)

Column name	Overview	Description	Setting value
USE_CPU_WAIT	Specifying a waiting time for the module operation start	Whether to specify a waiting time until 'Module READY' (X0) turns ON after an OPC UA server module is ready	• ENABLE: Enabled (specified) • DISABLE: Disabled (not specified) • Blank: Disabled (not specified) (on import only)
WAITING_TIME	Waiting time	The waiting time until 'Module READY' (X0) turns ON (unit: s)	• Numeral • 0 to 255 • Blank: 0 (on import only)
REVERSE_DIME NSIONS	Reversing the dimensional order of multidimensional arrays	Whether to reverse the dimensional order of multidimensional array elements. When enabled, the dimensional order of multidimensional arrays is changed from ascending to descending. This setting applies to the following settings: • Multidimensional array tag • Structure label with the data type other than a structure and including multidimensional arrays as structure members ■Operation on an OPC UA server module when enabled • Two-dimensional array: Object name [Two dimensions] [One dimension] • Three-dimensional array: Object name [Three dimensions] [Two dimensions] [One dimension] ■Operation on an OPC UA server module when disabled • Two-dimensional array: Object name [One dimension] [Two dimensions] • Three-dimensional array: Object name [One dimension] [Two dimensions] [Three dimensions] When using global labels with multidimensional arrays, disable this setting. Otherwise, the dimensional order of multidimensional arrays accessed from an OPC UA client will differ from global labels of a CPU module.	• ENABLE: Enabled (The dimensional order of multidimensional arrays is in descending order.) • DISABLE: Disabled (The dimensional order of multidimensional arrays is in ascending order.) • Blank: Disabled (The dimensional order of multidimensional arrays is in ascending order.) (on import only)

*1   Excluding lower-case characters. (If any lower-case character is included on import, it is automatically converted to an upper-case character.)

■export_info.txt
Format specifications

Item	Description
Character code	UTF-8 (with BOM)
Line feed code	CRLF (0x0D, 0x0A)
Output destination	A specified folder

Format overview

An export_info.txt file consists of repeating item names and setting values.

Ex.

```
[PROJECT NAME]
Untitled
[EXPORT DATE]
2022/03/08 13:16:05.728
[TOOL VERSION]
MX OPC UA Module Configurator-R Version 1.08J
```

Item specifications

Item	Description	Setting value
PROJECT NAME	Project name	■If a project file has been saved at least once File name of the project file (excluding the extension .mxcfg) ■If a project file has never been saved Untitled
EXPORT DATE	Export date and time	yyyy/MM/dd HH:mm:ss.fff
TOOL VERSION	Software version of MX OPC UA Module Configurator-R	MX OPC UA Module Configurator-R Version XX (XX indicates its version.)

Appendix 9 Log File Format

Communication event log file

This section shows the format of a communication event log between OPC UA server modules created by an OPC UA server module.

Format specifications

The format specifications are as follows:

Item	Description
Format	CSV format
Storage destination	/SD/SETTING/log
File name	YYYYMMDD-XXXX.log XXXX: Sequential number from 0000 to 9999
Character code	Shift JIS
Log output level	INFO or higher

Format overview

The format of a log file is as follows:

Item	Description
Date	The occurrence date of an event is displayed (YYYY-MM-DD).
Time	The occurrence time of an event is displayed (HH:MM:SS).
Category	The type of an event is displayed. • SYSTEM • COMM • OPCUA • UNIT
Level (number)	The level (number) of an event is displayed. • 1: DEBUG • 2: INFO • 3: WARNING • 4: ERROR
Level (character string)	The level (character string) of an event is displayed. • DEBUG • INFO • WARNING • ERROR
Output source	An output source of an event is displayed.
Message	The contents of an event are displayed.

Warning/error log file when importing a CSV file

If a created CSV file is not compliant with the specifications, a log file is output when importing the CSV file.

A warning or error description for the CSV file is displayed in the log file.

Note that a check is performed in stages; therefore, if an error is detected at one stage, a file is output without performing a check for the next stage.

Format specifications

The format specifications are as follows:

Item	Description
Character code	UTF-8 (with BOM)
Line feed code	CRLF (0x0D, 0x0A)
Output destination	A specified folder
File name	csv_import_yyyymmdd_hhmmssfff.log

Format overview

The output contents are as follows:

- [Type](tab)[Path to a CSV file]:[Row number]:[Corrective action]

Item		Description
Type		The type of a log message is displayed. • Warning: Some setting contents of a CSV file are incorrect but the file can be imported. • Error: Some setting contents of a CSV file are incorrect and the file cannot be imported.
Tab		—
Log message	Path to a CSV file	The path to a CSV file with incorrect setting contents is displayed.
	Colon	—
	Row number	The row number of a CSV file with incorrect setting contents is displayed.[*1] (Only for a warning or error for which the row number can be identified) (Example) For the third row: L.3
	Corrective action	Corrective action for the incorrect setting contents is displayed.[*2]

*1 If multiple rows are included in one setting as a result of including a line feed in a setting value in a CSV file, the minimum row number is displayed.
(Example) For a CSV file with the following contents, an error occurs because an unavailable character line feed is included in "POLLING2" and '100' is less than the minimum value of a cycle. The third and fourth rows are included in this setting, but '3' is displayed as a row number in a log message.

