OMRON

Machine Automation Controller

NJ/NX-series

CPU Unit
OPC UA

User's Manual

NJ501-1□00
NX102-□□□□

sysmac
always in control

Trademarks

- Sysmac and SYSMAC are trademarks or registered trademarks of OMRON Corporation in Japan and other countries for OMRON factory automation products.
- Microsoft, Windows, Excel, and Visual Basic are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.
- EtherCAT® is registered trademark and patented technology, licensed by Beckhoff Automation GmbH, Germany.
- ODVA, CIP, CompoNet, DeviceNet, and EtherNet/IP are trademarks of ODVA.
- The SD and SDHC logos are trademarks of SD-3C, LLC.

Other company names and product names in this document are the trademarks or registered trademarks of their respective companies.

Copyrights

Microsoft product screen shots reprinted with permission from Microsoft Corporation.

Introduction

Thank you for purchasing an NJ/NX-series CPU Unit.

This manual contains information that is necessary to use the OPC UA with the NJ/NX-series CPU Unit. Please read this manual and make sure you understand the functionality and performance of the NJ-series CPU Unit before you attempt to use it in a control system.

Keep this manual in a safe place where it will be available for reference during operation.

Intended Audience

This manual is intended for the following personnel, who must also have knowledge of electrical systems (an electrical engineer or the equivalent).

- Personnel in charge of introducing FA systems.
- Personnel in charge of designing FA systems.
- Personnel in charge of installing and maintaining FA systems.
- Personnel in charge of managing FA systems and facilities.

For programming, this manual is intended for personnel who understand the programming language specifications in international standard IEC 61131-3 or Japanese standard JIS B 3503.

Applicable Products

This manual covers the following products.

- NJ-series CPU Units NJ501-1□00 (Unit version 1.17 or later)
- NX-series CPU Units NX102-□□□□ (Unit version 1.30 or later)
- Sysmac Studio SYSMAC-SE2□□□
  (NJ501-1□00: version 1.21 or higher, NX102-□□□□: version 1.23 or higher)

Part of the specifications and restrictions for the CPU Units are given in other manuals. Refer to *Relevant Manuals* on page 2 and *Related Manuals* on page 19.

Relevant Manuals

The following table provides the relevant manuals for the NJ/NX-series CPU Units.
Read all of the manuals that are relevant to your system configuration and application before you use the NJ/NX-series CPU Unit.

The built-in EtherNet/IP port in the NJ/NX-series CPU Unit is used for this product.
For details on how to use the built-in EtherNet/IP port, refer to the *NJ/NX-series CPU Unit Built-in EtherNet/IP Port User's Manual* (Cat. No. W506)

Most operations are performed from the Sysmac Studio Automation Software. Refer to the *Sysmac Studio Version 1 Operation Manual* (Cat. No. W504) for information on the Sysmac Studio.
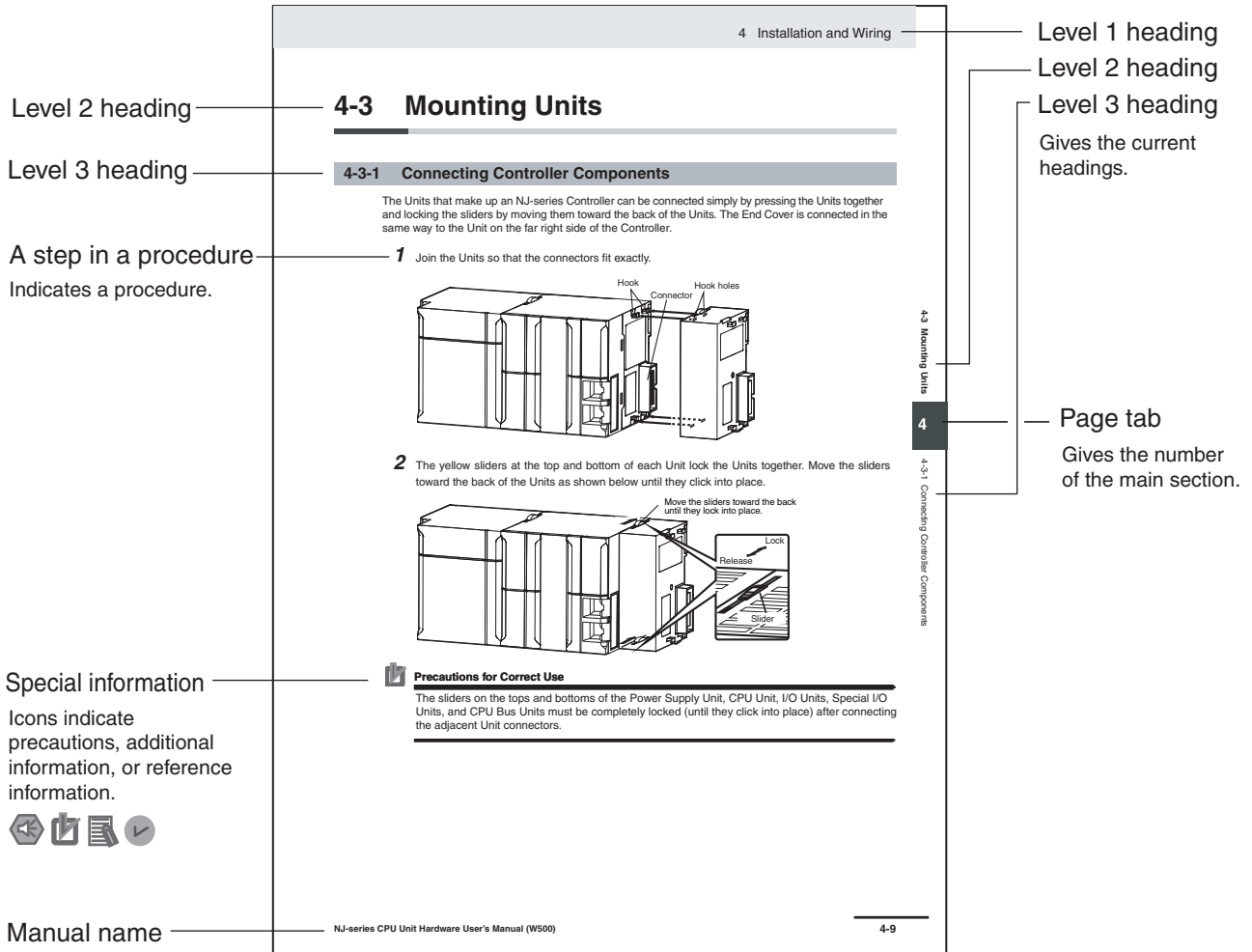
Purpose of use	Basic information				Manual					
	NJ-series CPU Unit Hardware User's Manual	NX-series NX102 CPU Unit Hardware User's Manual	NJ/NX-series CPU Unit Software User's Manual	NJ/NX-series Instructions Reference Manual	NJ/NX-series CPU Unit Motion Control User's Manual	NJ/NX-series Motion Control Instructions Reference Manual	NJ/NX-series CPU Unit Built-in EtherCAT Port User's Manual	NJ/NX-series CPU Unit Built-in EtherNet/IP Port User's Manual	NJ-series CPU Unit OPC UA User's Manual	NJ/NX-series Troubleshooting Manual
Introduction to NJ-series Controllers	●									
Introduction to NX102 CPU Units		●								
Setting devices and hardware										
Using motion control					●					
Using EtherCAT	●	●					●			
Using EtherNet/IP								●		
Software settings										
Using motion control					●					
Using EtherCAT			●				●			
Using EtherNet/IP								●		
Using OPC UA									●	
Writing the user program										
Using motion control					●	●				
Using EtherCAT			●	●			●			
Using EtherNet/IP								●		
Programming error processing										●
Using OPC UA									●	
Testing operation and debugging										
Using motion control					●					
Using EtherCAT			●				●			
Using EtherNet/IP								●		
Using OPC UA									●	
Learning about error management and corrections[1]	▲	▲	▲		▲		▲	▲		●
Maintenance										
Using motion control					●					
Using EtherCAT	●	●					●			
Using EtherNet/IP								●		

[1] Refer to the *NJ/NX-series Troubleshooting Manual* (Cat. No. W503) for the error management concepts and an overview of the error items. Refer to the manuals that are indicated with triangles for details on errors for the corresponding Units.

Manual Structure

Page Structure

The following page structure is used in this manual.

Level 2 heading

Level 3 heading

A step in a procedure
Indicates a procedure.

Special information
Icons indicate
precautions, additional
information, or reference
information.

Manual name

---

4   Installation and Wiring

4-3   Mounting Units

4-3-1   Connecting Controller Components

The Units that make up an NJ-series Controller can be connected simply by pressing the Units together and locking the sliders by moving them toward the back of the Units. The End Cover is connected in the same way to the Unit on the far right side of the Controller.

1 Join the Units so that the connectors fit exactly.

2 The yellow sliders at the top and bottom of each Unit lock the Units together. Move the sliders toward the back of the Units as shown below until they click into place.

Precautions for Correct Use

The sliders on the tops and bottoms of the Power Supply Unit, CPU Unit, I/O Units, Special I/O Units, and CPU Bus Units must be completely locked (until they click into place) after connecting the adjacent Unit connectors.

NJ-series CPU Unit Hardware User's Manual (W500)   4-9

Level 1 heading

Level 2 heading

Level 3 heading
Gives the current
headings.

Page tab
Gives the number
of the main section.

This illustration is provided only as a sample. It may not literally appear in this manual.

Special Information

Special information in this manual is classified as follows:

Precautions for Safe Use

Precautions on what to do and what not to do to ensure safe usage of the product.

Precautions for Correct Use

Precautions on what to do and what not to do to ensure proper operation and performance.

Additional Information

Additional information to read as required.
This information is provided to increase understanding or make operation easier.

Version Information

Information on differences in specifications and functionality for CPU Units with different unit versions and for different versions of the Sysmac Studio is given.

Note References are provided to more detailed or related information.

Precaution on Terminology

- In this manual, *built-in EtherNet/IP port* refers to the following port.
  - Built-in EtherNet/IP port of the NJ-series CPU Units NJ501-1□00
  - Built-in EtherNet/IP port (PORT 1) of the NX-series CPU Units NX102-□□□□
- In this manual, *download* refers to transferring data from the Sysmac Studio to the physical Controller and *upload* refers to transferring data from the physical Controller to the Sysmac Studio.
  For the Sysmac Studio, synchronization is used to both *upload* and *download* data. Here, *synchronize* means to automatically compare the data for the Sysmac Studio on the computer with the data in the physical Controller and transfer the data in the direction that is specified by the user.

Sections in this Manual

1	Overview of OPC UA Server Function	**A** Appendices
2	Structure of the OPC UA Server	**I** Index
3	Settings of the OPC UA Server	
4	Starting and Checking the Status of the OPC UA Server	
5	Security Function of OPC UA Server	
6	Connecting from the OPC UA Client and Reading/Writing Variables	
7	Execution Log Functions	
8	Other Functions	
9	Troubleshooting	

CONTENTS

Section 1   Overview of OPC UA Server Function

Section 2   Structure of the OPC UA Server

Section 3   Settings of the OPC UA Server

Section 4   Starting and Checking the Status of the OPC UA Server

Section 5   Security Function of OPC UA Server

Section 6   Connecting from the OPC UA Client and Reading/Writing Variables

Section 7   Execution Log Functions

Section 8   Other Functions

Section 9   Troubleshooting

Section A   Appendices

Index

Index

Terms and Conditions Agreement

Warranty, Limitations of Liability

Warranties

- **Exclusive Warranty**

  Omron's exclusive warranty is that the Products will be free from defects in materials and workmanship for a period of twelve months from the date of sale by Omron (or such other period expressed in writing by Omron). Omron disclaims all other warranties, express or implied.

- **Limitations**

  OMRON MAKES NO WARRANTY OR REPRESENTATION, EXPRESS OR IMPLIED, ABOUT NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OF THE PRODUCTS. BUYER ACKNOWLEDGES THAT IT ALONE HAS DETERMINED THAT THE PRODUCTS WILL SUITABLY MEET THE REQUIREMENTS OF THEIR INTENDED USE.

  Omron further disclaims all warranties and responsibility of any type for claims or expenses based on infringement by the Products or otherwise of any intellectual property right.

- **Buyer Remedy**

  Omron's sole obligation hereunder shall be, at Omron's election, to (i) replace (in the form originally shipped with Buyer responsible for labor charges for removal or replacement thereof) the non-complying Product, (ii) repair the non-complying Product, or (iii) repay or credit Buyer an amount equal to the purchase price of the non-complying Product; provided that in no event shall Omron be responsible for warranty, repair, indemnity or any other claims or expenses regarding the Products unless Omron's analysis confirms that the Products were properly handled, stored, installed and maintained and not subject to contamination, abuse, misuse or inappropriate modification. Return of any Products by Buyer must be approved in writing by Omron before shipment. Omron Companies shall not be liable for the suitability or unsuitability or the results from the use of Products in combination with any electrical or electronic components, circuits, system assemblies or any other materials or substances or environments. Any advice, recommendations or information given orally or in writing, are not to be construed as an amendment or addition to the above warranty.

  See http://www.omron.com/global/ or contact your Omron representative for published information.

Limitation on Liability; Etc

OMRON COMPANIES SHALL NOT BE LIABLE FOR SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, LOSS OF PROFITS OR PRODUCTION OR COMMERCIAL LOSS IN ANY WAY CONNECTED WITH THE PRODUCTS, WHETHER SUCH CLAIM IS BASED IN CONTRACT, WARRANTY, NEGLIGENCE OR STRICT LIABILITY.

Further, in no event shall liability of Omron Companies exceed the individual price of the Product on which liability is asserted.

Application Considerations

Suitability of Use

Omron Companies shall not be responsible for conformity with any standards, codes or regulations which apply to the combination of the Product in the Buyer's application or use of the Product. At Buyer's request, Omron will provide applicable third party certification documents identifying ratings and limitations of use which apply to the Product. This information by itself is not sufficient for a complete determination of the suitability of the Product in combination with the end product, machine, system, or other application or use. Buyer shall be solely responsible for determining appropriateness of the particular Product with respect to Buyer's application, product or system. Buyer shall take application responsibility in all cases.

NEVER USE THE PRODUCT FOR AN APPLICATION INVOLVING SERIOUS RISK TO LIFE OR PROPERTY OR IN LARGE QUANTITIES WITHOUT ENSURING THAT THE SYSTEM AS A WHOLE HAS BEEN DESIGNED TO ADDRESS THE RISKS, AND THAT THE OMRON PRODUCT(S) IS PROPERLY RATED AND INSTALLED FOR THE INTENDED USE WITHIN THE OVERALL EQUIPMENT OR SYSTEM.

Programmable Products

Omron Companies shall not be responsible for the user's programming of a programmable Product, or any consequence thereof.

Disclaimers

Performance Data

Data presented in Omron Company websites, catalogs and other materials is provided as a guide for the user in determining suitability and does not constitute a warranty. It may represent the result of Omron's test conditions, and the user must correlate it to actual application requirements. Actual performance is subject to the Omron's Warranty and Limitations of Liability.

Change in Specifications

Product specifications and accessories may be changed at any time based on improvements and other reasons. It is our practice to change part numbers when published ratings or features are changed, or when significant construction changes are made. However, some specifications of the Product may be changed without any notice. When in doubt, special part numbers may be assigned to fix or establish key specifications for your application. Please consult with your Omron's representative at any time to confirm actual specifications of purchased Product.

Errors and Omissions

Information presented by Omron Companies has been checked and is believed to be accurate; however, no responsibility is assumed for clerical, typographical or proofreading errors or omissions.

Safety Precaution

Refer to the following manuals for safety precautions.

- NJ-series CPU Unit Hardware User's Manual (Cat. No. W500)
- NX-series NX102 CPU Unit Hardware User's Manual (Cat. No. W593)
- Sysmac Studio Version 1 Operation Manual (Cat. No. W504)

Precautions for Safe Use

This section describes the precautions for the safe use of the OPC UA Server.

- Even if you accidentally add the client certificate of a client for which you do not want to permit connection in the *Trusted Certificate List*, the OPC UA Server of the NJ/NX-series Controller will permit connections from that client.

  As a result, confidential information on the server side may be leaked or unintended operation may be performed. Therefore, when you add a certificate to the *Trusted Certificate List* from the Sysmac Studio, make sure that all the certificates that you will register in the Trusted Certificate List are trusted client certificates.

- Even if a global variable is set to Network Publish in the Sysmac Studio, the OPC UA client may not be able to refer to or read/write the variable in some cases depending on the limits sets on variables that can be published to the OPC UA client.

  Refer to the event log or Execution Log, and review the variables to be published to the network depending on the cause of occurrence. For details on the restrictions on variables that can be published in the OPC UA client, refer to *Restrictions on Publishing to the OPC UA Client* on page 6-7 in *6-2-2 Reading/Writing the Variables of the CPU Unit* on page 6-5.

Refer to the following manuals for other precautions for safe use that are not described above.

- NJ-series CPU Unit Hardware User's Manual (Cat. No. W500)
- NX-series NX102 CPU Unit Hardware User's Manual (Cat. No. W593)
- Sysmac Studio Version 1 Operation Manual (Cat. No. W504)

Precautions for Correct Use

This section describes the precautions for the correct use of the OPC UA Server.

- If the IP address of the built-in EtherNet/IP port is changed after starting the use of the OPC UA Server, the OPC UA server certificate in the CPU Unit will be disabled, and it will not be possible to communicate with the OPC UA client. In that case, manually regenerate the server certificate, or set the IP address back to the original address.

- The server certificate is not applied for backup and restore because it is information belonging to individual CPU Units. If you replace the CPU Unit hardware, you cannot use the same server certificate for the new CPU Unit after the replacement.

  Even if you set the IP address of the built-in EtherNet IP port to the same value as the one for the previous CPU Unit, be sure to export the server certificate of the new CPU Unit and then perform installation again on the OPC UA clients.

- Even in cases where you recreate the server certificate by changing the IP address in the same CPU Unit, make sure to export the server certificate of the CPU Unit and install it at the OPC UA client side.

- The OPC UA Server is executed as a system service.

  Accordingly, if other system services are executed while the OPC UA Server is starting up, they may take longer.

  Moreover, if the system service execution time ratio is less (if it is below approx. 20%, as a reference), the response to the requests from the OPC UA client will be delayed. In such a case, design the task so that the system service execution time ratio increases.

Refer to the following manuals for other precautions for correct use that are not described above.

- NJ-series CPU Unit Hardware User's Manual (Cat. No. W500)
- NX-series NX102 CPU Unit Hardware User's Manual (Cat. No. W593)
- Sysmac Studio Version 1 Operation Manual (Cat. No. W504)

Regulations and Standards

Refer to the following manuals for regulations and standards.
- NJ-series CPU Unit Hardware User's Manual (Cat. No. W500)
- NX-series NX102 CPU Unit Hardware User's Manual (Cat. No. W593)

Software Licenses and Copyrights

This product incorporates the following third party software. The license and copyright information associated with this software is available at http://www.fa.omron.co.jp/nj_info_e/.

OpenSSL

This product includes software developed by the OpenSSL Project for use

in the OpenSSL Toolkit

(http://www.openssl.org/).

Copyright (C) 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)

LibXML2

This product includes code that was developed for the XML toolkit from

the GNOME project

(http://xmlsoft.org/).

Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.

OPC UA

This product includes code that was developed by Unified Automation GmbH for the OPC UA SDK (http://www.unifiedautomation.com/).

Copyright (C) 2008-2017 Unified Automation GmbH. All Rights Reserved.

The OPC UA SDK is based in part on <OPC UA Ansi C Stack> of the OPC Foundation. Initial version of <OPC UA Ansi C Stack> was founded and copyrighted by OPC Foundation,Inc. Copyright (C) 2008,2014 OPC Foundation, Inc., All Rights Reserved.

Versions

Hardware revisions and unit versions are used to manage the hardware and software in the NJ/NX-series Units and EtherCAT slaves. The hardware revision or unit version is updated each time there is a change in hardware or software specifications. Even when two Units or EtherCAT slaves have the same model number, they will have functional or performance differences if they have different hardware revisions or unit versions.

Checking Versions

You can check versions on the ID information indications or with the Sysmac Studio.

Checking Unit Versions on ID Information Indications

The unit version is given on the ID information indication on the side of the product.

The ID information on an NJ-series NJ501-□□□□ CPU Unit is shown below.
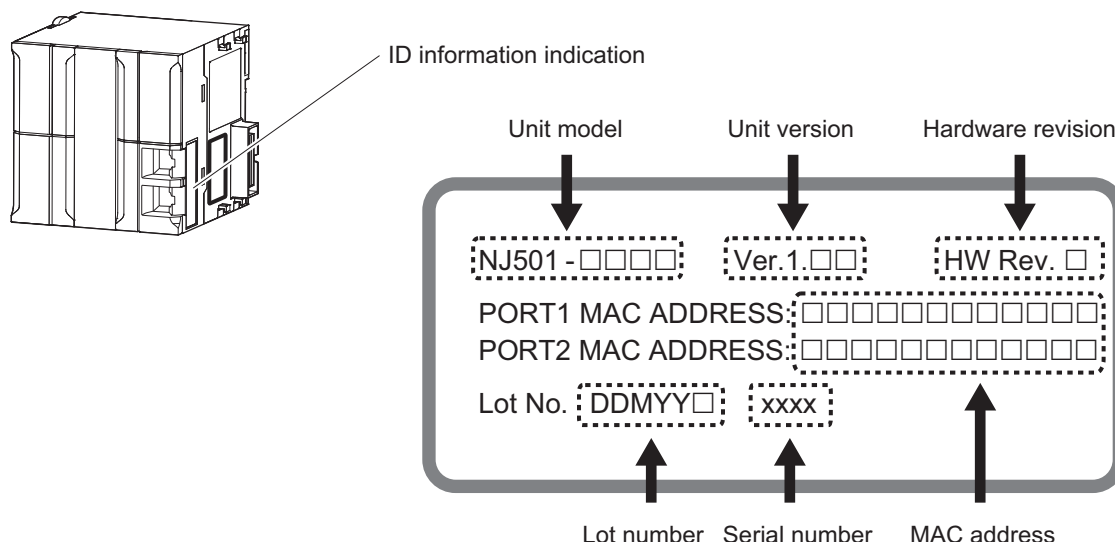
Note The hardware revision is not displayed for the Unit that the hardware revision is in blank.