Row number	Description
1 (column name row)	POLLING_NAME,USE_AS_DEFAULT,RATE
2	POLLING1,ENABLE,1000
3	"PO
4	LLING2",DISABLE,100

*2 If a line feed is included in a displayed setting value (set by a user), it is replaced with a line feed code (\n or \r\n) and displayed.

■Output example

An output example for a log is as follows:

- ErrorC:\project file\TARGET_DEVICE.CSV:L.3:Set the number of characters for the column name 'TARGET_DEVICE_NAME' to 256 characters or less.

Appendix 10 Software Licenses and Copyrights

This section describes the licenses and copyrights of software used in this product.

Jansson 2.9

Copyright© 2009-2016 Petri Lehtinen

Released under the MIT license

http://opensource.org/licenses/mit-license.php

Openssl

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

■Copyright

Copyright© 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

This Windows version of this product includes software written by Tim Hudson (tjh@cryptsoft.com)

■LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts.

・OpenSSL License

Copyright© 1998-2016 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

• Original SSLeay License

Copyright© 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

OPC UA

This product includes code that was developed by Unified Automation GmbH for the OPC UA SDK (http://www.unifiedautomation.com/).

Copyright (c) 2006-2016 Unified Automation GmbH. All rights reserved.

The OPC UA SDK is based in part on the ANSI C Stack of the OPC Foundation. Initial version of the ANSI C Stack was founded and copyrighted by OPC Foundation, Inc.

Copyright (C) 2008, 2014 OPC Foundation, Inc., All Rights Reserved.

Appendix 11 Use in a Redundant System

To use an OPC UA server module in a redundant system, a system must be constructed for switching a monitoring target and the system when an error (disconnection between an OPC UA server module and an OPC UA client etc.) is detected in an OPC UA server module.

Switch a monitoring target in an OPC UA client, and create a sequence program for switching the system.

> **Point**
>
> There is no difference in operations of an OPC UA server module when used in each system in the following system configurations:
> - A redundant system and a non-redundant system
> - A control system and a standby system

> **Restriction**
>
> - For constructing a redundant system, use a process CPU with firmware version '18' or later.
> - Set a different IP address of an OPC UA server module for system A and system B.

Procedure for switching a monitoring target

The following shows the procedure for switching a monitoring target.

Switch a monitoring target in an OPC UA client.

Operating procedure

1. Connect to an OPC UA server module.

When the connection is successful, data in system A and system B is acquired.

If it fails, connect to the OPC UA server module again by referring to the following:

2. Switch a monitoring target according to the status of 'Control system judgment flag' (SM1634) of a process CPU (redundant mode).

Status of 'Control system judgment flag' (SM1634)		Monitoring target
System A	System B	
ON	OFF	OPC UA server module in system A
OFF	ON	OPC UA server module in system B
OFF	OFF	No monitoring target Specify contents to display in an OPC UA client.

> **Point**
>
> For a sample (MC Works64) for displaying only data in the control system in an OPC UA client by using the control system judgment flag of a process CPU (redundant mode), refer to the following:
> ☞ Page 163 Example of switching a monitoring target (MC Works64)
> For details on system switching for a process CPU (redundant mode), refer to the following:
> 📖MELSEC iQ-R Process CPU Module User's Manual

Procedure for system switching

The following shows the procedure for system switching in a redundant system.

Switch the system in a sequence program.

Operating procedure

1. Monitor the status of an OPC UA server module.

An error is detected in any of the following cases:

- 'Module READY' (X0) is OFF.
- 'Module stop error status' (X10) is ON.
- 'Ethernet port status' (X5) is OFF for a certain period of time.

2. If an error is detected, execute the system switching instruction.

Execute the system switching instruction (SP.CONTSW) in a process CPU (redundant mode) in the control system.[*1]

*1 To execute this instruction, 'System switching by a user' (SM1646) must be turned ON in advance.

> **Point**
>
> For the sample program for monitoring the link-up state by using 'Ethernet port status' (X5) of an OPC UA server module and switching the system when the link-down is detected, refer to the following:
> ☞ Page 167 Sample program for system switching
> For details on system switching for a process CPU (redundant mode), refer to the following:
> 📖 MELSEC iQ-R Process CPU Module User's Manual

A

Operation example

The following shows an operation example when using an OPC UA server module in a redundant system.

System configuration

The following shows an example of a system configuration when using an OPC UA server module in a redundant system.
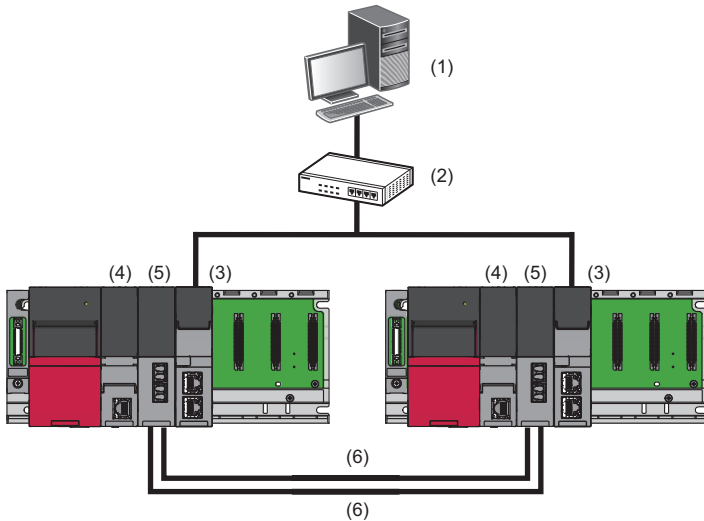
(1) OPC UA client
(2) Hub
(3) OPC UA server module
(4) Process CPU (redundant mode)[1]
(5) Redundant function module[1]
(6) Tracking cable[1]

*1   For details on a process CPU (redundant mode), refer to the following:
      📖MELSEC iQ-R Process CPU Module User's Manual

Example of switching a monitoring target (MC Works64)

The following shows an example of displaying only data in the control system in GraphWorX64 in the SCADA software package, MC Works64. To display only data in the control system in GraphWorX64, use Workbench for managing settings for each application of MC Works64.

■Settings for an OPC UA server module

Write the following settings in the configuration tool.

System	IP address	Access target device name	Communication setting	Tag name	Device	Remarks
A	192.168.3.3	Dev000	Own station (default)	CONT_SYS_FLAG	SM1634	Control system judgment flag
		Dev001	Own station (default)	TARGET	D0	Monitoring target (any)
B	192.168.3.4	Same as above				

■Settings for MC Works64

The following shows the procedure for displaying only data in the control system in GraphWorX64.

For details on MC Works64, refer to the following:

📖MC Works64 Version 4 Startup Manual

Operating procedure

1. Start Workbench.

2. Select "Platform Services" ⇨ "FrameWorX," and double-click "Global Search Settings."
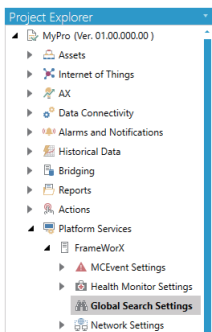
**3.** Select the checkbox of "Enable Global Search," and click the [Apply] button.

A
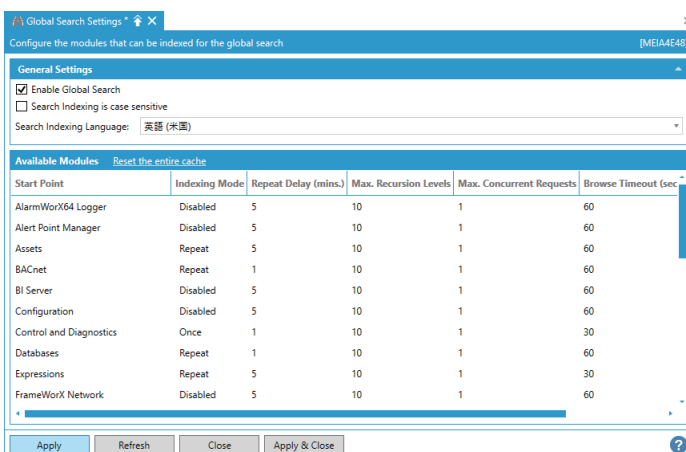
4. Select "Platform Services" ⇨ "FrameWorX" ⇨ "Network Settings," and double-click "OPC UA Network."
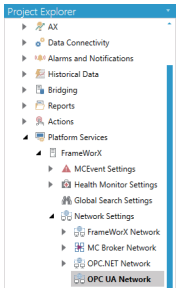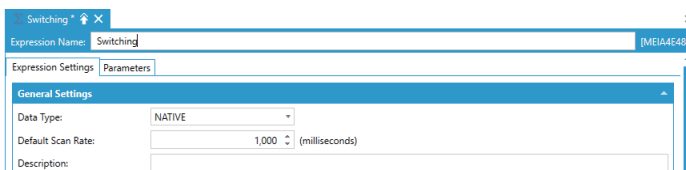