The ID information on an NX-series NX102-□□□□ CPU Unit is shown below.
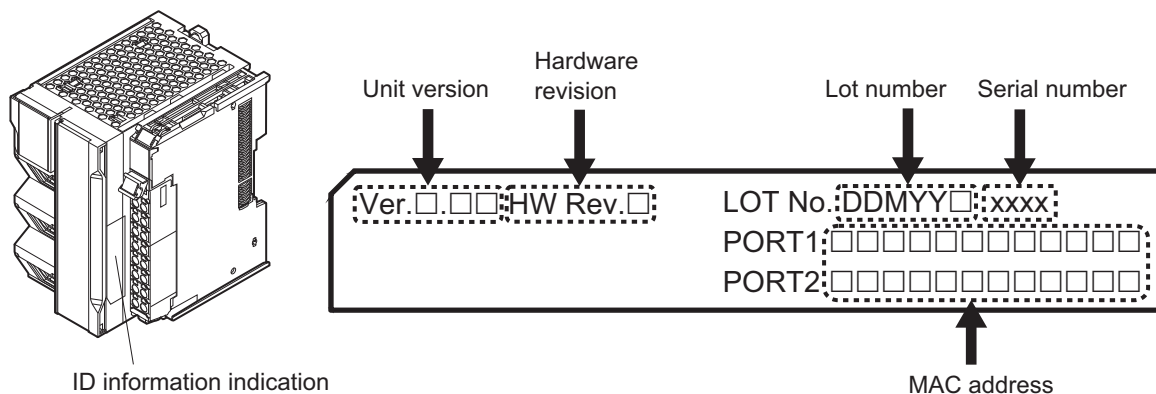
Note The hardware revision is not displayed for the Unit that the hardware revision is in blank.

Checking Unit Versions with the Sysmac Studio

You can use the Sysmac Studio to check unit versions.

● Checking the Unit Version of an NX-series CPU Unit

You can use the Production Information while the Sysmac Studio is online to check the unit version of a Unit. You can do this for the following Units.

Unit model	Available unit to check the unit version
NX102-□□□□	CPU Unit, NX Unit on CPU Rack

1 Right-click **CPU Rack** under **Configurations and Setup** - **CPU/Expansion Racks** in the Multiview Explorer and select **Production Information**.

The Production Information Dialog Box is displayed.

● Checking the Unit Version of an NJ-series CPU Unit

You can use the **Production Information** while the Sysmac Studio is online to check the unit version of a Unit. You can do this for the CPU Unit, the CJ-series Special I/O Units, and the CJ-series CPU Bus Units. You cannot check the unit versions of the CJ-series Basic I/O Units with the Sysmac Studio.

Use the following procedure to check the unit version.

1 Double-click **CPU/Expansion Racks** under **Configurations and Setup** in the Multiview Explorer. Or, right-click **CPU/Expansion Racks** under **Configurations and Setup** and select **Edit** from the menu.

The Unit Editor is displayed.

2 Right-click any open space in the Unit Editor and select **Production Information**.

The **Production Information** Dialog Box is displayed.

● **Changing Information Displayed in Production Information Dialog Box**

1 Click the **Show Detail** or **Show Outline** Button at the lower right of the **Production Information** Dialog Box.

The view will change between the production information details and outline.
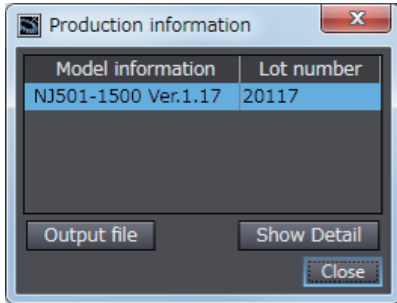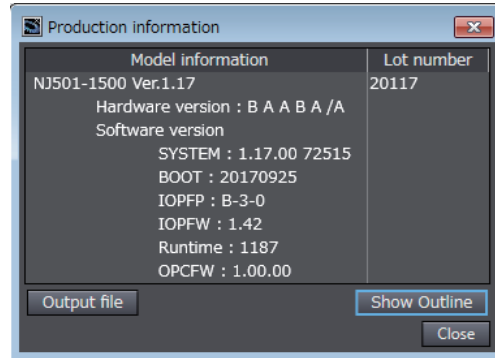
Outline View   Detail View

The information that is displayed is different for the Outline View and Detail View. The Detail View displays the unit version, hardware version, and software versions. The Outline View displays only the unit version.

Note The hardware revision is separated "/" and displayed on the right of the hardware version. The hardware revision is not displayed for the Unit that the hardware revision is in *blank*.

Unit Versions of CPU Units and the Sysmac Studio Versions

The functions that are supported depend on the unit version of the NJ/NX-series CPU Unit. The version of the Sysmac Studio that supports the functions that were added for an upgrade is also required to use those functions.

Refer to *A-5 Version Information* on page A-17 for the relationship between the unit versions of the CPU Units and the Sysmac Studio versions, and for the functions that are supported by each unit version.

Related Manuals

The followings are the manuals related to this manual. Use these manuals for reference.

Manual name	Cat. No.	Model numbers	Application	Description
NJ-series CPU Unit OPC UA User's Manual (This manual)	W588	NJ501-1☐00 NX102-☐☐☐☐	Using the OPC UA with the NJ-series CPU Unit.	Information on the OPC UA is provided.
NJ/NX-series CPU Unit Built-in EtherNet/IP™ Port User's Manual	W506	NX701-☐☐☐☐ NX102-☐☐☐☐ NX1P2-☐☐☐☐ NJ501-☐☐☐☐ NJ301-☐☐☐☐ NJ101-☐☐☐☐	Using the built-in Ether-Net/IP port on an NJ/NX-series CPU Unit.	Information on the built-in EtherNet/IP port is provided. Information is provided on the basic setup, tag data links, and other features.
NJ-series CPU Unit Hardware User's Manual	W500	NJ501-☐☐☐☐ NJ301-☐☐☐☐ NJ101-☐☐☐☐	Learning the basic specifi-cations of the NJ-series CPU Units, including intro-ductory information, design-ing, installation, and maintenance. Mainly hard-ware information is pro-vided.	An introduction to the entire NJ-series system is provided along with the following information on the CPU Unit. • Features and system configuration • Introduction • Part names and functions • General specifications • Installation and wiring • Maintenance and inspection
NX-series NX102 CPU Unit Hardware User's Manual	W593	NX102-☐☐☐☐	Learning the basic specifi-cations of the NX102 CPU Units, including introductory information, designing, installation, and mainte-nance. Mainly hardware informa-tion is provided.	An introduction to the entire NX102 system is pro-vided along with the following information on the CPU Unit. • Features and system configuration • Introduction • Part names and functions • General specifications • Installation and wiring • Maintenance and inspection
NJ/NX-series CPU Unit Software User's Manual	W501	NX701-☐☐☐☐ NX102-☐☐☐☐ NX1P2-☐☐☐☐ NJ501-☐☐☐☐ NJ301-☐☐☐☐ NJ101-☐☐☐☐	Learning how to program and set up an NJ/NX-series CPU Unit. Mainly software information is provided.	The following information is provided on a Control-ler built with an NJ/NX-series CPU Unit. • CPU Unit operation • CPU Unit features • Initial settings • Programming based on IEC 61131-3 language specifications
NJ/NX-series Instruc-tions Reference Manual	W502	NX701-☐☐☐☐ NX102-☐☐☐☐ NX1P2-☐☐☐☐ NJ501-☐☐☐☐ NJ301-☐☐☐☐ NJ101-☐☐☐☐	Learning detailed specifica-tions on the basic instruc-tions of an NJ/NX-series CPU Unit.	The instructions in the instruction set (IEC 61131-3 specifications) are described.
NJ/NX-series Trouble-shooting Manual	W503	NX701-☐☐☐☐ NX102-☐☐☐☐ NX1P2-☐☐☐☐ NJ501-☐☐☐☐ NJ301-☐☐☐☐ NJ101-☐☐☐☐	Learning about the errors that may be detected in an NJ/NX-series Controller.	Concepts on managing errors that may be detected in an NJ/NX-series Controller and infor-mation on individual errors are described.
Sysmac Studio Version 1 Operation Manual	W504	SYSMAC-SE2☐☐☐	Learning about the operat-ing procedures and func-tions of the Sysmac Studio.	Describes the operating procedures of the Sys-mac Studio.

Terminology

This section provides definitions of terms related to the OPC UA.

Term	Description
Address space	A collection of information that visualizes the OPC UA server with respect to the OPC UA client.
	By referencing this information, the OPC UA client can use the objects of the OPC UA server and their related information.
Application authentication	The authentication of each other's identity by the server and the OPC UA client through the exchange of the mutual X.509 digital certificates during the establishment of a connection from the OPC UA client to the server.
Certificate Authority	Organization that issues certificates.
Client authentication	Indicates the direct authentication of client certificates.
	• Authentication of a self-signed client certificate is performed depending on whether it is present in the trusted certificate list.
	• Authentication of a CA-signed client certificate is performed by checking the trust and revocation of the signed CA certificate.
Client certificate	An X.509 digital certificate that certifies the OPC UA client.
	It is generated and managed by the OPC UA client in combination with the private key of the certificate.
	In the NJ/NX-series, it is necessary to register the client certificate in the CPU Unit by the Sysmac Studio.
End point	The physical address that can be used on the OPC UA communications network used by the OPC UA client to access the OPC UA server. Specifically, the following address:
	opc.tcp:// [IPAddress]-[Port]
	In the case of the OPC UA Server, the default address is:
	opc.tcp://192.168.250.1:4840/
Event	A phenomenon that occurs in an unplanned and irregular manner in the NJ/NX-series Controllers.
Event log	A log for recognizing and recording the events that have occurred in the entire Controller. It is recorded in the CPU Unit.
	In the OPC UA Server, it indicates the errors and various states of the OPC UA Server.
Execution log	A log for recording the execution state of the OPC UA Server. It is saved in an SD Memory Card (sold separately).
	As compared to the event log, the execution log has a higher capacity and includes the access results from the OPC UA client to the variables.
	In view of future functional expansion, this Execution Log is considered as one of the types in the leading concept of the *Operation log* in the Sysmac Studio.
Issuer authentication	Indicates the authentication by the certificate authority itself that has signed the client certificate.
	Authentication of a CA-signed client certificate is performed by checking the trust and revocation of the certificate of the certificate authority itself.
Message	The data unit that expresses the requests or responses of the OPC UA server transmitted between the OPC UA client and the server.
Node	The basic component of the address space.
OPC UA	A protocol for communications between industrial devices that is independent of the manufacturer and platform, and is safe with a high reliability. It has an architecture in which the conventional OPC (Object Linking and Embedding for Process Control) has been generalized and widened in scope.
OPC UA client	An application or computer that supports the OPC UA and issues a service request to the OPC UA server. Specifically, the main entity of communications, such as the SCADA and MES.
OPC UA instruction	Indicates instructions related to the OPC UA Server.

Term	Description
OPC UA security mode	Setting the encryption and signature of messages in the security-related settings of messages in the OPC UA.
OPC UA security policy	Specification of algorithms such as signatures and encryption in the security-related settings of messages in the OPC UA.
OPC UA security profile	A common name for the client certificate, CA certificate, certificate revocation list, and security settings.
OPC UA Server	A communications service that provides the function of connecting to the OPC UA client in the NJ/NX-series. It is executed in a *system service* within the processing of the CPU Unit.
OPC UA server	Main entity of communications, such as an application, computer, or controller that supports the OPC UA, executes a service in response to a service request from the OPC UA client, and also sends a response.
Rejected certificate list	A list of client certificates that have been rejected at the server side in application authentication.
Server certificate	An X.509 digital certificate that certifies the OPC UA server. It is generated and managed by the OPC UA server in combination with the private key of the certificate. In the NJ/NX-series, it indicates the self-certificate that certifies an individual CPU Unit as an OPC UA server. It is different for each serial number of the CPU Unit.
Security policy	A common name for the OPC UA security mode and OPC UA security policy.
Security settings	A common name for user authentication settings, anonymous login, and security policy.
Trusted certificate list	A list of certificates of the communications partner that must be trusted in application authentication. There are the following two types of trusted certificate lists at the server side and the OPC UA client side: • Trusted certificate list at the server side: A list of client certificates that have been set to trust the OPC UA client. • Trusted certificate list at the OPC UA client side: A list of server certificates that have been set to trust the server.
User authentication	The authentication of the identity of the user operating the OPC UA client by the server during the establishment of a connection from the OPC UA client to the server.

Revision History

A manual revision code appears as a suffix to the catalog number on the front and back covers of the manual.

Cat. No. | W588-E1-03

Revision code

Revision code	Date	Revised content
01	January 2018	Original production
02	April 2018	Added information on the NX102-□□□□ NX-series CPU Units.
03	July 2019	Corrected mistakes.

1

Overview of OPC UA Server Function

This section describes an overview of the OPC UA Server function.

1-1 Overview and Features

This section describes an overview and features of the OPC UA Server function.

1-1-1 Overview

The OPC UA Server function enables the NJ/NX-series CPU Unit to operate as an *OPC UA server*. With this function, OPC UA clients can connect via Ethernet to the built-in EtherNet/IP port of the NJ/NX-series CPU Unit using the OPC UA communications, and then read and write variables in the CPU Unit.

The OPC UA communications can simultaneously achieve both addressing security risks and connecting with general-purpose methods. Therefore, the OPC UA Server function enables secure data exchanges between the CPU Unit and host systems such as SCADA or MES compatible OPC UA so that the host systems can collect manufacturing progress information or issue manufacturing instructions.

1-1-2 System Configuration

The OPC UA Server function supports the following system configuration.

Sysmac Studio

NJ/NX-series CPU Unit   Ethernet network   OPC UA communications

OPC UA Server function

Securely connects and reads and writes variables.

OPC UA Client
- SCADA software
- MES etc.

Built-in EtherNet/IP port
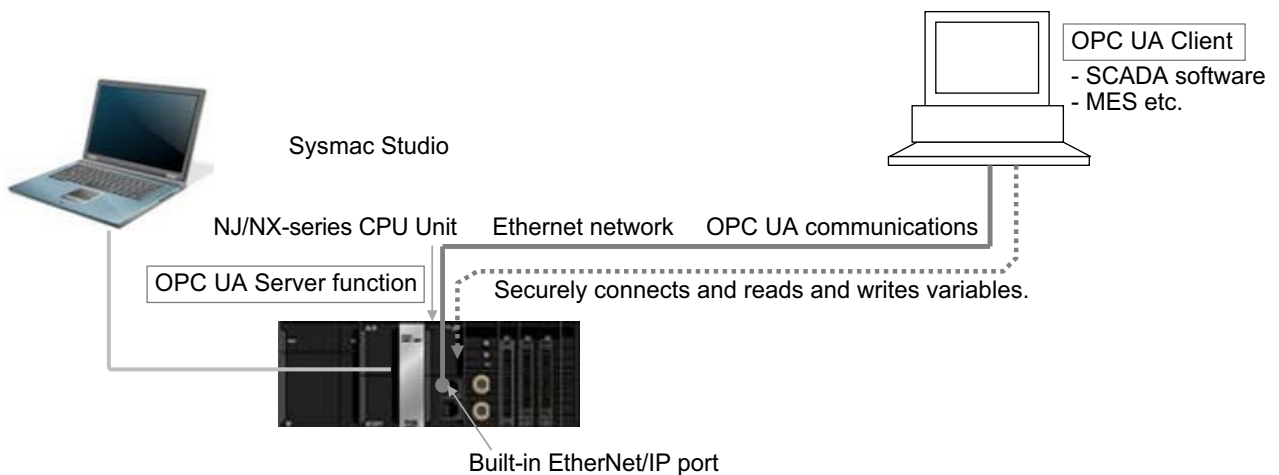
Refer to *A-5 Version Information* on page A-17 for the Unit version of the CPU Unit and the version of the Sysmac Studio that can be supported.

1-1-3 Features

The OPC UA Server function has the following features.

Supporting OPC UA Communications as Secure Industrial Standard Communications

OPC UA communications have the following features.

- A versatile global standard network from discrete control to process control, and from the sensor or controller level to the host monitoring and management level.
- Also defined as a recommended communications standard of Industrie 4.0 to connect the control networks in factories to the IT networks.

- Allows full-scale secure information exchange in the industrial system consisting of different devices.
- Allows to expand the visualization of information adapting to the system in the object-based Address Space.

Providing the Server Function of OPC UA Communications in the NJ/NX-series Controller

The NJ/NX-series OPC UA Server function has the following features.

- It allows the Controller to connect directly to the OPC UA client via Ethernet without relaying the computer.
- Since the NJ/NX-series CPU Unit has EtherCAT communications as the lower level network, it makes it easy to gather sensor and actuator level information on EtherCAT into OPC UA communications as a higher network.
- You can check the operation results of the OPC UA Server function from the event log in the Controller and the Execution Log.

1-2 Specifications

This section describes the specifications of the OPC UA Server function.

1-2-1 List of Supported CPU Units

The OPC UA Server is supported by the following CPU Unit models.

CPU Unit Models	Unit version
NJ501-1300	1.17 or later
NJ501-1400	
NJ501-1500	
NX102-9000	1.30 or later
NX102-1000	
NX102-1100	
NX102-1200	

1-2-2　Function Specifications

Specifications of the OPC UA Server

Item		NJ501-1□00	NX102-□□□□
Connection ports		Built-in EtherNet/IP port on the CPU Unit	Built-in EtherNet/IP port (PORT 1) on the CPU Unit
		Note:　The OPC UA Server can be used simultaneously with EtherNet/IP communications.	
OPC UA function		Server function	
Transport and data encoding		UA TCP binary	
Supported profile and model		• UA 1.02 Micro Embedded Device Server Profile • PLCOpen Information Model	
Endpoint URL (Server URL)		opc.tcp: // [IP address] : [port number] / By default, below. opc.tcp: //192.168.250.1: 4840 /	
Maximum number of sessions (client)		5	
Maximum number of monitored items per server		2,000	
Maximum number of subscriptions per server		100	
Variable type		Network variable	
Conditions as a whole network-published variables [1]	**Maximum number of variables that can be published**	10,000	
	Maximum number of value attributes that can be published	10,000	
	Maximum number of structure definitions that can be published	100	
Conditions that can not be published for each network-published variable [1]		• Multidimensional array specified structure • Structure containing multidimensional array(s) as member(s) • Structure whose nesting number exceeds three • Union, and structure containing union(s) as member(s) • Array whose start number is not 0; e.g., Array[2..5] • Array whose number of elements exceeds 1024 • Structure whose number of members exceeds 100 • Variable whose size exceeds 1024 bytes	
OPC UA security mode and policy		Allowable security methods can be specified from the following (multiple specifications possible): • Both signature and encryption required: SignAndEncrypt Signature and encryption algorithm: Basic256-Sha256/Basic256/Basic128Rsa15 (multiple specifications possible) • Only signature required: Sign Signature algorithm: Basic256Sha256/Basic256/Basic128Rsa15 (multiple specifications possible) • Neither signature nor encryption required	
Application authentication	**Authentication**	X.509	
	Number of certificates that can be stored	• Trusted certificate: 32 • CA certificate: 32 • Rejected certificate: 32	
User authentication	**Method of user authentication**	The following can be set: • User name and Password • Anonymous	

*1. For details, refer to *Restrictions on Publishing to the OPC UA Client* on page 6-7.

Precautions for Correct Use

For the NX102 CPU Unit, there are two built-in EtherNet/IP ports, PORT 1 and PORT 2. Note that only PORT 1 is the port that supports the OPC UA Server.

1-3   OPC UA Server Procedures

This section describes the OPC UA Server Procedures.

1-3-1   Overall Procedure

The overall procedure for using the OPC UA Server is as follows. For details, refer to *1-3-2 Procedure Details* on page 1-8.