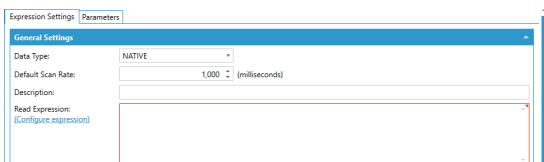**5.** Add an OPC UA server module for each system A and system B, and click the [Apply] button.
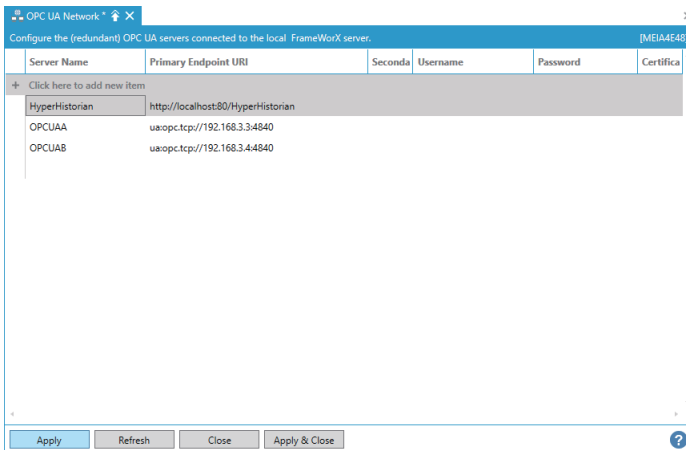
6. Select "Platform Services" ⇨ "Unified Data Manager" and right-click "Expressions," then select "Add Expression" from the shortcut menu.
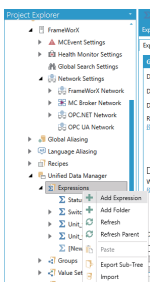
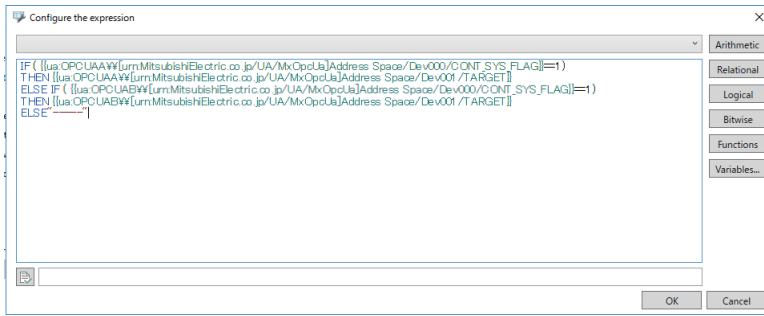**7.** Enter a name for "Expression Name."

8. Click "(Configure expression)" under "Read Expression" in the [Expression Settings] tab.

9. Enter an expression in the "Configure the expression" screen, and click the [OK] button.

For an expression to enter, refer to the following:

☞ Page 166 Expression example

Point 🔍

A variable can automatically be entered by clicking it in the "Configure the expression" screen and selecting a target tag under "OPC UA Network" in the "Data Points" screen.

(Example) Select "OPC UA Network" ⇨ "OPCUAA" ⇨ "Address Space" ⇨ "Dev000" ⇨ "CONT_SYS_FLAG" in the "Data Points" screen, and click the [OK] button.

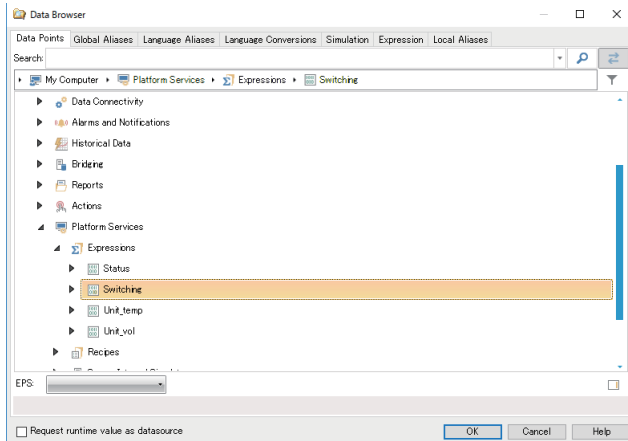The following is applied in the "Configure the expression" screen.