Step		Description	Reference
STEP*1.* Settings	**1-1.** IP address setting of the built-in EtherNet/IP port		*Section 3 Settings of the OPC UA Server*
	1-2. OPC UA Settings (offline)	• Offline: Whether OPC UA server is used or not	
	1-3. Settings for publishing variables to the OPC UA client	• Public settings of global variables	
	1-4. Downloading (synchronization)		
	(When using for the first time)		
	1-5. Cycling the power supply to the Controller or resetting the Controller		
	1-6. Confirm the start of OPC UA Server (online)		
	1-7. OPC UA Settings (online)	• Online: server certificate, client certificates, security settings	
STEP*2.* Operation	**2-1.** Connectiing from an OPC UA client		*Section 6 Connecting from the OPC UA Client and Reading/Writing Variables*
	2-2. Checking communications from the OPC UA client	• Referencing the server address space from the OPC UA client	
	2-3. Reading and writing variables from the OPC UA client	• Designing the variable designation	
STEP*3.* Shut-down	**3-1.** Stopping the Controller	• Disconnecting from the client. • Shutting down the OPC UA Server. • Turning OFF the power supply to the Controller.	*4-2-1 Checking Based on OPC UA Server Status of the Sysmac Studio* on page 4-5
STEP*4.* Trouble shooting	**4-1.** Client error check		
	4-2. Status Monitor	• Checking the operating status of the OPC UA server function, etc.	*4-2-1 Checking Based on OPC UA Server Status of the Sysmac Studio* on page 4-5
	4-3. Checking the event log	• Checking the status log	*Section 9 Troubleshooting*

1-3-2　Procedure Details

The procedure for using the OPC UA Server is shown separately for the OPC UA Server side and the OPC UA client side as follows.

Step	OPC UA Server	OPC UA client[*1]	Reference
STEP1. **Settings**			
1-1. IP address setting of the built-in Ether-Net/IP port	Set the IP address of the built-in EtherNet/IP port in **Configurations and Setup** - **Controller Setup** - **Built-in EtherNet/IP Port Settings** in the Multiview Explorer in the Sysmac Studio.		*3-1-1 IP Address Settings of the Built-in EtherNet/IP Port* on page 3-2
1-2. OPC UA Settings (offline)	Make the settings from **Configurations and Setup** - **OPC UA Server Settings**. (Select OPC UA Server to Use and set the port number)	• Create client certificates • Other settings of OPC UA client side	*3-2-2 OPC UA Server Settings* on page 3-5
1-3. Settings for publishing variables to the OPC UA client	In the the Global Variable Editor of the Sysmac Studio, register the global variables for OPC UA communications with *Network Publish Attribute* set to *Publish Only*, *Input*, or *Output*.		*3-3 Creating Variables for OPC UA Communications* on page 3-25
1-4. Downloading (synchronization)	Download the OPC UA Settings and global variables from the Sysmac Studio to the CPU Unit (using synchronize function)		*Sysmac Studio Version1 Operation Manual* (Cat. No.W504)
Conditional branching by OPC UA Server Use Option	In step 1-2, the OPC UA server was changed from *Do not use* (default) to *Use*.　*No* (Keep *Use*)　*Yes* (Used for the first time, etc.)		*3-2-2 OPC UA Server Settings* on page 3-5
(When using for the first time) **1-5.** Cycling the power supply to the Controller or resetting the Controller	Cycling the power supply to the Controller or select **Reset Controller** from the **Controller** Menu in the Sysmac Studio. Note: If you change the OPC UA server from *Do not use* to *Use* in step 1-2, the OPC UA Server will not be started unless this operation is performed.		*3-2-3 When necessary to cycle the power supply to the Controller or reset the Controller* on page 3-8 *4-1 Starting or Stopping the OPC UA Server* on page 4-2

Step		OPC UA Server	OPC UA client[1]	Reference
STEP1. Settings	**1-6.** Confirming the start of OPC UA Server (online)	Confirm that the OPC UA Server is started. In the Sysmac Studio, connect online to the CPU Unit, and then right-click **OPC UA Server Settings** and select **Server Status**.		*4-2-1 Checking Based on OPC UA Server Status of the Sysmac Studio* on page 4-5
	1-7. OPC UA Settings (online)	Use the following procedure from **Configurations and Setup** – **OPC UA Server Settings** in the Sysmac Studio.		*Section 5 Security Function of OPC UA Server*
		Server certificate operations: Right-click **OPC UA Server Settings** and select **Server Certificate**. Click the **Regenerate certificate** Button to set the details of the server certificate and perform the regenerate operation of the server certificate[2][3].		*Regenerating the Server Certificate* on page 3-11
		Export the server certificate.	Import the server certificate on the OPC UA client side	*Exporting Server Certificate* on page 3-11
		Client certificates operations: Right-click **OPC UA Server Settings** and select **Client Authentication**. • Operations such as adding the client certificates created on the client sides in step 1-2.		*Client Authentication* on page 3-13
		Security Settings operations: Right-click **OPC UA Server Settings** and select **Security Settings**. • User Authentication Settings • Anonymous login • Security Policy		*3-2-6 Security Settings* on page 3-20
		Note:In order to support the CA-signed client certificates, the CA certificate and certificate revocation list must be registered.		*A-3 When CA-signed Client Certificates Supported* on page A-11

Step	OPC UA Server	OPC UA client[1]	Reference
STEP2. **Operation** — **2-1.** Connecting from an OPC UA client		Connection to the OPC UA Server. Enter *opc.tcp: // [IP address] : [port number] /* as the URL. Note:By default on the NJ side, *opc.tcp: //192.168.250.1: 4840 /* Enter the IP address set in step 1-1 and the port number set in step 1-2 here. • Specify the OPC UA security mode and policy. • Enter user name and password (when user authentication is required) .	*6-1 Connecting from the OPC UA Client* on page 6-2
2-2. Checking communications from the OPC UA Client		• Refer the server address space from the OPC UA client • Design the variable designation	*6-2 Reading/Writing Variables from the OPC UA Client* on page 6-3
2-3. Reading and writing variables from the OPC UA client	Read/write variables in the CPU Unit from the OPC UA client via the OPC UA Server. Confirm variables in the CPU Unit with a monitor such as a Watch Tab Page on the Sysmac Studio.		*6-2-2 Reading/Writing the Variables of the CPU Unit* on page 6-5 *Sysmac Studio Version1 Operation Manual* (Cat. No.W504)
STEP3. **Shut-down** — **3-1.** Stopping the Controller	Shut down the OPC UA Server.	Disconnection	*4-1-1 How to Start or Stop the OPC UA Server* on page 4-2 *4-2-1 Checking Based on OPC UA Server Status of the Sysmac Studio* on page 4-5
	Turn OFF the power supply to the Controller.		

Step	OPC UA Server	OPC UA client[1]	Reference
STEP4. **Trouble shooting** / **4-1.** Client error check		Confirm the error on the OPC UA client side • Check network settings • Confirm the URL • Confirm the security policy • Confirm the server certificate, etc.	
4-2. Status Monitor	Monitor status such as the operating status of the OPC UA Server and the number of connected clients in the Server Status Tab Page of the Sysmac Studio.		*4-2-1 Checking Based on OPC UA Server Status of the Sysmac Studio* on page 4-5
4-3. Confirming the event log	Check errors saved as Controller Events using troubleshooting functions of the Sysmac Studio.		*Section 9 Troubleshooting*

*1. For operation of the OPC UA client, refer to the manual of each OPC UA client.

*2. The server certificate is generated with the IP address that is set.
After that, when you change the IP address by setting operation or instruction execution, be sure to regenerate the server certificate. If the server certificate is not regenerated, the IP address of the built-in EtherNet/IP port will not match the IP address of the server certificate. In that case, note that the OPC UA client can not connect to the OPC UA Server.

*3. If the OPC UA Server remains *Use* before and after the downloading (synchronization function) in step 1-4, this operation of regenerating the server certificate is not necessary.

2

Structure of the OPC UA Server

This section describes the structure of the OPC UA Server.

2-1   Internal Structure of the Overall OPC UA Communications System

This section describes the internal structure of the overall OPC UA communications system with the NJ/NX-series CPU Units as an OPC UA server.

2-1-1   Overview

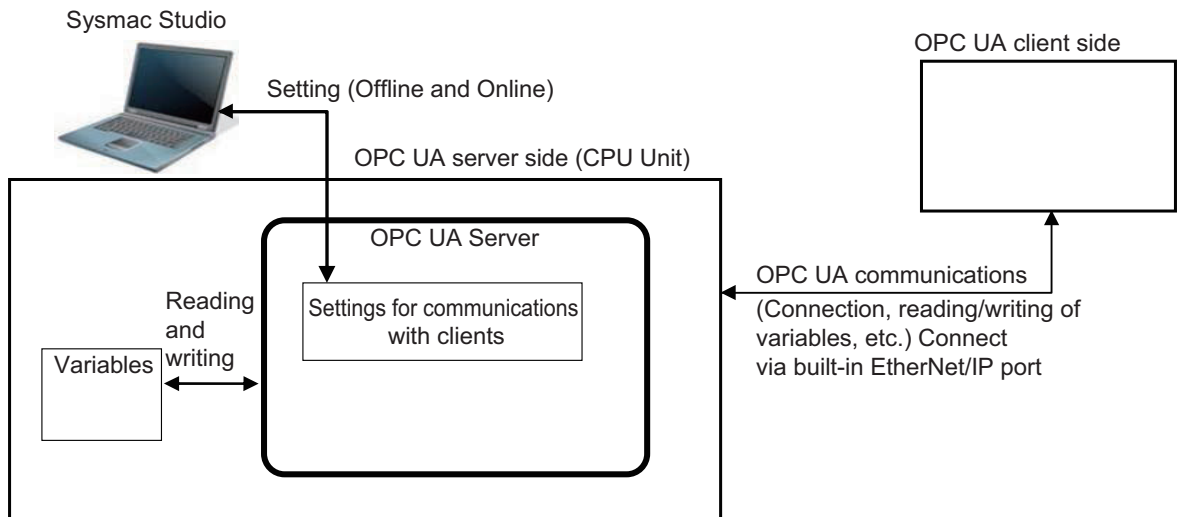An overview of the overall OPC UA communications system is provided below.

The description is given separately for the NJ/NX-series CPU Unit side as a server and the OPC UA client side.

OPC UA Server Side (CPU Unit Side)

- Set in advance the parameters for communications with the OPC UA client to the CPU Unit from the Sysmac Studio. There are settings that can be done offline and ones that are only available online.
- Start a communications service that is called *OPC UA Server* and execute the OPC UA communications.

OPC UA Client Side

- Connect from the OPC UA client to the CPU Unit as a server.
- Read and write variables in the CPU Unit as a server from the OPC UA client.

2-1-2   Details

The details of the structure of the overall OPC UA communications system is described by using the following figure.
Note that the (Figure a) to (Figure e) in the table shown below correspond to the (a) to (e) in the following figure.
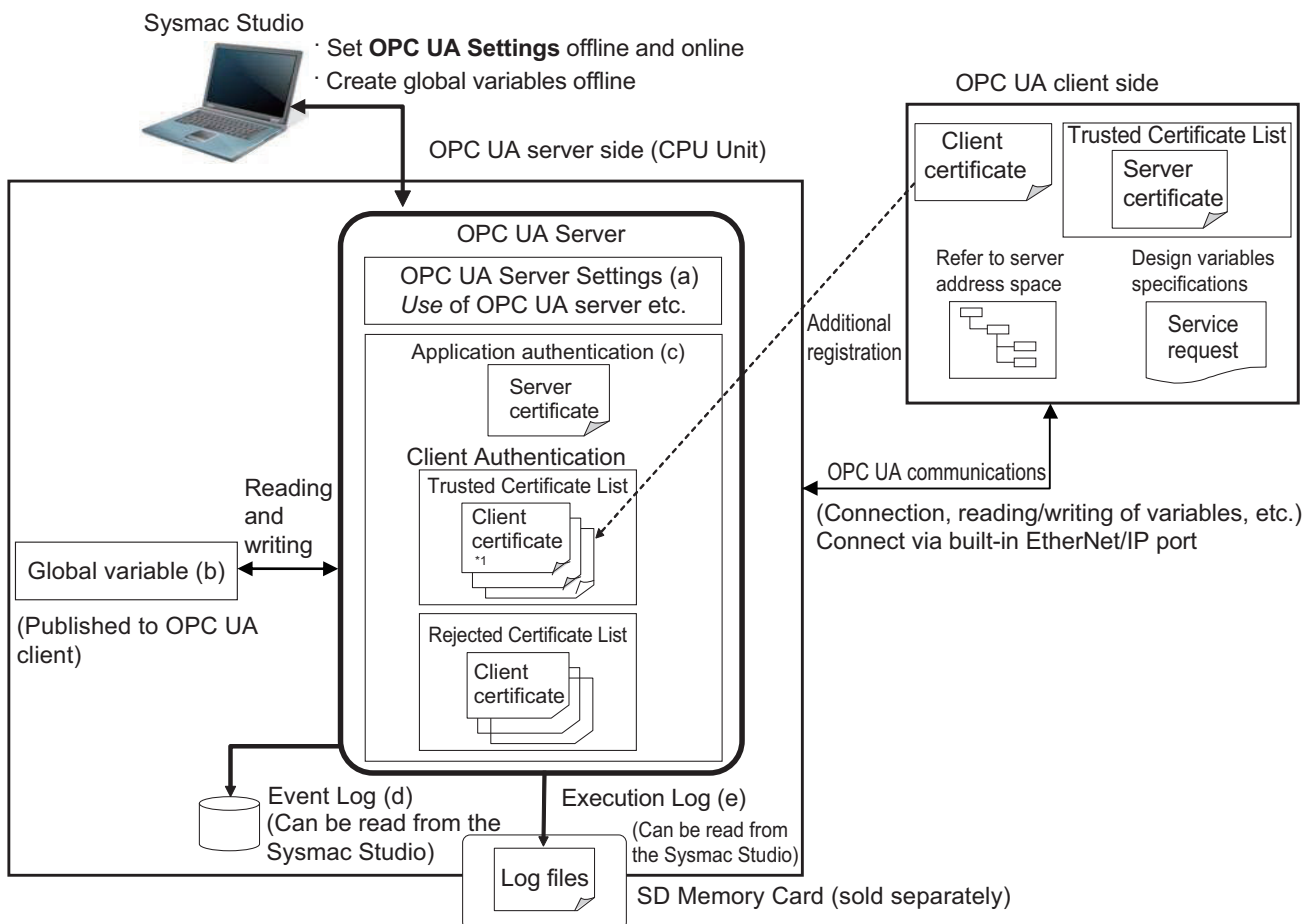
Note 1.   The above figure shows the case of a self-signed client certificate. You can also support a CA-signed client certificate. To use the CA-signed client certificate, refer to *A-3 When CA-signed Client Certificates Supported* on page A-11.

Basic Mechanism

The basic mechanism from the start for using the OPC UA Server to reading and writing variables is as follows. The basic mechanism is shown in accordance with the usage procedure.

Basic mechanism (the number indicates the order of procedure)	Reference
1. In the Sysmac Studio, set **OPC UA Server Settings** from **Configurations and Setup** - **OPC UA Settings** in Multiview Explorer by an offline operation. (Figure a).	*3-1 Controller Setup* on page 3-2 *3-2-2 OPC UA Server Settings* on page 3-5
2. Create global variables to be published for OPC UA communications (with the *network publish attribute* set to *Public Only*, *Input*, or *Output*) (Figure b).	*3-3 Creating Variables for OPC UA Communications* on page 3-25
3. Transfer OPC UA server settings and global variables to the CPU Unit using synchronization function from the Sysmac Studio.	*Sysmac Studio Version1 Operation Manual* (Cat. No.W504)

Basic mechanism (the number indicates the order of procedure)	Reference
4. In the Sysmac Studio, connect online to the CPU Unit, and perform operations of the application authentications and security settings (Figure c).	*Sysmac Studio Version1 Operation Manual* (Cat. No.W504) *3-2-5 Setting and Displaying the Certificate* on page 3-9 *3-2-6 Security Settings* on page 3-20
5. Turn ON the power supply to the Controller and start using the OPC UA Server. Note: The OPC UA server in **OPC UA Server Settings** must be set to *Use*.	*4-1 Starting or Stopping the OPC UA Server* on page 4-2
6. Connect from the OPC UA client to the OPC UA Server. • Connect to the server by specifying *opc.tcp: // [IP address] : [port No.] /* as the URL. • Enter the User name and Password from the OPC UA client.	*6-1 Connecting from the OPC UA Client* on page 6-2
7. Reading and writing from the OPC UA client • From the OPC UA client, refer to the address space of the OPC UA Server and design variables specifications. • Request service from the OPC UA client, read and write global variables of the CPU Unit published to OPC UA communications.	*6-2 Reading/Writing Variables from the OPC UA Client* on page 6-3

Status Confirmation

The following table shows how to confirm the status of the OPC UA Server.

Means of confirmation	Status confirmation mechanism	Reference
OPC UA server status	The server operating status and the number of currently connected OPC UA clients can be checked with the OPC UA server status in the Sysmac Studio.	*4-2 Checking the Status of the OPC UA Server* on page 4-5
Event Log	Failure of OPC UA Server and status are stored as event logs (Figure d) of the NJ/NX-series Controllers. You can confirm with troubleshooting functions of the Sysmac Studio.	*Section 9 Troubleshooting*
Execution Log	Logs (Figure e) for recording the execution status of the OPC UA Server, variable published-status, authentication processing, and operation of certificates are saved as a log file in the SD Memory Card (sold separately) in the CPU Unit. You can confirm in Operation Logs Display on the Sysmac Studio.	*Section 7 Execution Log Functions*

2-2 Overview of the Security Function of the OPC UA Server

This section describes the overview of the security function of the OPC UA Server.

The OPC UA Server of the NJ/NX-series CPU Unit supports the server function of the OPC UA. There are the following two security functions as a server in the OPC UA Server.

Function	Description
Connection authentication function of the OPC UA Server	When a connection request is accepted from an OPC UA client and its users, the OPC UA Server permits connections from only authenticated OPC UA clients and users.
Message security function	Upon receiving requests from OPC UA clients and sending responses to OPC UA clients, the OPC UA Server signs and encrypts the messages.

Set the following contents, in advance, to use the security functions as a server.

Function	Setting		Reference
Connection authentication function of the OPC UA Server	Certificate settings	• Regeneration of the server certificate (only when necessary)	*3-2-5 Setting and Displaying the Certificate* on page 3-9
		• Self-signed client certificates: Additional registration of client certificates, and trust or reject settings of each client certificate at client authentication	
		• CA-signed client certificates: Additional registration of CA certificates and certificate revocation list at client authentication and issuer authentication	*A-3 When CA-signed Client Certificates Supported* on page A-11
	User Authentication Settings	• User name and Password to authenticate • Prohibition or permission for anonymous login	*3-2-6 Security Settings* on page 3-20
Message security function	OPC UA security mode and policy that are allowed for the OPC UA client as a server		*3-2-6 Security Settings* on page 3-20

For details on the security functions, refer to *Section 5 Security Function of OPC UA Server*.

3

Settings of the OPC UA Server

This section describes the settings required to use the OPC UA Server.

3-1   Controller Setup

This section describes the following Controller Setup related to the OPC UA function.
- Setting the IP address of the built-in EtherNet/IP port
- Setting the Start delay time at startup when you want to shorten the startup time of the OPC UA Server

For general settings of the built-in EtherNet/IP port, refer to the *NJ/NX-series CPU Unit Built-in Ether-Net/IP Port User's Manual* (Cat. No. W506).

For details on the operation, refer to the *Sysmac Studio Version 1 Operation Manual* (Cat. No. W504).

3-1-1   IP Address Settings of the Built-in EtherNet/IP Port

Select one of the following settings in the **IP address** of **TCP/IP Settings** in **Configurations and Setup** - **Controller Setup** - **Built-in EtherNet/IP Port Settings** in the Multiview Explorer in the Sysmac Studio:

Fixed Setting, or **Fix at the IP address obtained from BOOTP server**

For details on the settings, refer to the *NJ/NX-series CPU Unit Built-in EtherNet/IP Port User's Manual* (Cat. No. W506)

The server certificate is automatically or manually generated with the IP address that is set in the Controller Setup. For information on automatic generation of server certificates, refer to *3-2-4 Automatic Generation of the Server Certificate* on page 3-8. For information on the manual regeneration of server certificates, refer to the *Regenerating the Server Certificate* in *3-2-5 Setting and Displaying the Certificate* on page 3-9.

> **Precautions for Correct Use**
>
> If you change the IP address by downloading the settings or executing the instruction after the server certificate is generated automatically or manually, the IP address of the built-in Ether-Net/IP port will not match that of the Server certificate. As a result, the OPC UA client can not connect to the OPC UA Server. Then, a *Server Certificate Mismatch* event (event code: 15020000 hex) occurs. In that case, manually regenerate the server certificate or set the IP address back to the original address.
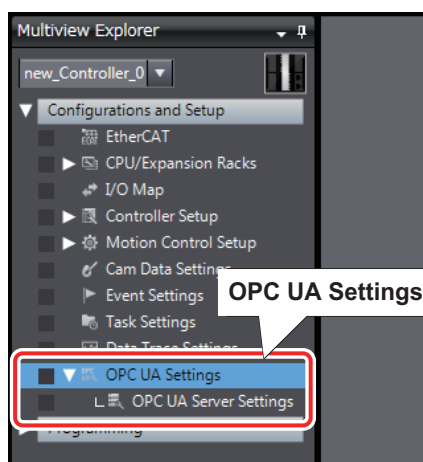
3-2   OPC UA Settings

You must set the OPC UA Settings before the OPC UA Server runs.

This section describes how to set the OPC UA Settings.

3-2-1   Overview of OPC UA Settings

The following is an overview of the OPC UA Settings.

The OPC UA Settings are located in **Configurations and Setup** in Multiview Explorer in the Sysmac Studio as follows.