{{ua:OPCUAA\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]Address Space/Dev000/CONT_SYS_FLAG}}
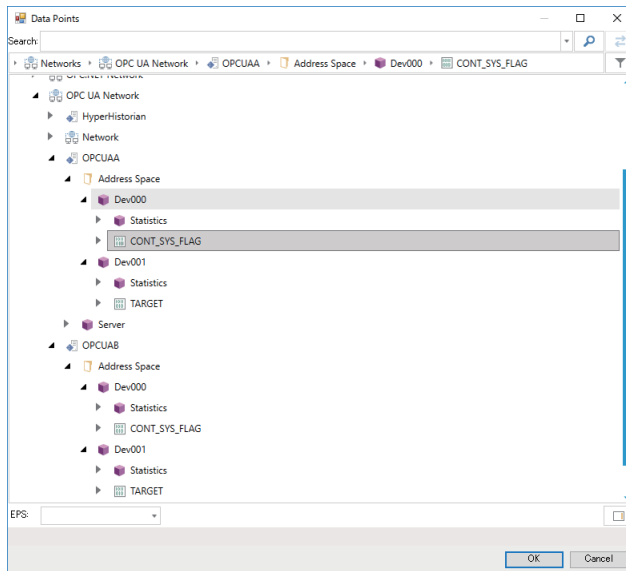
10. Start GraphWorX64.

A

11. Assign the expression created in step 9 to a data source such as a process point in the "Data Browser" screen.

The expression created in step 9 is displayed by selecting the following items:

👉 "Platform Services" ⇨ "Expressions"

■Expression example

The following shows an example of processing for switching a monitoring target by using the control system judgment flag.

x=IF({{ua:OPCUAA\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]Address Space/Dev000/CONT_SYS_FLAG}}==1)

THEN({{ua:OPCUAA\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]Address Space/Dev001/TARGET}})

ELSE IF({{ua:OPCUAB\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]Address Space/Dev000/CONT_SYS_FLAG}}==1)

THEN({{ua:OPCUAB\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]Address Space/Dev001/TARGET}})

ELSE("-----")

Item	Description
ua:OPCUAA\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]	An OPC UA server module added to an OPC UA network (system A)
ua:OPCUAB\\[urn:MitsubishiElectric.co.jp/UA/MxOpcUa]	An OPC UA server module added to an OPC UA network (system B)
Dev000	An access target device name set in the configuration tool (system A)
Dev001	An access target device name set in the configuration tool (system B)
CONT_SYS_FLAG	A tag name set in the configuration tool
TARGET	A tag name set in the configuration tool
"-------"	A character string displayed in GraphWorX64 when data missing occurs

Precautions

- When applying this sample program to an actual system, ensure the applicability and confirm that it will not cause system control problems.
- A character string displayed when data missing occurs may be displayed depending on the timing of system switching or system startup.
- Data update in an OPC UA server module and data collection (display) in MC Works64 are not synchronized.
- An OPC UA server module in system A and one in system B do not operate synchronously.

Sample program for system switching

The following shows the sample program for monitoring the link-up state by using 'Ethernet port status' (X5) of an OPC UA server module and switching the system in a process CPU (redundant mode) when link-down is detected.

■Settings for an OPC UA server module

For the setting method of an OPC UA server module, refer to the following:

■Settings for a process CPU (redundant mode)

The following shows the procedure for setting a process CPU (redundant mode).

Operating procedure

1. Start GX Works3.

2. Select [Project] ⇨ [New], and set the following items:

Item	Description
Series	RCPU
Type	R32P
Mode	Redundant
Program Language	Ladder

3. Add module labels.

4. Open the "Module Configuration" window, and set the following modules:

Slot	Module name	Start XY[1]
CPU	R32PCPU	3E00
0	R6RFM	0000
1	RD81OPC96	0020

*1 Select [Edit] ⇨ [Start XY Batch Input] to set this item.