There are three types of **OPC UA Settings**; items to set offline, items to set or operate online, and items to display or operate online. The details are as follows.

Items of OPC UA Settings	Contents	Offline or online	Procedure	Reference
OPC UA Server Settings	Set the following items in the OPC UA Server Settings Tab Page. • Use of the OPC UA Server: Set whether to use. • End Point Settings: Display the End point and set the port number. • Execution Log Settings: Set whether to record, set the number of log files, and set the number of records.	Settings offline	Double-click **OPC UA Server Settings** or right-click it and select **Edit** from menu	*3-2-2 OPC UA Server Settings* on page 3-5

Items of OPC UA Settings	Contents	Offline or online	Procedure	Reference
Server Certificate	Display and operate the server certificate in the Server Certificate Tab Page.	Setting or operation online	Right-click **OPC UA Server Settings** and select from the menu.	*3-2-3 When necessary to cycle the power supply to the Controller or reset the Controller* on page 3-8
Client Authentication	• For a self-signed client certificate: Display and operate the Trusted Certificate List and the Client Rejected Certificate List in the Client Authentication Tab Page.			
	• For a CA-signed client certificate: Display and operate the Trusted Certificate List of the CA certificate that is signed and the Certificate Revocation List in the Client Authentication Tab Page.			*Client Authentication* on page A-12
Issuer authentication	• For a CA-signed client certificate only: Display and operate the Trust List of the CA's own Certificate and the Certificate Revocation List in the Issuer Authentication Tab Page.			*Issuer Authentication* on page A-14
Security Settings	The following settings are made in the Security Setting Tab Page. • User name and Password to authenticate • Prohibition or permission for anonymous login • Security mode policy			*3-2-6 Security Settings* on page 3-20
Server Status	Display the operating status of the OPC UA Server and shutdown the OPC UA Server in the Server Status Tab Page.	Display or operation online	Right-click **OPC UA Server Settings** and select from the menu.	*4-2-1 Checking Based on OPC UA Server Status of the Sysmac Studio* on page 4-5
Operation Log Display	List and operate the Execution Logs in the Show Operation Log Tab Page.		Right-click **OPC UA Settings** and select from the menu.	*7-2 Checking the Execution Log* on page 7-13

> **Precautions for Correct Use**

OPC UA Server Settings such as whether or not the OPC UA Server is used are set offline and transferred to the CPU Unit.

On the contrary, *Certificate Settings* and *Security Settings* are set online by connecting to the CPU Unit.

In an online operation, there are restrictions on the operation authority from the Sysmac Studio depending on the function. For details on the operation authority of the OPC UA Server in the Sysmac Studio, refer to *8-1 The Sysmac Studio Operation Authority Verification Related to the OPC UA Server* on page 8-2.

3-2-2   OPC UA Server Settings

The following shows how to make the *OPC UA Server Settings* and its contents.

The OPC UA Server Settings consist of the following.
- OPC UA Server Use Option setting
- End point Settings
- Execution Log Settings

1 Double-click **OPC UA Server Settings** under **Configurations and Setup** - **OPC UA Settings** in Multiview Explore in the Sysmac Studio. Alternatively, right-click **OPC UA Server Settings** and select **Edit** from the menu.
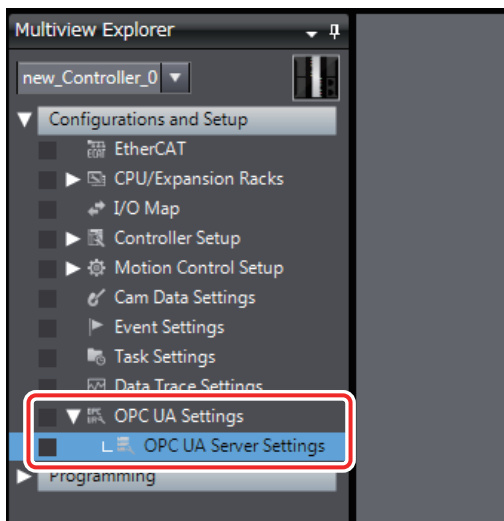
The following **OPC UA Server Settings** Tab Page is displayed.
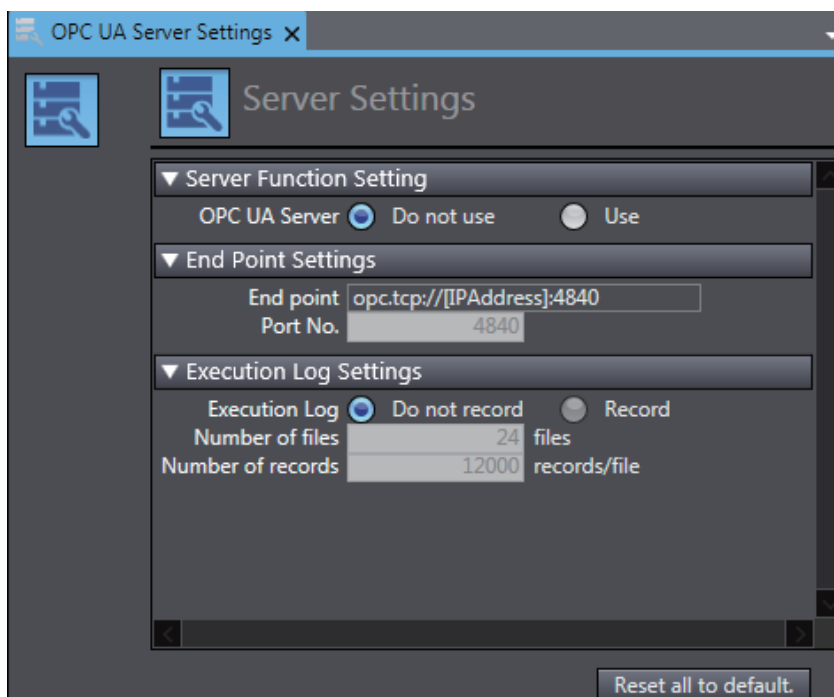
Use of the OPC UA Server

You can set whether to use the OPC UA Server in **Server Function Setting**,

Set the following items.

Parameter	Setting group	Description	Set value	Default	Update Timing	Changes in RUN mode
Server Settings	Server Function Setting	Set whether to use the OPC UA Server	• Do not use • Use	Do not use	When downloaded to CPU Unit	Not allowed

After you download the project whose **OPC UA Server** in the OPC UA Settings was changed from *Do not use* to *Use* to the CPU Unit, and then cycle the power supply to the Controller or reset the Controller, the OPC UA Server will start automatically at that time.

For details on how to start the OPC UA, refer to *4-1 Starting or Stopping the OPC UA Server* on page 4-2.

End Point Settings

In the **End Point Settings**, display the end point and set the port number.

Set and display the following items.

Parameter	Setting group	Description	Set value or display value	Default	Update Timing	Changes in RUN mode
End Point Settings	End point	The End point notation of the OPC UA Server is displayed. • The [IPAddress] section on the right column shows the IP address of the built-in EtherNet/IP port in the NJ/NX-series CPU Unit. • The [Port] section on the right column automatically shows the value of the set **Port No.** shown below.	opc.tcp: // [IPAddress] : [Port] Note. Not allowed to set. Display only.	opc.tcp://192. 168.250.1:48 40	---	---
	Port No.	Set the port number to be used for the OPC UA Server[*1].	1025 to 65535	4840	When downloaded to CPU Unit	Not allowed.

*1. It can be set only when OPC UA server is set to *Use*.

✓ Precautions for Correct Use

- The IP Address Displayed at the End point

  The IP address that is displayed at the **End point** is the IP address of the built-in EtherNet/IP port.

  For details on how to set the IP address from the Sysmac Studio, refer to the *NJ/NX-series CPU Unit Built-in EtherNet/IP Port User's Manual* (Cat. No. W506).

  The IP address of the built-in EtherNet/IP port can also be changed with the *ChangeIPAdr* (Change IP Address) instruction.

  However, if you change the IP address by downloading the settings or executing the instruction after server certificate is generated automatically or manually, the IP address of the built-in EtherNet/IP port will not match that of the server certificate. As a result, the OPC UA client can not connect to the OPC UA Server. Then, a *Server Certificate Mismatch* event (event code: 15020000 hex) occurs. In that case, manually regenerate the server certificate or set the IP address back to the original address.

- Duplication of Used Port Number with Other Communications Services

  Make sure that the port number set in **End point** - **Port No.** does not use the same port number used for other communications service (such as FTP server, HTTP server, CIP message, FINS/TCP, and system). For the port number used for the built-in EtherNet/IP port, refer to the *NJ/NX-series CPU Unit Built-in EtherNet/IP Port User's Manual* (Cat. No. W506).

Execution Log Settings

Specify whether or not to record Execution Logs, and set each specification related to the logs in the **Execution Log Settings**.

Set the following items.

Parameter	Setting group	Description	Set value	Default
Execution Log Settings	Execution Log	Sets whether to record Execution Logs.	Do not record Record	Do not record
	Number of files	Sets the maximum number of files of the Execution Logs. When the maximum number of files is reached, the oldest file is deleted and a new file is created[1].	2 to 100	24
	Number of records	Sets the number of log records that can be contained in each Execution Log file[1].	100 to 65,536	12,000
	Reset all to default Button	Returns all parameters to the default settings.	---	---

*1. It can be set only when OPC UA server is set to *Use* and *Execution Log* is set to *Record*.

For details on the Execution Log, refer to *Section 7 Execution Log Functions*.

3-2-3   When necessary to cycle the power supply to the Controller or reset the Controller

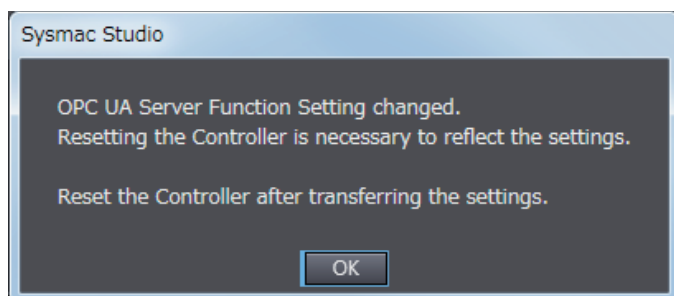You need to cycle the power supply to the Controller or reset the Controller in the following cases:

- Changing OPC UA Server Use Option [*1] under **OPC UA Settings** before downloading or restoring the setting to the CPU Unit, and to enable the changes

*1. That means either case of *Do not use* to *Use* or *Use* to *Do not use.*

- When the Clear All Memory is executed with **Use** that is set in OPC UA Server Use Option

When data is downloaded or restored after OPC UA Server Use Option is changed

If the OPC UA Server Use Option is changed, the following dialog box is displayed after the data is downloaded or restored.

```
Sysmac Studio

OPC UA Server Function Setting changed.
Resetting the Controller is necessary to reflect the settings.

Reset the Controller after transferring the settings.

                 [ OK ]
```

1   Click the **OK** Button.

2   Then, cycle the power supply to the Controller or reset the Controller.

After the execution of Clear All Memory while the OPC UA Server Use Option set to Use

When Clear All Memory is executed with the OPC UA Server Use Option set to *Use*, a similar dialog box is displayed. For details on how to perform Clear All Memory operation, refer to *8-3 Clear All Memory Function Related to the OPC UA Server* on page 8-9.

3-2-4   Automatic Generation of the Server Certificate

The server certificate is automatically generated in the following case:

- When you cycle the power supply to the Controller or reset the Controller after downloading the project whose **OPC UA Server** in the OPC UA Settings was changed from *Do not use* to *Use* to the CPU Unit

  And

- When there is no server certificate in the CPU Unit

The value of the IP address of the automatically generated server certificate is generated from the IP address of the built-in EtherNet/IP port at the time.

If you change the IP address after the server certificate is generated automatically or manually, be sure to regenerate the server certificate manually. For details on how to operate, refer to *Regenerating the Server Certificate* in *Server Certificate* in *3-2-5 Setting and Displaying the Certificate*. If the IP address of the server certificate does not match the IP address of the built-in EtherNet/IP port, OPC UA clients can not connect to the OPC UA Server.

3-2-5   Setting and Displaying the Certificate

The following shows how to set and display the certificate and their contents.

The certificate setting can be operated only when online, and only by the *Administrator* in the operation authority verification settings.

The certificate can be displayed only when online, and only by the person other than *Observer* in the operation authority verification settings.

The certificate setting and display consists of the following contents:

- Server Certificate
- Client Authentication
- Issuer Authentication

Server Certificate

You can display and operate the server certificate in the CPU Unit connected online.

1 In the Sysmac Studio, connect online to the CPU Unit, right-click **OPC UA Server Settings** under **Configurations and Setup** - **OPC UA Settings** in Multiview Explorer and select **Server Certificate** from the menu.
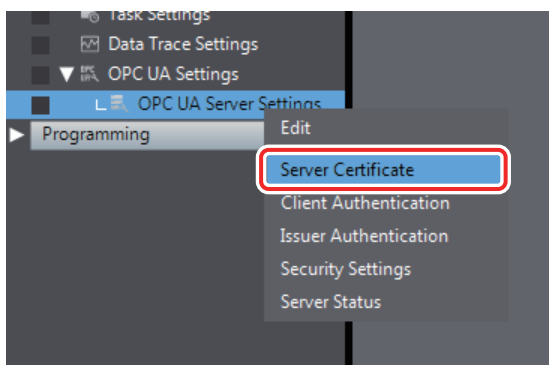
The current server certificate in the CPU Unit is acquired and displayed on the following **Server Certificate** Tab Page.
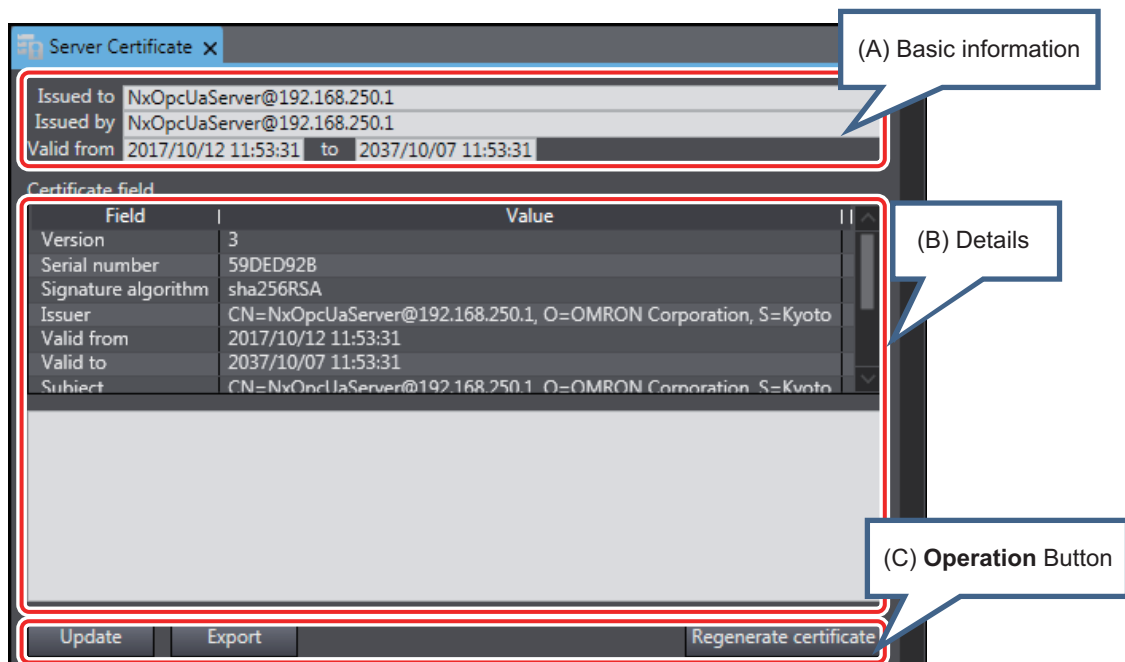
The following contents are displayed.

Classifi-cation	Item *1	Description	
(A) Basic information	Issued to	The common name of the subject is displayed.	Set to NxOpcUaServer @ [IPAddress] in the case of server certificate.
	Issued by	The issuer's common name is displayed.	
			The [IPAddress] part is the IP address of the server certificate.
			Example) NxOpcUaServer @ 192.168.250.1
	Valid from	The start date and time and the end date and time of the validity period are displayed.	
(B) Details	Version	Version information of the certificate.	
	Serial number	Identification number of the certificate.	
	Signature algorithm	Signature algorithm attached to the certificate.	
	Issuer	Name of the issued CA. In the case of a server certificate, it is self-signed and is as follows:	
		CN = NxOpcUaServer@[IPAddress]:, O = Omron Corporation, L = Kyoto, S = Kyoto, C = JP	
		Example: CN=NxOpcUaServer@192.168.250.1, O=Omron Corporation, L=Kyoto, S=Kyoto, C=JP	
	Valid from	Start date and time of certificate validity period. Example: 2017/02/13 19:37:23	
	Valid to	End date and time of certificate validity period. Example: 2027/02/13 19:37:23	
	Subject	Owner of the public key. It is the same as the issuer.	
		Example: CN = NxOpcUaServer@192.168.250.1, O = Omron Corporation, L = Kyoto, S = Kyoto, C = JP	
	Type	---	
	Public key	Public key of the applicant and its types	
	Thumbprint	Message digest of the CA.	
	Detailed Text Box	Detailed information in the selected Certificate field is displayed.	
		• Default status is empty.	
		• Each element of the issuer is displayed in a new line.	
		The IP address of the server certificate is displayed after the first line *CN = NxOpcUaServer@*. This is the IP address of the built-in EtherNet/IP port at the time the server certificate was generated.	
(C) Operation button	**Update** Button	The Server Certificate Setting Tab Page display is updated with the data in the CPU Unit.	
		For details, refer to the *Updating Server Certificate Tab Page* below.	
	Export Button	Export the Server certificate being displayed as an X.509 certificate file.	
		For details, refer to the *Exporting Server Certificate* below.	
	Regenerate certificate Button	Regenerate the secret key and the server certificate in CPU Unit on online connection.	
		For details, refer to the *Regenerating the Server Certificate* below.	

*1. For the meaning of each item, refer to X.509.

📝 **Precautions for Correct Use**

The IP address after *CN = NxOpcUaServer @* displayed in the first line of the above **Detailed Text Box** must match that of the built-in EtherNet/IP port. If it does not match, the OPC UA client can not connect to the OPC UA Server. Then, a *Server Certificate Mismatch* event (event code: 15020000 hex) will occur. In that case, manually regenerate the server certificate.

● **Updating Server Certificate Tab Page**

The display on the **Server Certificate** Tab Page is updated with the data in the CPU Unit connected online.

1 Click the **Update** Button to reacquire the Server Certificate in the CPU Unit and update the **Server Certificate** Tab Page display.

● **Exporting Server Certificate**

The server certificate is exported as X.509 certificate file.

1 When you click the **Export** Button, the following **Export server certificate** Dialog Box is displayed.
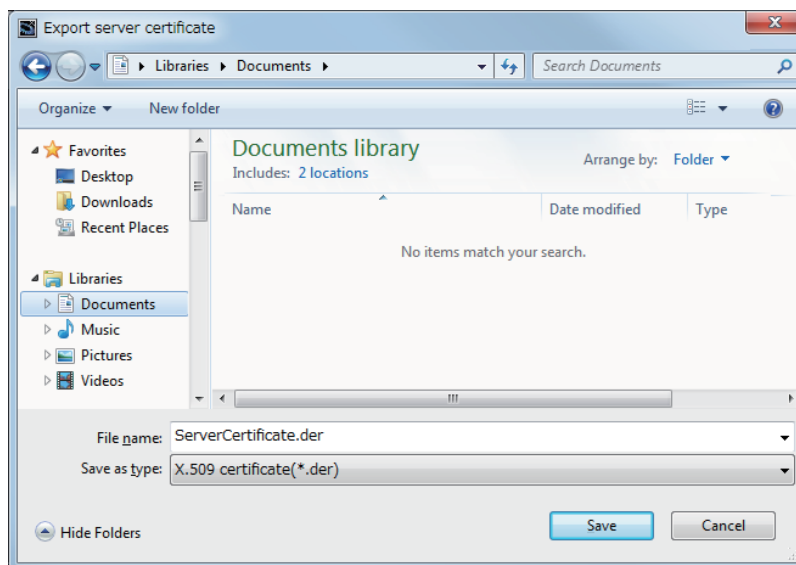
- The file type is *X.509 certificate*, and the identifier is **.der*.
- The default filename is *ServerCertificate.der*.

2 Click the **Save** Button to save the Server certificate file in the specified path.

Precautions for Correct Use

If you replace the CPU Unit or change the IP address of the CPU Unit and regenerate the Server certificate, export the Server certificate by the above operation and import it to the OPC UA client.

● **Regenerating the Server Certificate**

If you set the DN (Distinguished Name) information of the Server certificate and the validity period, you can regenerate the Server certificate in the CPU Unit manually.

The value of the IP address of the server certificate is generated from the IP address of the built-in EtherNet/IP port at the time of regeneration.

If you change the IP address after the server certificate is generated automatically, be sure to regenerate the server certificate manually. If the IP address of the server certificate does not match the IP address of the built-in EtherNet/IP port, OPC UA clients can not connect to the OPC UA Server.