5. Select [Edit] ⇨ [Parameter] ⇨ [Fix] to fix the parameters.

6. Add a module.

7. Set the redundant settings.

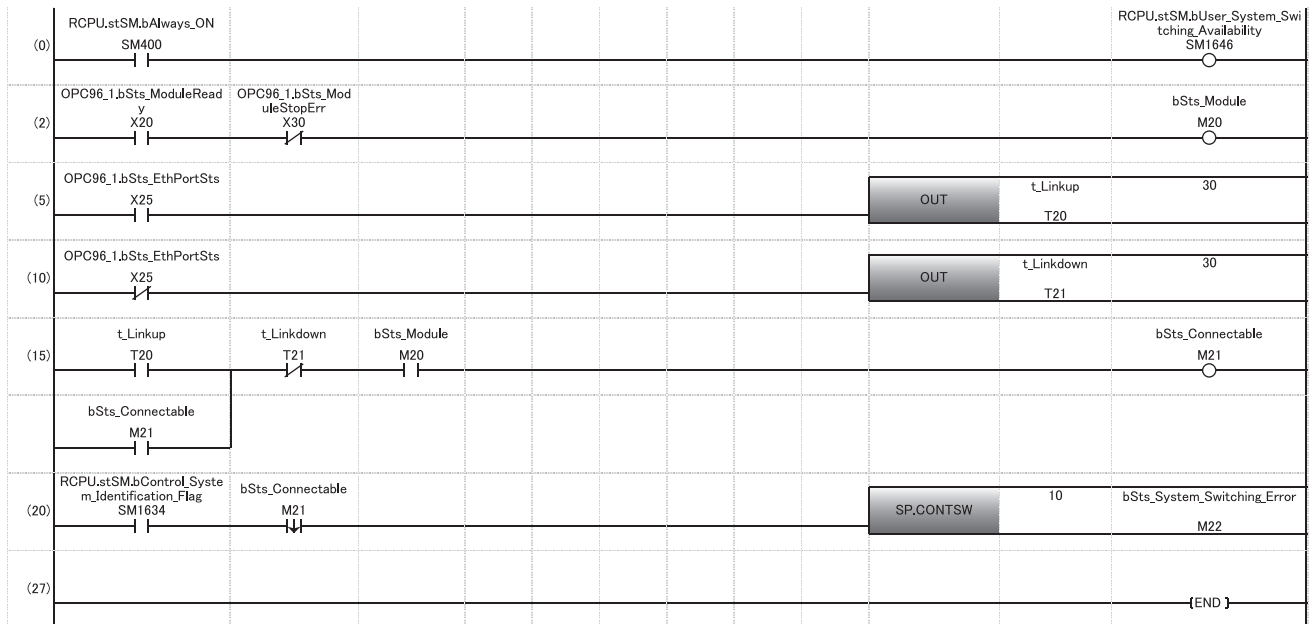For details on the redundant settings, refer to the following:

📖MELSEC iQ-R Process CPU Module User's Manual

8. Write the sample program for system switching.

■Devices used in the sample program for system switching

Category	Label name	Description	Device
Module labels	RCPU.stSM.bAlways_ON	Always ON	SM400
	RCPU.stSM.bControl_System_Identification_Flag	Control system judgment flag	SM1634
	RCPU.stSM.bUser_System_Switching_Availability	System switching by a user	SM1646
	bSts_ModuleReady	Module READY status	X20
	bSts_ModuleStopErr	Module stop error status	X30
	bSts_EthPortSts	Ethernet port status	X25
Global labels to be defined	Define global labels as follows:		

	Label Name	Data Type		Class	Assign (Device/Label)
1	bSts_Module	Bit	...	VAR_GLOBAL	M20
2	t_Linkup	Timer		VAR_GLOBAL	T20
3	t_Linkdown	Timer		VAR_GLOBAL	T21
4	bSts_Connectable	Bit		VAR_GLOBAL	M21
5	bSts_System_Switching_Error	Bit		VAR_GLOBAL	M22

■Sample program for system switching

(0)   Turns 'System switching by a user' (SM1646) ON.

(2)   Monitors the status of an OPC UA server module.[*1]

       Uses 'Module READY' (X0) and 'Module stop error status' (X10) of the OPC UA server module to set a condition used for system switching as an internal relay.

(5)   Monitors the Ethernet port status of the OPC UA server module.

       Sets a timer value used for link-up detection.[*1]

(10)   Monitors the Ethernet port status of the OPC UA server module.

       Sets a timer value used for link-down detection.[*1]

(15)   Monitors if the connection with the OPC UA client is available.

       Uses (2), (5), and (10) to set a condition used for system switching as an internal relay.

(20)   Executes the system switching instruction.

       Executes the system switching instruction when the internal relay set in the control system and (15) falls.

*1   Change a condition and a timer value used for system switching according to an environment.

Precautions

The following shows the considerations for using the sample program for system switching and programming for a redundant system.

■Considerations for using the sample program for system switching

- When applying this sample program to an actual system, ensure the applicability and confirm that it will not cause system control problems.
- 'Ethernet port status' (X5) of an OPC UA server module turns ON when link-up is detected in either of Ethernet port (CH1) or Ethernet port (CH2). When monitoring the status between an OPC UA server module and an OPC UA client, do not use Ethernet port (CH2) of an OPC UA server module.
- The link-up state of Ethernet port (CH1) of an OPC UA server module is used for system switching in this sample program. If a hub is used between an Ethernet port of an OPC UA server module and one of an OPC UA client, link-down between the Ethernet port of the OPC UA client and the hub cannot be detected.
- An OPC UA server module in system A and one in system B do not operate synchronously.
- The system is switched regardless of the status of an OPC UA server module in the standby system in this sample program.

■Considerations for programming for a redundant system

- Create a program executed in both systems.
- Exclude a device used for a program from targets for tracking transfer.

Appendix 12 Added and Changed Functions

This section shows the added and changed functions of an OPC UA server module and MX OPC UA Module Configurator-R.

Added/changed contents	Firmware version	Software version	Reference
Importing global labels and common device comments is supported.	—	'1.01B' or later	Page 63 Global Label and Common Device Comment Import Function
Structures and structure labels are supported.	'02' or later		Page 42 Structure label Page 53 Structure Definition Setting
Authentication with a user certificate is supported.			Page 55 Security Setting Page 86 User certificate management
A security policy is added. • Basic256Sha256			Page 59 OPC UA Server Setting
OPC UA specification 1.03 is supported.		—	📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
Multilevel structures[1] are supported.	'03' or later	'1.03D' or later	Page 42 Structure label Page 53 Structure Definition Setting
The firmware update function is supported.	'04' or later	'1.05F' or later	Page 87 Firmware update management 📖MELSEC iQ-R Module Configuration Manual
The global label-related data update function is supported by a module.	'06' or later	'1.06G' or later	Page 23 Global label-related data update function Page 32 Access target device
Device-unassigned global labels are supported.			—
Bit specification and digit specification are supported.			Page 35 Tag 📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
The time type is supported.			Page 35 Tag Page 54 Adding a member 📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
The number of structure members is increased.			📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
The number of monitored items per subscription is increased.		—	
The maximum numbers of array elements and characters are increased.		'1.06G' or later	
The number of name characters is increased.			
Security policies are added. • Aes256-Sha256-RsaPss • Aes128-Sha256-RsaOaep	'08' or later	'1.07H' or later	Page 18 Security policy Page 59 OPC UA Server Setting
Import and export for CSV files are supported.	'09' or later[2]	'1.08J' or later	Page 29 Importing a CSV file Page 31 Exporting a CSV file
OPC UA specification 1.04 is supported.	'09' or later		📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
Reversing the dimensional order of multidimensional arrays is supported.			Page 62 [Operation Setting] tab 📖MELSEC iQ-R OPC UA Server Module User's Manual (Startup)
Vulnerability measures are enhanced.	'10' or later	'1.09K' or later	—

A

Added/changed contents	Firmware version	Software version	Reference
The startup self-diagnostic setting is added.	'12' or later	—	Page 90 Basic Setting
OPC UA information models are supported.		'1.11M' or later	⌺MELSEC iQ-R OPC UA Server Module User's Manual (Information Model)
Windows 11 is supported.	—		⌺MELSEC iQ-R OPC UA Server Module User's Manual (Startup)

*1 Structures including a structure as a member
*2 Project files into which a CSV file is imported without setting the data type of a tag are supported. (When importing this type of CSV file in the configuration tool, Not Assigned is set for the data type of the tag and this type of tag is treated as invalid in a module.)

MEMO

INDEX

MEMO

I

REVISIONS

Revision date	*Manual number	Description
April 2017	SH(NA)-081694ENG-A	First edition
December 2018	SH(NA)-081694ENG-B	■Added or modified parts TERMS, Section 1.1, Section 2.3, Section 2.6, Section 2.7, Section 2.9, Section 2.10, Section 2.11, Section 4.3, Appendix 4, Appendix 5, Appendix 6, Appendix 10
February 2019	SH(NA)-081694ENG-C	Partial correction
May 2019	SH(NA)-081694ENG-D	■Added or modified parts Section 2.6, Appendix 9, Appendix 10, Appendix 11
April 2020	SH(NA)-081694ENG-E	■Added or modified parts Section 1.2, Section 2.11, Section 3.2, Section 4.5, Appendix 3, Appendix 4, Appendix 11
June 2020	SH(NA)-081694ENG-F	■Added or modified part Section 4.3
October 2020	SH(NA)-081694ENG-G	■Added or modified parts SAFETY PRECAUTIONS, CONDITIONS OF USE FOR THE PRODUCT, Section 4.4
July 2021	SH(NA)-081694ENG-H	■Added or modified parts Section 1.2, Section 2.3, Section 2.6, Section 2.10, Section 4.4, Section 4.5, Appendix 3, Appendix 4, Appendix 11
August 2021	SH(NA)-081694ENG-I	■Added or modified parts Section 2.9, Section 4.3, Appendix 11
December 2021	SH(NA)-081694ENG-J	■Added or modified parts Section 1.1, Section 2.9, Section 2.11, Section 4.3, Section 4.4, Appendix 11
December 2022	SH(NA)-081694ENG-K	■Added or modified parts Section 1.2, Section 2.2, Section 2.3, Section 2.9, Section 2.10, Section 2.11, Section 4.3, Section 4.4, Appendix 2, Appendix 4, Appendix 7, Appendix 8, Appendix 9, Appendix 12, COPYRIGHTS
May 2023	SH(NA)-081694ENG-L	■Added or modified parts Section 2.11, Section 4.3, Section 4.4, Appendix 12
September 2023	SH(NA)-081694ENG-M	■Added or modified parts Section 1.2, Section 4.4
April 2024	SH(NA)-081694ENG-N	■Added or modified parts Section 3.2, Appendix 12
May 2024	SH(NA)-081694ENG-O	■Added or modified parts INTRODUCTION, RELEVANT MANUALS, GENERIC TERMS AND ABBREVIATIONS, Section 1.2, Section 2.1, Section 2.2, Section 2.11, Section 4.3, Section 4.4, Appendix 3, Appendix 12

WARRANTY

Please confirm the following product warranty details before using this product.