1   When you click the **Regenerate certificate** Button, the following **Regenerate certificate** Dialog Box is displayed.
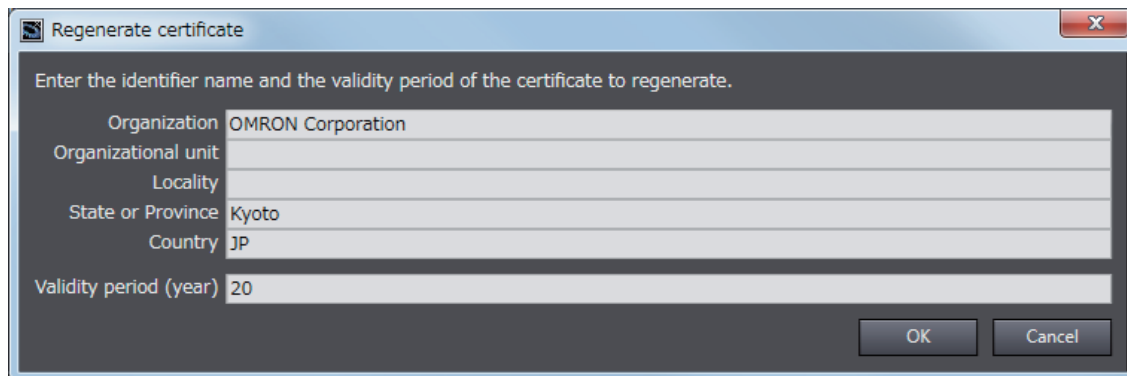
2   Set the following items.

Item	Effective character /range	Default value displayed on the Sysmac Studio	OPC UA Server is set to *Use*, and default value when the Controller power is turned on	Omission
Organization name	0 to 9, a to z, A to Z, half-width space [ ], hyphen [-], dot [.], Underscore [_], comma [,], slash [/], parenthesis [(], closing parenthesis [)]	Value stored in the subject of the Certificate being displayed	OMRON Corporation	Cannot be omitted
Organizational unit name			---	Can be omitted
Municipality			Kyoto	Cannot be omitted
Prefecture	Within 64 characters.		Kyoto	Cannot be omitted
Country	Two half-width alphabetic characters		JP	Cannot be omitted
Validity period (years)	An integer from 1 to 20	20	20	Cannot be omitted

3   When you click the **OK** Button, the following confirmation dialog box is displayed.
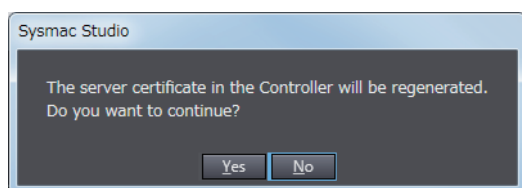
4   Click the **Yes** Button to regenerate the server certificate in the CPU Unit in the entered DN information and valid period. Click the **No** Button to close the confirmation dialog box and return to the state before execution.

After the server certificate is regenerated, communications with OPC UA clients can not be performed as it is. To communicate with the OPC UA clients, export the server certificate and install it on the OPC UA client side. For information on how to export server certificates, refer to *Exporting Server Certificate* on page 3-11.

Client Authentication

You can display and operate self-signed client certificates in the CPU Unit connected online.

> **Additional Information**
>
> For the CA-signed client certificate, refer to the *A-3 When CA-signed Client Certificates Supported* on page A-11.

1 In the Sysmac Studio, connect online to the CPU Unit, right-click **OPC UA Server Settings** under **Configurations and Setup - OPC UA Settings** in Multiview Explorer and select **Client Authentication**.
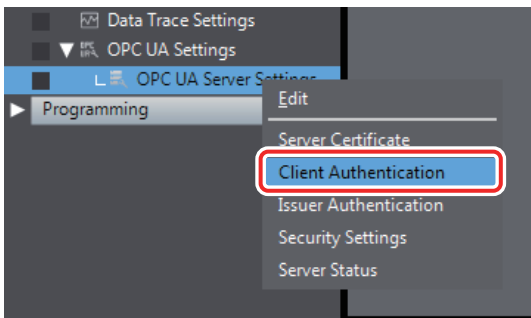
The following **Client Authentication** Tab Page is displayed.

(A) Trusted Certificate List
(B) Certificate Revocation List
(C) Rejected Certificate List
(D) Move to Trusted Certificate Button
(E) **Update** Button

The following contents are displayed.

Parameter	Description
(A) Trusted Certificate List	The Trusted Client Certificate List in the CPU Unit is displayed.
	• Common name, expiration of validity period, organization, domain name are displayed.
	• The default display order is ascending order of common names. You can sort the list by the name of each item by clicking each column header. Ascending and descending order are switched each time you click.
	• **Add** Button ([+]):
	Adds the certificate selected in the **Add Certificate** Dialog Box to the Trusted Certificate List in the CPU Unit. For details, refer to the *Adding a Client Certificate (Transfer to the CPU Unit)* below.
	• **Delete** Button ([🗑]):
	Deletes the selected certificate from the Trusted Certificate List in the CPU Unit.
	For details, refer to the *Deleting a Client Certificate* below.
	• **Show Detail** Button:
	Display details of the selected certificate.
(B) Certificate Revocation List	The **Certificate Revocation List** is used only for CA-signed client certificate.
	For details, refer to the *A-3 When CA-signed Client Certificates Supported* on page A-11.
(C) Rejected Certificate List	The rejected client certificate list in the CPU Unit is displayed.
	• **Delete** Button ([🗑]):
	Deletes the selected certificate from the Rejected Certificate List in the CPU Unit.
	• **Show Detail** Button:
	Display details of the selected certificate.
(D) **Move to Trusted Certificate** Button	The Rejected Certificate List in the CPU Unit is moved to the Trusted certificate.
	• **Move to Trusted Certificate** Button:
	Move the certificate selected in the Rejected Certificate List to the Trusted Certificate.
	For details, refer to *Permitting a Rejected Client Certificate* on page 3-17 below.
(E) **Update** Button	The display in the **Client Authentication** Tab Page is updated with the data in the CPU Unit.
	For details, refer to *Updating the Client Authentication Tab Page* on page 3-19 below.

● **Adding a Client Certificate (Transfer to the CPU Unit)**
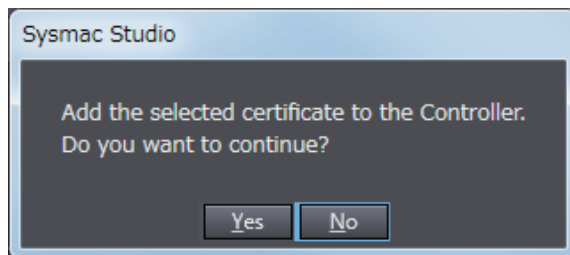
The client certificate file (extension .der) in the computer is added to the Trusted Certificate List in the CPU Unit.

1 Click the **Add** Button ([+]). The following **Add Certificate** Dialog Box is displayed.
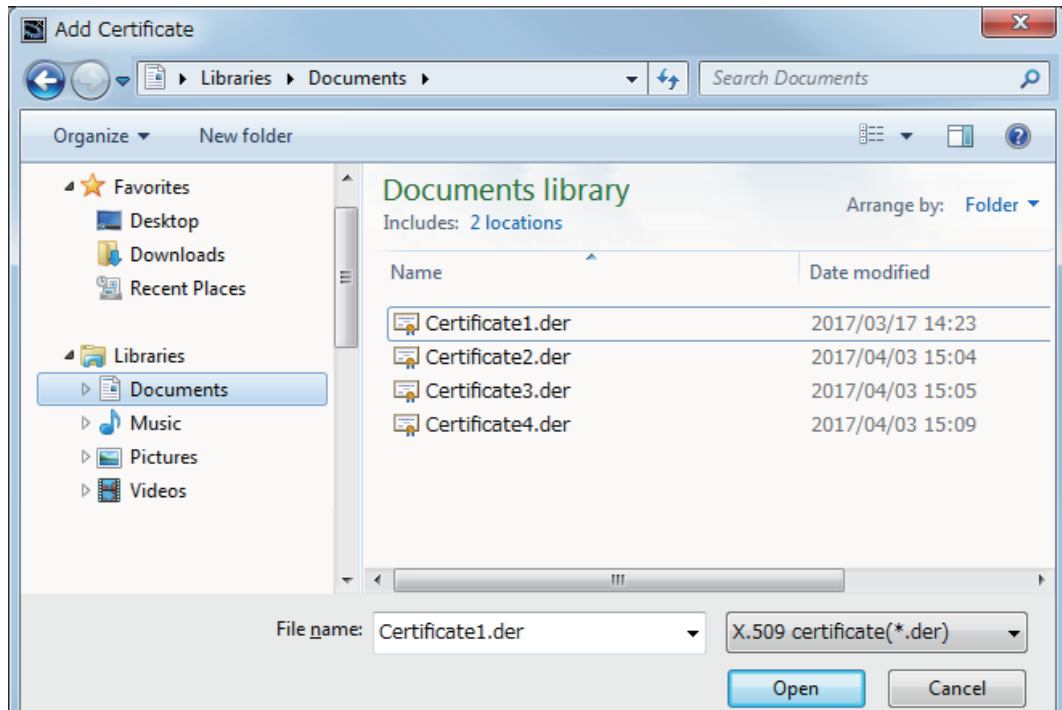
**2**   Select one or more client certificate files (extension .der) to be added, and click the **Open** Button.

The following dialog box to confirm the execution is displayed.

3   If you click the **Yes** Button, the selected client certificate is added to the Trusted Certificate List in the CPU Unit.
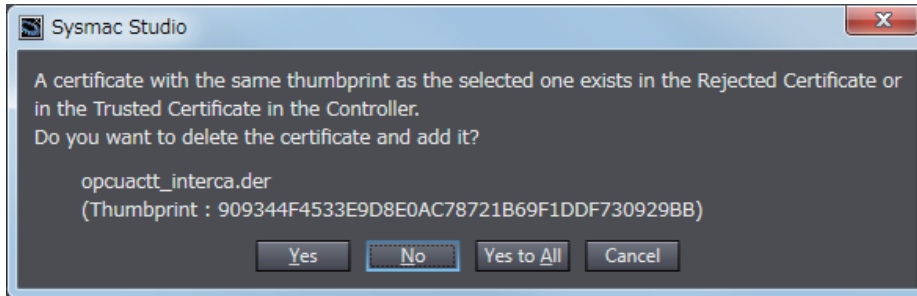
When the addition is successful, the following confirmation dialog box is displayed.
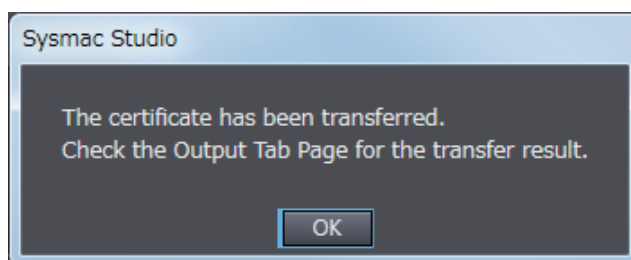
If the addition fails, the following confirmation dialog box is displayed.

- When the client certificate already exists in the Rejected Certificate List

    If the client certificate to be added already exists in the *Rejected Certificate List* in the CPU Unit, the following confirmation dialog box is displayed.

- When the client certificate already exists in the Trusted Certificate List

    If the client certificate to be added already exists in the *Trusted Certificate List* in the CPU Unit, the following confirmation dialog box is displayed.
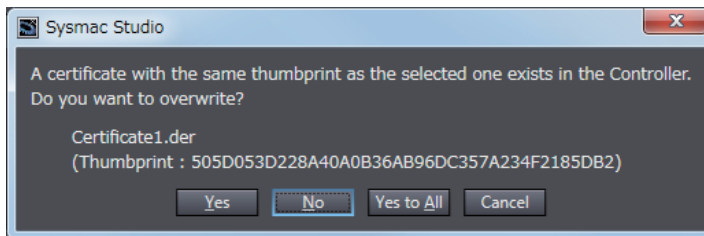
- When the transfer fails

    If the client certificate cannot transfer when you cannot open a client certificate file to be added, the following confirmation dialog box is displayed.
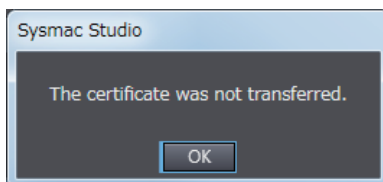
🔊 **Precautions for Safe Use**

Even if you accidentally add the client certificate of a client for which you do not want to permit connection in the *Trusted Certificate List*, the OPC UA Server of the NJ/NX-series Controller will permit connections from that client.

As a result, confidential information on the server side may be leaked or unintended operation may be performed. Therefore, when you add a certificate to the *Trusted Certificate List* from the Sysmac Studio, make sure that all the certificates that you will register in the *Trusted Certificate List* are trusted client certificates.

● **Deleting a Client Certificate**

You can delete the selected client certificate in the CPU Unit. You can delete a certificate in the Trusted Certificate List and the Rejected Certificate List.

1 Select the client certificate you want to delete and click the **Delete** Button (🗑). The following confirmation dialog box is displayed.

> **Sysmac Studio**
>
> Deleting the certificate can not be undone.
> Are you sure you wish to delete it?
>
> [Yes] [No]
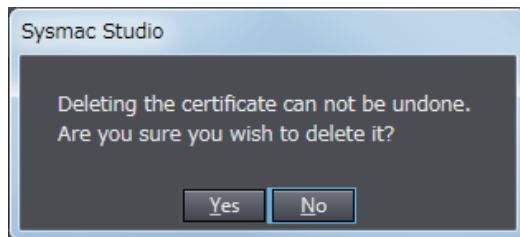
2 Click the **Yes** Button to delete the client certificate in the CPU Unit.

● **Permitting a Rejected Client Certificate**

You can move the selected client certificate from the Rejected Certificate List to the **Trusted Certificate List** in the CPU Unit.

1 Select the client certificate you want to move, and click the **Move to Trusted Certificate** Button.

The following **Processing** Dialog Box is displayed.

> Processing...
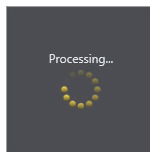
2 After a while, the client certificate in the CPU Unit is moved and the **Client Authentication** Tab Page display is updated to the latest information.

If the move fails, the following confirmation dialog box is displayed.

> **Sysmac Studio**
>
> Could not move the certificate.
> The target certificate does not exist in the Controller.
> Please obtain the latest state by 'update', and then try again.
>
> [OK]
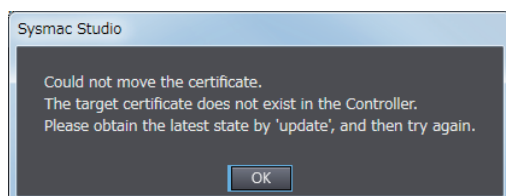
📝 **Additional Information**

Automatic Addition of Client Certificates to the Rejected Certificate List

When an OPC UA client connects to the OPC UA Server and the client does not exist in the Trusted Certificate List, the client's certificate is automatically added to the Rejected Certificate List.

● **Displaying the Detailed View of Certificates**

If you want to display the detailed contents of the selected client certificate, perform the following operations.

1   Click the **Show Detail** Button.

The **Processing** Dialog Box is displayed.
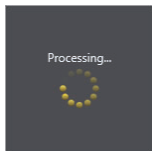
2   After a while, the detailed contents of the client certificate in the CPU Unit are displayed.
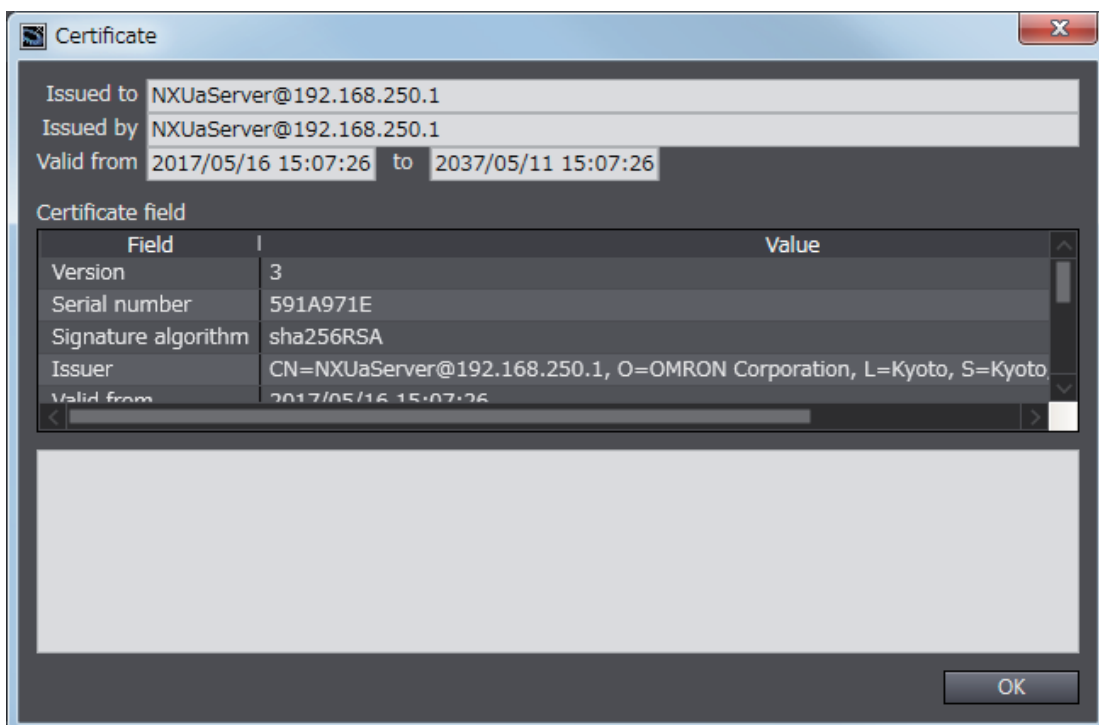
If the certificate details display fails, the following confirmation dialog box is displayed.
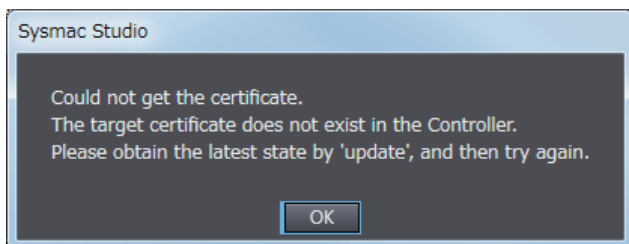
● **Updating the Client Authentication Tab Page**

The display on the **Client Authentication** Tab Page is updated with the data in the CPU Unit connected online.

1 Click the **Update** Button to reacquire the Client Certificate List in the CPU Unit and update the **Client Authentication** Tab Page display.

⬛ **Additional Information**

When a new OPC UA client connects to the server while a client certificate is displayed and operated, and the client does not exist in the Trusted Certificate List, the client's certificate will be automatically added to the Rejected Certificate List. In such a case, it is necessary to update the **Client Authentication** Tab Page.

Issuer Authentication

You can display and operate the certificate authority itself that signed the client certificate in the CPU Unit connected online. For details, refer to the *A-3 When CA-signed Client Certificates Supported* on page A-11.

3-2-6   Security Settings

The following shows how to make the security settings and their contents.

The Security settings consist of the following contents.

- User Authentication Settings
- Anonymous login
- Security Policy

The Security settings can be operated only when online, and only by the *Administrator* in the operation authority verification settings.

1 In the Sysmac Studio, connect online to the CPU Unit, right-click **OPC UA Server Settings** under **Configurations and Setup** - **OPC UA Settings** in Multiview Explorer and select **Security Settings** from the menu.
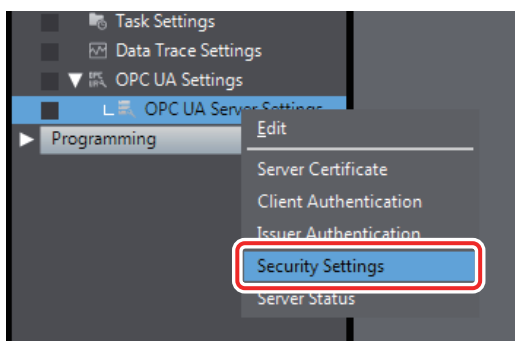
The following **Security Settings** Dialog Box is displayed.
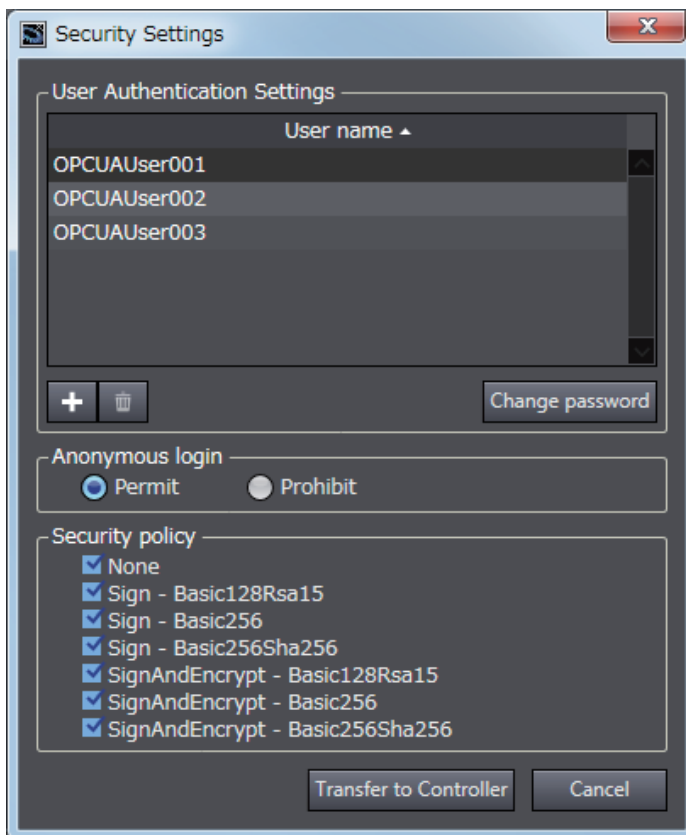
Set the following items.