1. Gratis Warranty Term and Gratis Warranty Range

If any faults or defects (hereinafter "Failure") found to be the responsibility of Mitsubishi occurs during use of the product within the gratis warranty term, the product shall be repaired at no cost via the sales representative or Mitsubishi Service Company.

However, if repairs are required onsite at domestic or overseas location, expenses to send an engineer will be solely at the customer's discretion. Mitsubishi shall not be held responsible for any re-commissioning, maintenance, or testing on-site that involves replacement of the failed module.

[Gratis Warranty Term]

The gratis warranty term of the product shall be for one year after the date of purchase or delivery to a designated place. Note that after manufacture and shipment from Mitsubishi, the maximum distribution period shall be six (6) months, and the longest gratis warranty term after manufacturing shall be eighteen (18) months. The gratis warranty term of repair parts shall not exceed the gratis warranty term before repairs.

[Gratis Warranty Range]

(1) The range shall be limited to normal use within the usage state, usage methods and usage environment, etc., which follow the conditions and precautions, etc., given in the instruction manual, user's manual and caution labels on the product.

(2) Even within the gratis warranty term, repairs shall be charged for in the following cases.

1. Failure occurring from inappropriate storage or handling, carelessness or negligence by the user. Failure caused by the user's hardware or software design.
2. Failure caused by unapproved modifications, etc., to the product by the user.
3. When the Mitsubishi product is assembled into a user's device, Failure that could have been avoided if functions or structures, judged as necessary in the legal safety measures the user's device is subject to or as necessary by industry standards, had been provided.
4. Failure that could have been avoided if consumable parts (battery, backlight, fuse, etc.) designated in the instruction manual had been correctly serviced or replaced.
5. Failure caused by external irresistible forces such as fires or abnormal voltages, and Failure caused by force majeure such as earthquakes, lightning, wind and water damage.
6. Failure caused by reasons unpredictable by scientific technology standards at time of shipment from Mitsubishi.
7. Any other failure found not to be the responsibility of Mitsubishi or that admitted not to be so by the user.

2. Onerous repair term after discontinuation of production

(1) Mitsubishi shall accept onerous product repairs for seven (7) years after production of the product is discontinued. Discontinuation of production shall be notified with Mitsubishi Technical Bulletins, etc.

(2) Product supply (including repair parts) is not available after production is discontinued.

3. Overseas service

Overseas, repairs shall be accepted by Mitsubishi's local overseas FA Center. Note that the repair conditions at each FA Center may differ.

4. Exclusion of loss in opportunity and secondary loss from warranty liability

Regardless of the gratis warranty term, Mitsubishi shall not be liable for compensation to:

(1) Damages caused by any cause found not to be the responsibility of Mitsubishi.

(2) Loss in opportunity, lost profits incurred to the user by Failures of Mitsubishi products.

(3) Special damages and secondary damages whether foreseeable or not, compensation for accidents, and compensation for damages to products other than Mitsubishi products.

(4) Replacement by the user, maintenance of on-site equipment, start-up test run and other tasks.

5. Changes in product specifications

The specifications given in the catalogs, manuals or technical documents are subject to change without prior notice.

INFORMATION AND SERVICES

For further information and services, please contact your local Mitsubishi Electric sales office or representative.
Visit our website to find our locations worldwide.

MITSUBISHI ELECTRIC Factory Automation Global Website
Locations Worldwide
www.MitsubishiElectric.com/fa/about-us/overseas/

TRADEMARKS

Intel is either a registered trademark or a trademark of Intel Corporation in the United States and/or other countries.
Microsoft and Windows are trademarks of the Microsoft group of companies.
Unicode is either a registered trademark or a trademark of Unicode, Inc. in the United States and other countries.
The company names, system names and product names mentioned in this manual are either registered trademarks or trademarks of their respective companies.
In some cases, trademark symbols such as '™' or '®' are not specified in this manual.

COPYRIGHTS

For the open source software used in this product, refer to the following:

MITSUBISHI ELECTRIC CORPORATION

When exported from Japan, this manual does not require application to the
Ministry of Economy, Trade and Industry for service transaction permission.

Specifications subject to change without notice.