Parameter	Description	Set value	Default	Update Timing	Changes in RUN mode
User Authentication Settings	The list of configured user names is displayed. • The default display order is the order stored in the user name setting file. You can sort by clicking the header of the user name. Ascending and descending order are switched each time you click. • **Add** Button (+): Adds the user name. For details, refer to *Adding a User Name* on page 3-22. • **Delete** Button (🗑): Deletes the selected user name. • **Change password** Button: Changes the password of the currently selected user name. For details, refer to *Changing the Password* on page 3-22 below.	User name [*1] and password (up to 20 people)	None	When clicking the **Transfer to Controller** Button	Not allowed.
Anonymous login	Sets whether to prohibit or permit anonymous logins.	• Prohibit • Permit	Permit		
Security Policy	Set the allowable range as the server of the Security Mode and Policy in the OPC UA specifications. Multiple checks are possible. For details on the specified items, refer to *5-2-2 OPC UA Security Mode and Policy* on page 5-6.	• None • Sign - Basic128Rsa15 • Sign - Basic256 • Sign - Basic256Sha256 • SignAndEncrypt - Basic128Rsa15 • SignAndEncrypt - Basic256 • SignAndEncrypt - Basic256Sha256	All checked (all allowed)		
Transfer to Controller Button	Transfer the Security Settings (User authentication settings, anonymous login, and security policy) to the CPU Unit. For details, refer to *Transfering the Security Settings* on page 3-23 below.	---	---	---	---

*1. The restrictions on each entry of user name and password are as follows.

Item	Valid character	Range of characters	Default
User name	0 to 9, a to z, A to Z (case sensitive) Note: The following are reserved words and cannot be set (not case sensitive). • Administrator • Designer • Maintainer • Operator • Observer • Anonymous	4 to 32 characters	Blank
Password	0 to 9, a to z, A to Z (case sensitive)	8 to 32 characters	Blank
Confirm New Password	Same as above password.	Same as above password.	Blank

> **Precautions for Correct Use**
>
> When you take security into consideration, be sure to clear *None* under **Security Policy**.

● **Adding a User Name**

Add a user name.

1 When you click the **Add** Button(+), the following **Add a User** Dialog Box is displayed.

2 In the **User name** field, enter the user name, and enter the password in the **Password** and **Confirm Password** fields, and then click the **OK** Button.

● **Changing the Password**

Change the password of the currently selected user name.

1 Click the **Change password** Button, the following **Change Password** Dialog Box is displayed.

2 Enter the password in the fields of **Current Password**, **New Password**, and **Confirm New Password**, and click the **OK** Button.

● **Transfering the Security Settings**

The Security Settings (user authentication setting, anonymous login, and security policy) displayed in the **Security Settings** Tab Page are transferred to the CPU Unit.

1 Click the **Transfer to Controller** Button. The following dialog box is displayed.

> **Sysmac Studio**
>
> Transfer the security settings to the Controller. Do you want to continue?
>
> [Yes] [No]
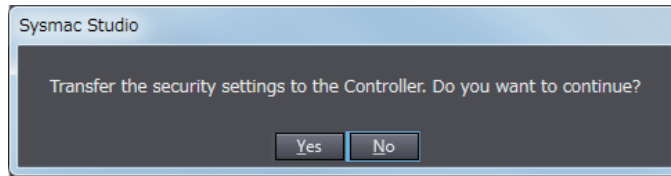
2 Click the **Yes** Button to transfer the User name and Password displayed in the User Authentication Settings to the CPU Unit.

When the transfer is successful, the following confirmation dialog box is displayed.

> **Sysmac Studio**
>
> The security settings were transferred.
>
> [OK]
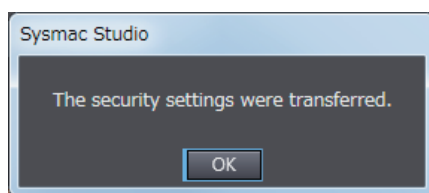
3-2-7   Server Status

You can check the status of the OPC UA Server such as the operating status of the OPC UA Server and the number of connected clients.

You can also instruct the shutdown of the OPC UA Server from the Sysmac Studio.

For details, refer to *4-2-1 Checking Based on OPC UA Server Status of the Sysmac Studio* on page 4-5.

3-2-8   Displaying the Operation Logs

You can display a list of the Execution Logs in the SD Memory Card mounted in the CPU Unit and operate the list.

For details, refer to *7-2-2 Checking Logs in the Operation Log Window in the Sysmac Studio* on page 7-13.

> **Additional Information**
>
> In view of future expansion of functions, in the Sysmac Studio, the display of the Execution Logs is placed under the *Operation Log* Display as the lower level of the upper concept *Operation Log*.

3-2-9   Operations for the OPC UA Settings

The following table shows whether the setting data of the OPC UA Settings is applied for each operation of synchronization (transfer), backup or restore, or Clear All Memory.

OK: Applicable, AS:Applicable by selection, NA: Not applicable

Setting data of OPC UA Settings		Operations				
		Synchronization (transfer) from the Sysmac Studio	Backup	Restore		Clear All Memory operation from the Sysmac Studio
			One of the following cases: • SD Memory Card Backup functions • Sysmac Studio Controller backup functions	When one of the following methods is used: • SD Memory Card Backup function • Sysmac Studio Controller Backup function	When one of the following methods is used: • Automatic transfer from SD Memory Card • Program transfer from SD Memory Card	
OPC UA Server settings		OK	OK	OK	OK	Clear
Server certificate		NA	NA	NA	NA	Select whether to clear or not.
OPC UA security profile	Client certificate	NA	OK [*1]	AS [*2]	NA	
	CA certificate					
	Certificate Revocation List					
	Security settings (User authentication settings, anonymous login, and security policy)					
Execution Log		NA	NA	NA	NA	Do not clear

*1. Client certificates, CA certificates, Certificate Revocation Lists, and Security Settings are not applicable when exporting and importing backup files in the Sysmac Studio.

*2. Whether to restore or not can be selected below.
When the SD Memory Card backup function is used: Depends on the restore command file (RestoreCommand.ini).
When the Sysmac Studio Controller backup function is used: Depends on selecting the *data to restore* in the **Restore** Dialog Box.

3-3   Creating Variables for OPC UA Communications

This section describes how to create variables for OPC UA communications.

The variables that can be published to OPC UA communications are the global variables [1].

*1. System-defined variables can not be published to OPC UA communications.

3-3-1   Global Variables Published to OPC UA Communications

To publish global variables to the OPC UA communications, the attributes of variables is set to *Network Publish Attribute*.

1   In the Global Variable Editor of the Sysmac Studio, set the *Network Publish* attribute of the global variable to *Public Only*, *Input*, or *Output*.

Variables in which these attributes are set are called *variables published to the network*.
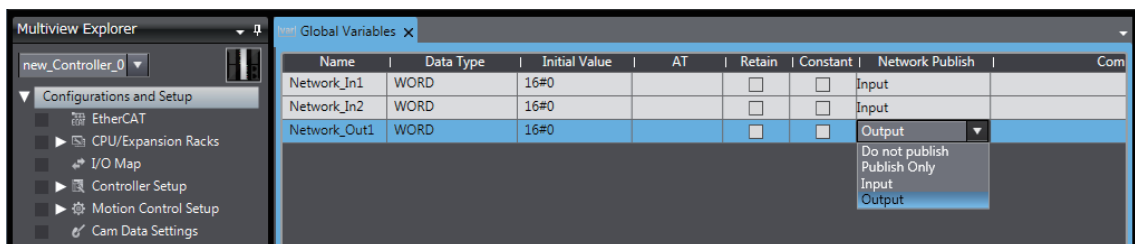
If a variable is published to the network, it can be read and written from the OPC UA client.

The possibility of reading from or writing to the OPC UA client in accordance with the network publish attribute is as follows.

Attributes of Variables	Set value	Possibility of reading from or writing to the OPC UA client	
		Read	Write
Network Publish Attribute	Do not publish (default value in the Sysmac Studio).	No	No
	Publish Only	Yes	Yes
	Input	Yes	Yes
	Output	Yes	Yes

The following table shows the maximum number of variables and value attributes with the Network Publish attribute that can be published to clients as an OPC UA Server.

Item	Maximum number
Number of public variables	10,000
Number of value attributes	10,000

For details of the data types that can be published, refer to *6-2 Reading/Writing Variables from the OPC UA Client* on page 6-3.

📑 **Additional Information**

Publish Only, *Input*, and *Output* in the *Network Publish* attribute are settings shared with Ether-Net/IP communications. As for OPC UA communications, there is no difference between *Publish Only*, *Input*, and *Output*.

3-3-2   Adding or Deleting Network-published Variables

You can add or delete network-published variables in either of the following ways:

• Downloading (synchronization) after editing the global variable table offline
• Online editing

4

Starting and Checking the Status of the OPC UA Server

This section describes how to start or stop the OPC UA Server, and also how to check the status of the OPC UA Server.

4-1   Starting or Stopping the OPC UA Server

This section describes how to start or stop the OPC UA Server.

4-1-1   How to Start or Stop the OPC UA Server

The method of starting and stopping the OPC UA Server and the method of starting the OPC UA Server after stopping it are described below.

Starting the OPC UA Server

The method of starting the OPC UA Server is as below.

1   In the Multiview Explorer of the Sysmac Studio, double-click **OPC UA Server Settings** under **Configurations and Setup - OPC UA Settings**. Or, right-click **OPC UA Server Settings** and select **Edit** from the menu.

2   Select *Use* Option for **OPC UA Server** under **OPC UA Settings - OPC UA Server Settings**. The factory default setting is *Do not use* (Stop).

3   Place the Sysmac Studio online with the CPU Unit and download (synchronize) *OPC UA Settings*.

4   Cycle the power supply to the Controller or reset the Controller.
The OPC UA Server Use Option is enabled and the OPC UA Server starts.

> **Precautions for Correct Use**
>
> When you download (synchronize) or restore the *OPC UA Settings* by changing **OPC UA Server** to *Use* from *Do not use*, you must either cycle the power supply to the Controller or reset the Controller in order to start the OPC UA Server. The OPC UA Server will not start unless you cycle the power supply to the Controller or reset the Controller.

Stopping the OPC UA Server

Either of the following methods can be used to stop the OPC UA Server.

● **Method a) Executing the OPCUA_Shutdown (Shutdown OPC UA Function) instruction from the user program**

For the OPCUA_Shutdown (Shutdown OPC UA Function) instruction, refer to *A-2-1 OPCUA_Shutdown (Shutdown OPC UA Function)* on page A-7.

● **Method b) Shutting down from the Sysmac Studio**

1   Place the Sysmac Studio online with the CPU Unit, right-click **OPC UA Server Settings** under **Configurations and Setup - OPC UA Settings** in the Multiview Explorer, and then select **Server Status**.

2   Click the **Server shutdown** Button.

Starting the OPC UA Server after Stopping It

To start the OPC UA Server after shutting it down, either cycle the power supply to the Controller or reset the Controller.

4-1-2   Conditions under Which the OPC UA Server Cannot be Started

The OPC UA Server cannot be started in the following cases.
- When the OPC UA Server is in the *Halt error* state
- When the Controller power is not turned ON again, or the Controller is not reset after the OPC UA Server is in *Shutdown* state
- When the Controller power is not turned ON again or the Controller is not reset after the **OPC UA Server** is changed from *Use* to *Do not use* and the *OPC UA Settings* are downloaded (synchronized) or restored.

4-1-3   Conditions under Which the OPC UA Server Stops

The OPC UA Server stops in the following cases.
- When the OPC UA Server shut down from the Sysmac Studio or the OPCUA_Shutdown (Shutdown OPC UA Function) instruction is executed
- When the Controller power is turned ON again or the Controller is reset after the **OPC UA Server** is changed from *Use* to *Do not use* and the *OPC UA Settings* are downloaded (synchronized) or restored.
- When the data is restored from the SD Memory Card or the Sysmac Studio
- When the Clear All Memory operation is executed from the Sysmac Studio

Additional Information

- The OPC UA Server continues to operate even when a major fault level Controller error occurs.
- When a Controller error occurs and you refer to the address space of the NJ/NX-series Controller from the OPC UA client, you can check the following from *ErrorStatus* under *DeviceStatus*.
  - NoError: Normal
  - MajorFault: Major fault
  - ContinuousError: Partial fault or minor fault

4-1-4   Operation of the OPC UA Service Function in each State of the CPU Unit

The execution state of the OPC UA service function changes depending on the state of the CPU Unit. The operation of the OPC UA service function in the *startup state*, *normal operation*, and *error state* is described below.

Process of CPU Unit		OPC UA Service function
Operation during startup state		Stopped.
Operation during normal operation	PROGRAM mode	Executed.
	RUN mode	Executed.
	Downloading	Stopped.
	During online editing	Executed.
	During backup	Executed.
	During restore operation, after restore operation	Stopped. The power supply must be cycled or the Controller must be reset after restoring data.
	During execution of Clear All Memory operation, after execution of Clear All Memory operation	Stopped. The power supply must be cycled or the Controller must be reset after the execution of Clear All Memory operation.
Error state	Major fault	Executed. However, stopped during a CPU error (WDT error).
	Partial fault	Executed. However, stopped during an OPC UA Server error.
	Minor fault	Executed. However, may be stopped during an OPC UA Server error.

4-2 Checking the Status of the OPC UA Server

This section describes how to check the status of the OPC UA Server.

You can use the following methods to check the status of the OPC UA Server.
- OPC UA server status of the Sysmac Studio
- Event log
- Execution Log

4-2-1 Checking Based on OPC UA Server Status of the Sysmac Studio

The method of checking the server status and its contents are described below.

The server status can be operated only in the online state.

1 Place the Sysmac Studio online with the CPU Unit, right-click **OPC UA Server Settings** under **Configurations and Setup - OPC UA Settings** in the Multiview Explorer, and then select **Server Status**.
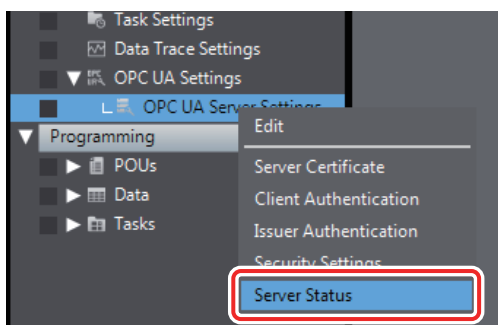
The following **Server Status** Tab Page is displayed.
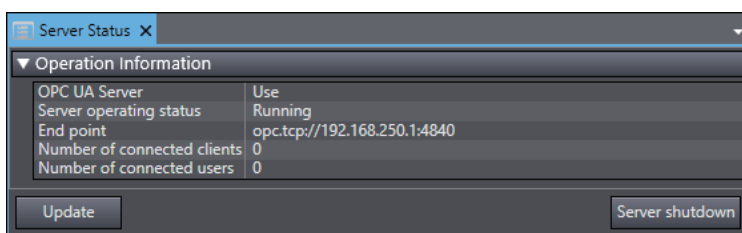
You can check the following states unless the operating status of the OPC UA Server is *Initializing* or *Shutdown*.

Category	Item	Description
Operation Information	OPC UA Server	Displays the setting status of the OPC UA Server. Any one of the following is displayed. • Use • Do not use
	Server operating status	Displays the operating status of the OPC UA Server. Any one of the following is displayed. • Initializing • Preparing • Running • Halt error • Shutdown Refer to *4-2-5 Conditions for Reconfiguring the OPC UA Server* on page 4-9 for details on the operating status
	End point	Displays the end point of the OPC UA Server. • The end point is displayed only when the server operating status is *Running*. • When the server operating status is other than the above, "---" is displayed.
	Number of connected clients	Displays the number of currently connected OPC UA clients. • "---" is displayed only when the server operating status is *Initializing*. • When the server operating status is other than the above, the number of connected clients is displayed.
	Number of connected users	Displays the number of currently connected users.
Buttons	**Update** Button	Acquires the operation information from the server and updates the Server Status Tab Page.
	Server shutdown Button	Shuts down the server function. For details, refer to *Shutting Down the Server Function* below.

● **Shutting Down the Server Function**

Shutdown the OPC UA Server.

1   When you click the **Server shutdown** Button, the following confirmation dialog box is displayed.

Sysmac Studio

Shutting down the server stops all OPC UA communications and access to the memory card.
It is not possible to start the server until you cycle the power supply of the Controller.
Are you sure you want to execute the operation?

Yes   No
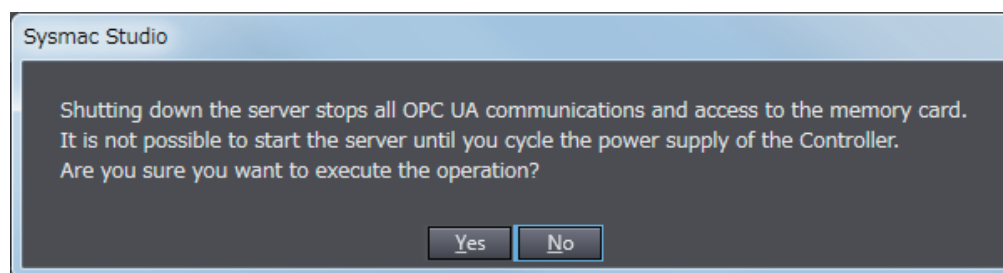
2   Click the **Yes** Button. The following dialog box is displayed.

Sysmac Studio

The server was shut down.

OK
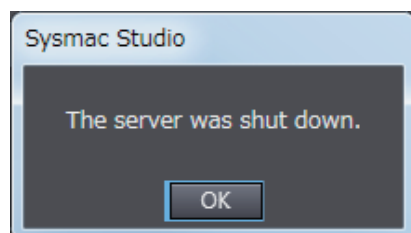
4-2-2   Checking Based on the Event Log

You can check the operating status of the OPC UA Server by the event log of the Controller.

For details, refer to *9-2 Troubleshooting* on page 9-7.

4-2-3   Checking Based on the Execution Log

You can check the operating status of the OPC UA Server by the Execution Log function of the OPC UA Server.

For details, refer to *Section 7 Execution Log Functions*.

4-2-4   Operating Status of the OPC UA Server

This section describes the operating status of the OPC UA Server.

The OPC UA Server has five operation states, such as *Initializing*, *Preparing*, *Running, Halt error*, and *Shutdown*. The operating status transits as shown in the figure below.
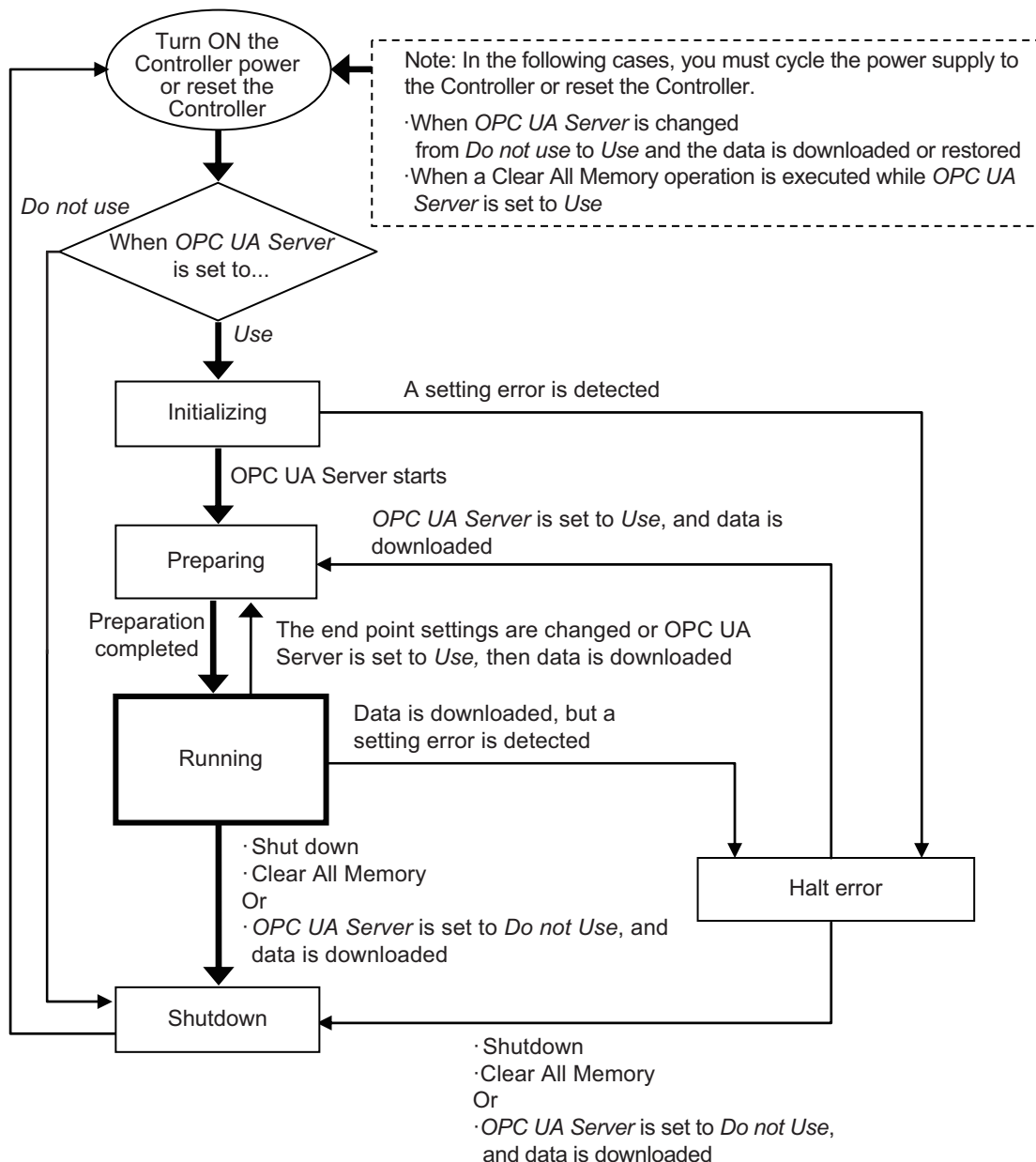
- If the OPC UA server is set to *Use* after the Controller power is turned ON [*1], the OPC UA Server enters the *Initializing* state. When the initialization process is complete, the OPC UA Server enters the *Preparing* state, then it shifts to the *Running* state after the completion of preparation.

- In the *Running* state, if the OPC UA Server is shutdown [*2], or if OPC UA server is set to *Do not Use* and data is downloaded, the OPC UA Server shifts to the *Shutdown* state.

*1. In the following cases, you must cycle the power supply to the Controller or reset the Controller.

- When *OPC UA Server* is changed from *Do not use* (setting in the CPU Unit) to *Use* and the data is downloaded or restored*

  * It includes both the Restore operation executed from the SD memory card and the Restore operation executed from the Sysmac Studio.

- When a Clear All Memory operation is executed while *OPC UA Server* is set to *Use* (setting in the CPU Unit)

*2. When shutdown of the OPC UA Server is instructed from the Sysmac Studio, or when the OPCUA_Shutdown (Shutdown OPC UA Function) instruction is executed.

The details of each status are given below.

Status	Description	Remarks
Initializing	This is the status in which the initial processing of the OPC UA Server is executed.	The OPC UA server settings are read, and each function or monitor is initialized.
Preparing	This is the status in which the OPC UA Server is prepared.	The Controller shifts to this status when the OPC UA Server is used. Configuration of the end point and configuration of the address space (variables to be published) is performed in this status. This is the status in which requests from the OPC UA client cannot be accepted.
Running	This is the status in which the OPC UA Server is running.	The Controller shifts to this status when the configuration of the OPC UA Server is completed. This is the status in which requests from the OPC UA client can be accepted.
Halt error	This is the status in which the OPC UA Server is stopped due to a setting error.	The Controller shifts to this status when a setting error is detected during initialization, or when a download is executed during operation, and a setting error exists in the data.
Shutdown	This is the state while the OPC UA Server is processing to shut down, or when the OPC UA Server has shutdown.	The Controller shifts to this state in the following cases: • When shutdown of the OPC UA Server is instructed from the Sysmac Studio, or when the OPCUA_Shutdown (Shutdown OPC UA Function) instruction is executed • OPC UA Server is set to Do not Use, and data is downloaded After the shutdown processing of the OPC UA Server is completed, the user can safely turn OFF the power supply to the Controller. The OPC UA Server cannot be started until you cycle the power supply to the Controller or reset the Controller.

4-2-5   Conditions for Reconfiguring the OPC UA Server

The OPC UA Server is reconfigured if the following changes are made while the OPC UA Server is running.

- When synchronization (download) is executed
- When the restore operation is executed
- When the IP address of the built-in EtherNet/IP port is changed
- When the server certificate is regenerated
- When the security settings are updated

> **Additional Information**
>
> Even if a network-published variable is added by online editing while the OPC UA Server is running, the OPC UA Server is not reconfigured, and the network-published variable is added to the existing address space. In that case, OPC UA clients can access to the variable that you have added.

5

Security Function of OPC UA Server

This section describes the security function of the OPC UA Server.

5-1   Details of the Connection Authentication Function of the OPC UA Server

This section describes the following two stages of connection functions in detail with regard to the connection authentication function of the OPC UA Server.

Function	Description
Application authentication	Authentication of applications between the OPC UA server and OPC UA client
User authentication	Authentication of the user that operates the client applications of the OPC UA

5-1-1   Application Authentication

The OPC UA server and the OPC UA client authenticate each other's identity by exchanging mutual digital certificates (hereinafter, called *certificates*). This is called *Application authentication*.

In application authentication, the certificates supported by the OPC UA server and the OPC UA client are X.509-standard certificates.

The certificates supported by the OPC UA Server are of the following three types:

Certificate	Description
Server certificate	This is a certificate for certifying an OPC UA server. In the case of an OPC UA server, it is a self-signed certificate.
Client certificate	This is a certificate for certifying the OPC UA client.
	Both self-signed client certificates and CA-signed client certificates can be used.
CA certificate and Certificate Revocation List	In the case of a CA-signed client certificate, this certificate is used to authenticate the certificate chain.

In the OPC UA Server, the following functions are enabled for each certificate:

Certificate	Function
Server certificate	• Generation (automatic generation or manual regeneration [1]) of the server certificate (self-signed certificate)
	• Export of the server certificate from the CPU Unit [1]
	• Advance expiration notice of the server certificate, and notification of expiry
Client certificate	• Authentication of the client certificate during a connection [1]
	• Addition of the client certificate (transfer to the CPU Unit) [1]
	• Trust or reject setting of the client certificate [1]
	• Notification of expiry of client certificate
CA certificate and	Used only in the case of a CA-signed client certificate.
Certificate Revocation List	For details, refer to *A-3 When CA-signed Client Certificates Supported* on page A-11.

*1. This operation can be performed only by the *Administrator* in the operation authority verification settings of the Sysmac Studio.

For details on each operation method from the Sysmac Studio, refer to *3-2-5 Setting and Displaying the Certificate* on page 3-9.

Server Certificate

In the OPC UA Server, the following functions are enabled for the server certificate.

● Generation of the Server Certificate (Self-signed Certificate)

The server certificate can be generated by any of the following methods. Each of these methods is for a self-signed certificate.

- Automatic generation

  If a server certificate does not exist in the CPU Unit when the OPC UA Server is started, the server certificate is automatically generated.

  The contents of the server certificate that is automatically generated are as follows:

Category	Item *1	Description
Basic information	Issued to	NxOpcUaServer@[IPAddress]
	Issued by	[IPAddress] is the IP address of the built-in EtherNet/IP port at the time of automatic generation.
	Valid from	The server certificate is valid from the date and time of automatic generation up to the date and time twenty years from the start date and time
Detailed information	Version	Version information of the certificate
	Serial number	Unique to each certificate
	Signature algorithm	Algorithm of the signature added to the certificate.
	Issuer	CN = NxOpcUaServer@[IPAddress]:, O = Omron Corporation, L = Kyoto, S = Kyoto, C=JP
		[IPAddress] is the IP address of the built-in EtherNet/IP port at the time of automatic generation.
	Valid from	Date and time of automatic generation
	Valid to	Date and time twenty years from the date and time of automatic generation
	Subject	Same as the issuer
	Public key	Public key of the applicant and its types.
	Thumbprint	Message digest of the CA.
	Detailed Text Box	Each element of the issuer is displayed in a new line.

*1. For the meaning of each item, refer to X.509.

- Manual regeneration

  By setting the DN (Distinguished Name) information and the valid period of the server certificate, the server certificate in the CPU Unit can also be manually regenerated.

  This function is executed when it is necessary to recreate the server certificate, for example, when the following events occur:

  Server Certificate Mismatch (event code: 15020000 hex)

  Server Certificate Expired (event code: 35D10000 hex)

  Server Certificate Expiration Notice (event code: 35D20000 hex)

  Note that regeneration of the server certificate can be executed only by the *Administrator* set as the operation authority.

Precautions for Correct Use

When you download to the CPU Unit a project for which **OPC UA Server** is set to *Use* in the OPC UA Settings, and then cycle the power supply to the Controller, the server certificate is automatically generated by the IP address of the built-in EtherNet/IP port at that time.

Thereafter, when you change the IP address of the built-in EtherNet/IP port, the IP address of the built-in EtherNet/IP port and the IP address of the server certificate do not match. Therefore, a *Server Certificate Mismatch* event (event code: 15020000 hex) occurs. In that case, manually regenerate the server certificate, or set the IP address back to the original address.

● **Export of the Server Certificate from the CPU Unit**

Export the server certificate in the CPU Unit.

This function is executed in cases where the OPC UA client side requires the server certificate before connecting to the OPC UA server.

Note that export of the server certificate can be executed only by the *Administrator* set as the operation authority.

● **Advance Expiration Notice of the Server Certificate, and Notification of Expiry**

The CPU Unit performs a notification 30 days before the expiry of the server certificate, and also when the server certificate expires.

The notification is recorded in the event log and the Execution Log.

Client Certificate

A self-signed client certificate is described below.

For details on using a CA-signed client certificate, refer to *A-3 When CA-signed Client Certificates Supported* on page A-11.

In the OPC UA Server, the following functions are enabled for the client certificate.

● **Authentication of the Client Certificate during a Connection**

The OPC UA Server compares the client certificate that is sent during a connection from the OPC UA client, and the client certificate in the Trusted Certificate List that is set from the Sysmac Studio, and allows the connection only if the client certificate is set in advance in the Trusted Certificate List.

If the client certificate does not exist, the OPC UA Server saves the client certificate in the Rejected Certificate List and rejects the connection.

The client certificate is saved in the following locations in the CPU Unit. Each of these locations is set from the Sysmac Studio.

Save location	Description
Trusted Certificate List	This is the location where the certificates of the OPC UA client that are allowed a connection are placed.
Rejected Certificate List	This is the location where the certificates of the OPC UA client that are rejected a connection are placed.

● **Addition of the Client Certificate (Transfer to the CPU Unit)**

This function is executed in cases where the OPC UA Server requires the client certificate before connecting to the OPC UA client.

Note that addition (transfer) of the client certificate to the CPU Unit can be executed only by the *Administrator* set as the operation authority.

● **Automatic Addition of the Client Certificate to the Rejected Certificate List**

In the following case, the CPU Unit automatically adds the client certificate of the OPC UA client to the Rejected Certificate List.

• When the OPC UA client establishes a connection with the OPC UA Server, and when the OPC UA client does not exist in the Trusted Certificate List in the CPU Unit

● **Trust or Reject Setting of the Client Certificate**

By placing the Sysmac Studio online with the CPU Unit, and moving the client certificate of the CPU Unit as described below, you can set whether to trust or reject a connection.

Note that the trust or reject settings of the client certificate can be made only by the *Administrator* set as the operation authority.

• Settings for allowing a connection

The client certificate is moved from the Rejected Certificate List to the Trusted Certificate.

● **Notification of Expiry of Client Certificate**

The CPU Unit performs a notification when the certificate in the Trusted Certificate List expires.

The notification is recorded in the event log and the Execution Log.

5-1-2　User Authentication

The OPC UA Server authenticates the identity of the user that operates the client applications of the OPC UA by either of the following methods.

• Authentication based on user name and password
• Authentication based on Anonymous

This is called *User authentication*.

The OPC UA Server supports *Allow access to all* in a fixed manner as the user access authority of the OPC UA.

For details on the operation method from the Sysmac Studio, refer to *Adding a User Name* and *Changing the Password* in *3-2-6 Security Settings* on page 3-20.

Authentication Based on User Name and Password

Only users for whom the user name and password are matching can connect to the OPC UA Server.

Note that registration, deletion, and change of the user name and password can be executed only by the *Administrator* set as the operation authority.

Authentication Based on Anonymous

It is also possible to not perform authentication of the identity of the user that operates the client applications of the OPC UA by the user name and password.

5-2 Details of the Message Security Function

This section describes the details of the message security function in the OPC UA communications.

In the OPC UA Server, the signature and encryption of messages allowed by the server is set by a security policy.

5-2-1 Signature and Encryption

- Signature refers to signature information that is added and encrypted to assure the validity of certificates and messages.
- Encryption refers to conversion of a message into a code whose meaning is not understood by a particular method (algorithm) during the transmission and reception of the message so that it is not stolen or modified by a third person during communications.

5-2-2 OPC UA Security Mode and Policy

This is a security mechanism for messages that are allowed during exchange with the OPC UA client.

The signature for the messages, the encryption of messages, and the algorithm for the signature and encryption are set.

Place the Sysmac Studio online with the CPU Unit, and make the settings as shown below.

In the Multiview Explorer, right-click **OPC UA Server Settings** under **Configurations and Setup - OPC UA Settings**, and then select **Security Settings**. Under **Security Policy**, specify the OPC UA security mode and policy to be allowed from the following. You can select multiple items.

OPC UA security modes and policies that can be selected	Description	
None	Neither signature nor encryption are required. Not recommended for security reasons.	
Sign - Basic128Rsa15	A signature is required and the integrity (measures against modifications, etc.) of data is secured.	Basic128Rsa15 is supported as the algorithm of the signature.
Sign - Basic256		Basic256 is supported as the algorithm of the signature.
Sign - Basic256Sha256		Basic256Sha256 is supported as the algorithm of the signature.
SignAndEncrypt - Basic128Rsa15	A signature and encryption are required, and the integrity (measures against modifications, etc.) and reliability (measures against wiretapping, etc.) of data are secured.	Basic128Rsa15 is supported as the algorithm of the signature and encryption.
SignAndEncrypt - Basic256		Basic256 is supported as the algorithm of the signature and encryption.
SignAndEncrypt - Basic256Sha256		Basic256Sha256 is supported as the algorithm of the signature and encryption.

For details on the OPC UA security mode and policy, refer to the OPC UA specifications.

Precautions for Correct Use

When you take security into consideration, be sure to clear *None* under **Security Policy**.

6

Connecting from the OPC UA Client and Reading/Writing Variables

This section describes establishing a connection from the OPC UA client and reading/writing the variables of the OPC UA Server.

6

6-1   Connecting from the OPC UA Client

This section presents an overview of connecting to the OPC UA Server from the OPC UA client.

Execute the following on the OPC UA server from the OPC UA client.
- Specify the URL of the target OPC UA Server
- Connect to the target OPC UA Server

6-1-1   Specifying the URL of the Target OPC UA Server

Enter *opc.tcp://[IP address]:[Port No.]/* as the URL, and specify the end point of the target OPC UA Server.

As for the URL, enter the URL set in **OPC UA Server Settings - End Point** under **Configurations and Setup - OPC UA Settings** in the Multiview Explorer of the Sysmac Studio.

(By default, *opc.tcp://192.168.250.1:4840/* is set.)

6-1-2   Connecting to the Target OPC UA Server

Set the security policy within the range permitted at the server side[1].

For details on OPC UA security modes and policies that can be selected, refer to *5-2 Details of the Message Security Function* on page 5-6.

[1]. The range of permitted security policies depends on the setting of **Security Policy** under **Security Settings**, which is displayed when **OPC UA Server Settings** is right-clicked under **Configurations and Setup - OPC UA Settings** in the Multiview Explorer of the Sysmac Studio.

Select a user authentication method within the permissible range at the server side.

If you select a method based on the user name and password, enter the user name and password[2].

[2]. Set from **OPC UA Server Settings - Security Settings** under **Configurations and Setup - OPC UA Settings** in the Multiview Explorer of the Sysmac Studio.

Additional Information

If a connection cannot be established, check for a connection error at the OPC UA client, and then check the settings, etc.

As for the status at the server side, connect the Sysmac Studio to the NJ/NX-series Controller, check for a certificate error, connection rejection, etc. from the event log, and then take necessary actions. For details, refer to *9-2 Troubleshooting* on page 9-7. Or, check the contents of the Execution Log, and take necessary actions. For details, refer to *Section 7 Execution Log Functions*.

6-2 Reading/Writing Variables from the OPC UA Client

This section describes the address space of the NJ/NX-series Controller visible to the OPC UA client, and also reading/writing the variables of the CPU Unit from the OPC UA client.

6-2-1 Address Space of the NJ/NX-series Controller

The address space of the NJ/NX-series Controller is published as described below.

Address space of the NJ/NX-series Controller that can be referenced by the client

```
Root
  ⊢Objects
     ⊢ DeviceSet
        ⊢ Configuration
           ⊢ Resources
              ⊢SupportedTypes
                 ⊢ NxControllerType
              ⊢ ContollerName ◄─────────── Controller name
                 ⊢ DeviceStatus ◄────────── Controller state
                    ⊢ ErrorStatus ◄──────── Error state of the Controller
                    ⊢Mode ◄──────────────── Mode of the Controller
                    ⊢ UnpublishedVariablesStatus ◄── Status of unpublished variables
              ⊢ GlobalVars ◄─────────────── Published variables
                 ⊢ Var1 ⎫
                 ⊢ Var2 ⎬ ◄───────────────── Each Published variable
                 ⊢ Var3 ⎭
                 ⊢ NumOfVars ◄────────────── Number of published variables
                 ⊢ NumOfValues ◄──────────── Number of value attributes
                                             of published variables
```

Controller Name

The Controller name set in the Sysmac Studio is displayed as the folder name.

Controller State

The Controller state is displayed as shown below under *DeviceState*.

Properties	Description	Values
ErrorState	Indicates the error state of the Controller.	• NoError: Normal • MajorFault: Major fault • ContinuousError: Partial fault or minor fault
Mode	Indicates the mode of the Controller.	• RUN: RUN mode • PROGRAM: PROGRAM mode
UnpublishedVariablesStatus	Indicates the status of unpublished variables	The following bits change to TRUE when a relevent error occurs. Bit 00: Number of Public Variables Exceeded Bit 01: Number of Published Value Attributes Exceeded Bit 02: The number of user-defined data types has been exceeded Bit 03: Variables of an unsupported data type exist Bit 04 to bit 15: Reserved (The value is FALSE)

Number of Published Variables

The number of variables published under GlovalVars of the OPC UA Server is displayed. This will allow you to check if the number of variables exceeds the upper limit.

Number of Value Attributes of Published Variables

The number of value attributes in the OPC UA attribute of the variables published under GlovalVars of the OPC UA Server is displayed. As a result, it is possible to check if the number of value attributes of variables exceeds the upper limit.

6-2-2 Reading/Writing the Variables of the CPU Unit

With a read/write request from the OPC UA Client, global variables can be read from or written to the CPU Unit via the target OPC UA Server.

Reading/writing the Global Variables of the CPU Unit

The OPC UA Server publishes only those global variables to the OPC UA client in which the network publish attribute is *Publish Only*, *Output*, or *Input*. Note that system-defined variables cannot be published.

Variables that are published to OPC UA client

Variables that are not published to OPC UA client

Published variables
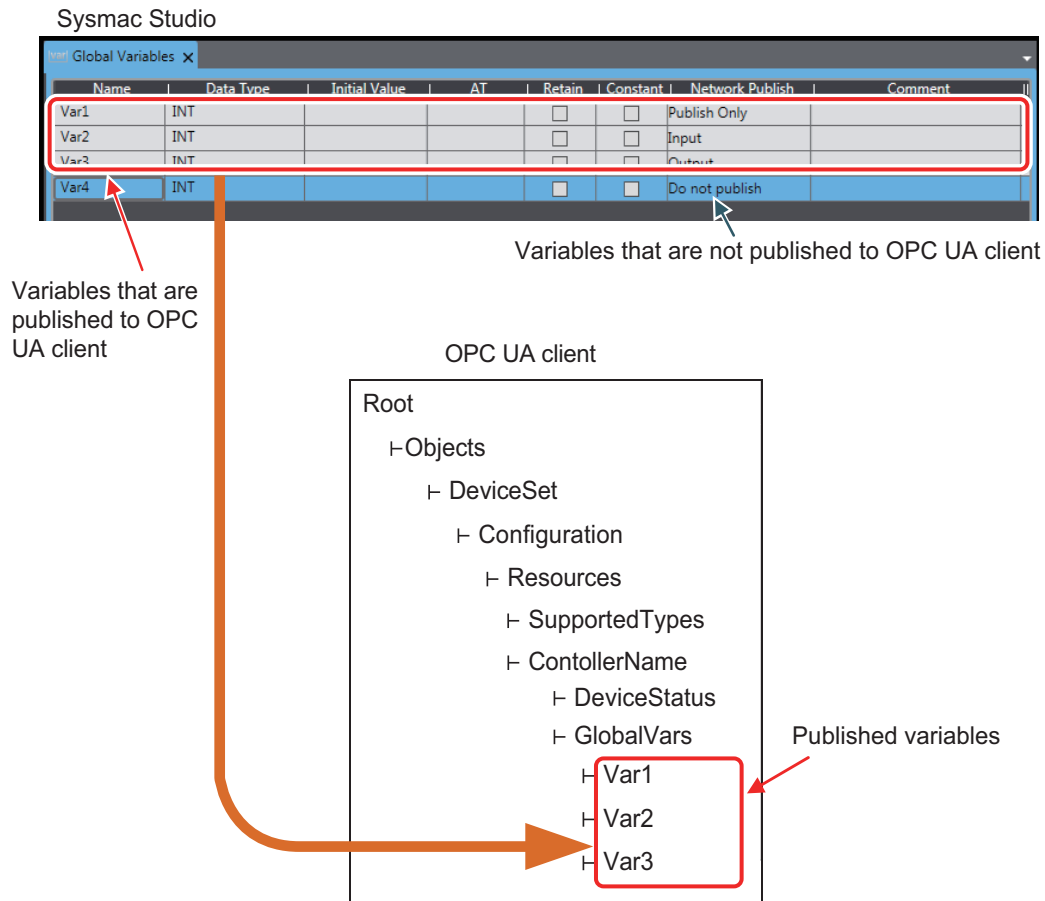
● **Settings of Global Variable Attributes**

Global variable attribute	Setting of the variable on the OPC UA Server
Name	Set to *DisplayName* and *BrowseName*.
Data type	Refer to *Data Type of Variables Published to the OPC UA Client* on page 6-6.
Initial value	---
AT specification	---
Retained	---
Constant	When this is set to *ON, AccessLevel* is set to *Readable* (Set to ReadOnly). When this is set to *OFF, AccessLevel* is set to *Readable, Writeable*.
Network Publish	*Do not publish* indicates that the variable is not published to the OPC UA client. *Publish Only*, *Output*, and *Input* indicate that the variable is published to the OPC UA client. Both reading and writing are possible. However, even if registered as a network-published variable, there are restrictions on variables to be published to OPC UA clients. For details, refer to *Restrictions on Publishing to the OPC UA Client* on page 6-7.
Comment	---

● **Data Type of Variables Published to the OPC UA Client**

- Basic data type

  The basic data types of the CPU Unit correspond to the OPC UA data types, as shown below.

Controller Data type	OPC UA Data type	Description of OPC UA data type
BOOL	Boolean	Value indicating two states represented by an 8-bit value
SINT	SByte	8-bit signed integer
USINT BYTE	Byte	8-bit unsigned integer
INT	Int16	16-bit signed integer
UINT WORD	UInt16	16-bit unsigned integer
DINT	Int32	32-bit signed integer
UDINT DWORD	UInt32	32-bit unsigned integer
LINT	Int64	64-bit signed integer
ULINT LWORD	UInt64	64-bit unsigned integer
REAL	Float	IEEE-754 single-precision floating-point value
TIME LREAL	Double	IEEE-754 double-precision floating-point value
STRING	String	UTF-8 string ending in NULL
DATE_AND_TIME DATE TIME_OF_DAY	DateTime	Date and time 64-bit data type. 100-ns time from January 01, 1601

Note Conforms to PLCopen OPC UA Information Model 1.00 Specifications.

- Array

  As for the arrays of the CPU Unit, as shown below, an entire array variable is published as one node.

  Example) ArrayVar1, ArrayVar2, and ArrayVar3 are array variables.
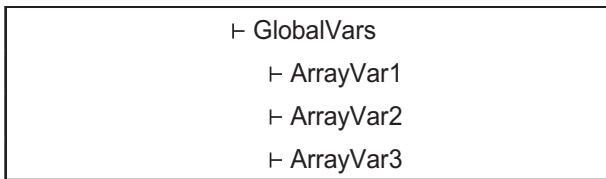
  ```
  ⊢ GlobalVars
      ⊢ ArrayVar1
      ⊢ ArrayVar2
      ⊢ ArrayVar3
  ```

  - Reading and writing between the OPC UA server and the OPC UA client is performed by the entire array variable.
  - Elements in the array can not be displayed, and reading/writing in element units is not supported.
  - One-dimensional or multi-dimensional arrays can be specified.

- Structure

  As for the structures of the CPU Unit, as shown below, an entire structure variable is published as one node.

  Example) StructVar1, StructVar2, and StructVar are structure data type variables
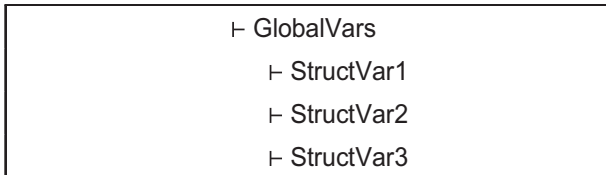
  ```
  ⊢ GlobalVars
      ⊢ StructVar1
      ⊢ StructVar2
      ⊢ StructVar3
  ```

  - Reading and writing between the OPC UA server and the OPC UA client is performed by the entire structure variable.
  - Member hierarchies in the structure can not be displayed, and reading/writing in member units is not supported.

- Enumerated type

  The enumerated type of the CPU Unit is published as the Int32 type.

  The enumerated type is handled as the DINT type in the CPU Unit.

Reading/Writing Variables from the OPC UA Client

The OPC UA client can perform reading/writing of the global variables of the CPU Unit serving as the OPC UA Server.

Whether the OPC UA Client can read/write global variables depends on the setting value of the *Network Publish* attribute, as shown below.

Setting value of Network Publish attribute of the global variable	Reading/writing variables from the OPC UA client
Do not publish	Both reading and writing are impossible.
Publish Only, *Input*, or *Output*	Both reading and writing are possible.

Restrictions on Publishing to the OPC UA Client

Not all variables registered as network-published variables are published to the OPC UA client.

The variables published to the OPC UA client are restricted based on the following restrictions.

If there are variables that are not published to the OPC UA client, you need to review the network-published variables to make sure that they remain within the following limits.

● **Restrictions**

The restrictions on public variables in the OPC UA Server are described below.

Scope of restriction	Item	Description
All network-published variables	Number of public variables	10,000 max.
	Number of value attributes of public variables [1]	10,000 max.
	Number of structure definitions that can be published [2]	100 max.
Individual network-published variable	Size of public variable	1,024 bytes max.
	Array specification	• The maximum number of elements per variable is 1,024. • Only elements whose element number starts with a *zero* can be published.
	Structure	• The maximum number of members per structure type variable [3] is 100. • The maximum number of hierarchies is three. • A multidimensional array specified structure [4] as well as a structure containing a multidimensional array as a member [5] cannot be published.
	Unions	• Cannot be published. • A structure containing union(s) as member(s) cannot be published.

*1. The number of value attributes is the sum total calculated as below:

Number of value attributes = (Number of basic data type variables) + (Number of array-specified elements) + (Number of values in the structure)

*2. Details of Number of structure definitions that can be published are as follows:

• Specify the number of definitions. Even if the same definition is used in multiple variables, the number of definitions is not counted up.
• If the data type of the members of the structure is also a structure, the number of members (that are structures) is also counted.
• If the data type of the members of the structure is either basic data type or array, the members are not counted.

*3. In the *Number of members per structure type variable*, if the data type of the members of the structure is also a structure, the number of subordinate members (that are structures) is not counted as the restrictions are applied.

*4. The *Multidimensional array specified structure* indicates a multidimensional array in which the elements are structures.

*5. The *Structure containing a multidimensional array as a member* indicates a structure containing (a) multidimensional array as member(s).

A variable that is not published to the OPC UA Server due to the above restrictions is not displayed in the OPC UA client even if it is registered as a network-published variable.

● **Method of Checking the CPU Unit**

When an address space is prepared in the OPC UA Server of the CPU Unit, the above restrictions are checked according to the procedures described below.

Step 1: The group of network-published variables is sorted in the ascending order of the character code UTF-16 of the variable name.
For example, sorting is done in the order of single-byte numbers (in the order of 0 to 9) -> single byte alphabets (in the order of A to Z) -> double-byte characters. Note that single-byte alphanumeric characters are not case sensitive.

Step 2: Based on the list of the variables sorted by the variable name, check the variables first in terms of the above restrictions set for all network-published variables, and then in terms of the restrictions set for individual. If they remain within the above restrictions set for all network-published variables as well as the ones set for individual, the variables will be published to OPC UA clients.

● **Registering the Check Results**

If, as a result of the above checks, variables that are not published to the OPC UA Server are found to exist, the check results are registered in the event log and the Execution Log for each restriction.

• The occurrence information of the unpublished variables is registered in the event log.

• In addition to the occurrence information, detailed information of each published variable is also registered in the Execution Log.

Item	Event log	Execution Log (Category name - Log code (position of log name))	
Number of public variables in all network-published variables	Too Many Public Variables (Event code: 35D30000 hex)	• Occurrence information: SERVER-0100 (The maximum number of variables that can be published has been exceeded) • Information about the number of public variables: SERVER-0110 (Number of OPC UA public variables)	Detailed information of each published variable: SERVER-0111 (Detailed information of OPC UA public variables)
Number of value attributes of public variables in all network-published variables	Too Many Public Value Attributes (Event code: 35D50000 hex)		
Number of structure definitions that can be published in all network-published variables	Too Many Structure Definitions (Event code: 35D60000 hex)		
Size of public variables of each network-published variable	Unsupported Data Type (Event code: 35D40000 hex)	• Occurrence information: SERVER-0101 (Variables containing an unsupported data type)	
Array specifications of each network-published variable			
Structures of each network-published variable			
Unions of each network-published variable			

• Both the event log and the Execution Log are registered when any of the following operations is performed:

   • When the power is turned ON or when the Controller is reset

   • During a download

   • During a restore operation

   • When a variable added through online editing is subject to the restrictions.

For details on the event log and the Execution Log, refer to *9-2 Troubleshooting* on page 9-7 and *7-1-5 Execution Log File Specifications* on page 7-5, respectively.

● **Method of Checking Variables Added through Online Editing**

For a variable added through online editing from the Sysmac Studio, the above check operation is performed for the added variable if any limit for all network-published variables has not been reached yet. If the added variable does not exceed any limit, the variable is published to the OPC UA client. If any limit item applied to all network published variables has been exceeded, the added variable is not published.

Note that if multiple network-published variables are simultaneously added through online editing, checking is performed according to the above sorting order only for the group of added variables (re-checking of all variables is not performed).

> **Precautions for Safe Use**
>
> Even if a global variable is set to Network Publish in the Sysmac Studio, the OPC UA client may not be able to refer to or read/write the variable in some cases depending on the limits sets on variables that can be published to the OPC UA client.
>
> Refer to the event log or Execution Log, and review which variables to be published to the network depending on the cause of occurrence.

7

Execution Log Functions

This section describes how to use the Execution Logs for tracing the operations of the OPC UA Server.

7-1   Execution Logs

This section provides an overview of the Operation Logs, operational procedures, settings and specifications for the Execution Logs.

7-1-1   Overview

The Execution Logs are used to trace operations on the CPU Unit of the OPC UA Server. They are saved to the SD Memory Card (sold separately) mounted in the CPU Unit.

The following can be checked with log codes and log names in the Execution Logs.

Refer to **Category Name**, **Log code**, **Log name**, *and **Details*** in the record formats of *7-1-6 Format of Records* on page 7-5 for details.

Meaning of category name	Meaning of log name	Description
OPC UA server	OPC UA Server started	Registered when the power turns on if the OPC UA Server Use Option is set to *Use*.
	Preparing of OPC UA Server started	Registered when the OPC UA server enters the *Preparing* state.
	OPC UA Server running	Registered when the OPC UA server enters the *Running* state.
	OPC UA Server shutdown completed	Registered when the OPC UA server enters the *Shutdown* state.
	OPC UA Server error	Registered when the OPC UA server enters the *Halt error* state.
	Maximum number of variables that can be published is exceeded	Registered when the maximum number of variables that can be published is exceeded among the global variables with the network publish attribute.
	Variable including unsupported data type	Registered for each variable when there are unsupported data types on the OPC UA server among the global variables with the network publish attribute.
	Number of OPC UA public variables	Registered the total number of variables that the OPC UA Server publishes to clients, when the address space is re-prepared or changed.
	Details of OPC UA public variables	Registered details of the variables that the OPC UA Server publishes to clients, when the address space is re-prepared or changed.
Authentication	Application authentication	Registered when application authentication processing completes (successful or failure).
	User authentication	Registered when user authentication processing completes (successful or failure).
	Security settings updated	Registered when the security settings are updated.

Meaning of category name	Meaning of log name	Description
Certificate	Server certificate updated	Registered when a server certificate is generated.
	Notice of expiration of server certificate	Registered only once when the number of days left until expiration is less than 30.
	Server certificate expired	Registered when the server certificate has expired.
	Server certificate mismatch	Registered when the IP address of the Server and the IP address of the Controller are different.
	Certificate added	Registered when the user adds a certificate in the CPU Unit by operating the Sysmac Studio.
	Certificate deleted	Registered when the user deletes a certificate in the CPU Unit by using the Sysmac Studio.
	Certificate moved	Registered when the user moves a certificate in the CPU Unit by using the Sysmac Studio.
	Certificate discarded	Registered when a certificate received from an OPC UA client is discarded without being saved because the number of certificates saved in the CPU Unit has reached the limit.
	Certificate Revocation List added	Registered when the user adds a Certificate Revocation List in the CPU Unit by operating the Sysmac Studio.
	Certificate Revocation List deleted	Registered when the user deleted a Certificate Revocation List in the CPU Unit by operating the Sysmac Studio.

The Execution Logs are recorded by setting Execution Log to Record from **Configurations and Setup** - **OPC UA Settings** - **OPC UA Server Settings** in Multiview Explorer of the Sysmac Studio.

When the Execution Logs are recorded, the Execution Log files are constantly saved to the SD Memory Card mounted in the CPU Unit while the OPC UA Server is running.

The Execution Logs are temporarily recorded in the internal buffer (volatile memory) of the CPU Unit and then saved to the SD Memory Card. While the SD Memory Card is being replaced, the execution logs are kept in the internal buffer (volatile memory) of the CPU Unit. When you insert an SD Memory Card, the Execution Logs temporarily stored in the internal buffer are then saved automatically to the SD Memory Card. Refer to *7-4-3 Execution Log Operation when Replacing the SD Memory Card* on page 7-20 for details.

You can check the contents of the Execution Logs in the **Execution Log** Tab Page of the Operation Log Window in the Sysmac Studio.

Precautions for Correct Use

When you use Execution Logs, be sure to insert an SD Memory Card into the CPU Unit.

The Execution Logs are temporarily recorded in the internal buffer of the CPU Unit and then saved to the SD Memory Card. If no SD Memory Card is mounted at power-OFF or shutdown processing of the CPU Unit, the Execution Logs recorded in the internal buffer will be lost. In that case, an *Execution Log Save Failed* event (event code: 15000000 hex) will occur.

7-1 Execution Logs

7

7-1-1 Overview

7-1-2   How to Use the Execution Log

Use the Execution Logs according to the following procedure.

Step	Reference
STEP1 Set **Execution Log**.	*7-1-3 Setting the Execution Log* on page 7-4
STEP2 Insert the SD Memory Card into the CPU Unit.	*NJ-series CPU Unit Hardware User's Manual* (Cat No. W500) *NX-series NX102 CPU Unit Hardware User's Manual* (Cat. No. W593)
STEP3 Start the OPC UA Server.	*4-1 Starting or Stopping the OPC UA Server* on page 4-2
STEP4 Check the Execution Logs.	*7-2 Checking the Execution Log* on page 7-13

7-1-3   Setting the Execution Log

Set the following settings in **OPC UA Server Settings** from **Configurations and Setup - OPC UA Settings** in Multiview Explorer of the Sysmac Studio.

Setting	Description	Value
Execution Log	Set whether or not to record Execution Logs.	• Do not record (Default) • Record
Number of files	Set the maximum number of Execution Log files to be stored in the directory. When the maximum number of files is reached, the oldest file is deleted and a new file is created.	2 to 100 (Default: 24) Unit: files
Number of records	Set the number of records (logs) per Execution Log file. When the set number of records is reached, a file with the next serial number is created and then saved.	100 to 65,536 (Default: 12,000) Unit: records/file

7-1-4   Checking the Execution Log

Refer to *7-2 Checking the Execution Log* on page 7-13 to check Execution Logs.

7-1-5   Execution Log File Specifications

This section describes the specifications of Execution Log files.

- Each Execution Log file is composed of multiple records.
- Each record is expressed in one line.
- The maximum number of records to be contained in each Execution Log file is set in the Sysmac Studio.
- The size of each record is 256 bytes max.
- The following table shows file names and types.

File name	File type	Remarks
OPCUA_ExecutionLog.log	Latest log file in the log	---
OPCUA_ExecutionLog_YYYYMMDDHHmmssSSS.log Note: YYYY: Year, MM: Month, DD: Day HH; Hour, mm: minute, ss: Second, SSS: Millisecond If each digit is not used, the space if filled with a 0.	Log file in which maximum number of records reached	Example: OPCUA_Execution-Log_20170724220915040.log
OPCUA_ExecutionLog.fjc	System files	Log control file

Note The system time of the CPU Unit is used for the time information included in the file name.

- The files are stored in the following directories (in the SD Memory Card).

-Log files:

/packages/OPCUA_Server/ExecutionLog/

-Log control file:

/packages/OPCUA_Server/System/

Precautions for Correct Use

Do not delete the following files in the SD Memory Card.
- OPCUA_ExecutionLog.log (latest log file)
- OPCUA_ExecutionLog.fjc (log control file)

If they are deleted, the log files will not be saved correctly; for example, the Execution Log data will be lost.

7-1-6   Format of Records

The following is the format of records.
Each record is expressed in one line and composed of multiple parameters. The parameters are separated from each other by a tab.

Serial number<tab>**Date**<tab>**Time**<tab>**Millisecond**<tab>**Category name**<tab>**Log code**<tab>**Log name**<tab>**Details**CR+LF

Parameter	Size	Description
Serial number	1 to 5 bytes	0 to 65,535 When 65,535 is exceeded, this value returns to 0. The serial number is given across multiple files. (Even if a new file is created, the serial number is not reset to 0.)
Date [1]	10 bytes (Fixed)	Displays the year, month, and date when the log was recorded. [1] YYYY-MM-DD Example: 2017-06-23

Parameter	Size	Description
Time[1]	8 bytes (Fixed)	Displays hours, minutes, and seconds when the log was recorded. [1] hh:mm:ss Example: 15:33:45
Millisecond[1]	3 bytes (Fixed)	Displays a 3-digit decimal integer (000 to 999) for the millisecond of the time when the log was recorded.[1] Example: 10 ms: 010 623 ms: 623
Category name[2]	16 bytes max. (Variable)	Displays the category.
Log code	4 bytes (Fixed)	Displays a 4-digit decimal code that is a unique identification code in the category.
Log name	32 bytes max. (Variable)	Displays a name that indicates the contents of the log.
Details	168 bytes max. (Variable)	Displays the details of the Execution Log. In the **Details** parameter, information items are separated from each other by a tab. The number of information items in the **Details** parameter is variable. The contents differ according to the category.
CR+LF	2 bytes	Displays the end of the record.

[1] The system time of the CPU Unit is used for **Date**, **Time**, and **Millisecond**.

[2] **Category name**:

Category name	Meaning of category name	Description	Main usage
SERVER	OPC UA server	Record the state transition (operating state) of the OPC UA Server.	Troubleshooting at a start-up of the device: When, for example, an OPC UA client is not able to connect to the OPC UA Server (to identify the primary cause)
AUTH	Authentication	Record the execution results of application authentication and user authentication.	Troubleshooting at a start-up of the device: When, for example, an OPC UA client is not able to connect to the OPC UA Server
CERT	Certificate	Record changes to the server certificate, client certificates, CA certificates, and certificate revocation list retained by the OPC UA Server.	Troubleshooting the device is running. When, for example, an OPC UA client is not able to connect to the OPC UA Server, though it was able to before

Category name, **Log code**, **Log name**, and **Details** are as follows:

Category name	Log code (Decimal)	Log name	Meaning of log name	Details
SERVER	0001	Start	OPC UA Server started	None
	0004	Prepare	Preparing of address space of OPC UA Server started	None
	0005	Run	OPC UA Server running	None
	0006	Shutdown	OPC UA Server shutdown completed	None

Category name	Log code (Decimal)	Log name	Meaning of log name	Details
SERVER (continued)	0007	HaltError	OPC UA Server error	Error message Note Refer to [1] below this table for a list of the error messages.
	0100	MaxVariables	Maximum number of variables that can be published is exceeded	Format: **Details 1** Details 1: • MaxVariables: The number of variables exceeded the upper limit. • MaxValues: The number of value attributes of a variable exceeded the upper limit. • MaxDataTypes: The number of structure definitions exceeded the upper limit.

	0101	InvalidDataType	Variable including unsupported data type	Format:
				    Details 1<tab>**Details 2**<tab>**Details 3**
				
				Details 1:
				• Variable name: Up to 60 bytes is displayed for the name of each variable that cannot be published.
				  Note: In the case of multi-byte characters, the last character may not be displayed correctly.
				Details 2:
				• MultiDimensionalArray:
				  - Structure with multidimensional array specified
				  - Structure containing member with multidimensional array
				• Union: Union is included
				• SubscriptOfArrary:
				  - Array not beginning with the starting number of 0
				  - Member of structure containing array not beginning with the starting number of 0
				• NestedStructre: Number of hierarchy levels of structure exceeds upper limit
				• MaxMembers: Number of members of structure exceeds upper limit
				• MaxSize: Variable size exceeds upper limit
				• MaxArrayElements: Number of elements of array variable exceeds upper limit
				Details 3:
				• Variable size: When Details 2 is *MaxSize*, the variable size is recorded (decimal number, unit is bytes). Otherwise, there is no Details 3.
				
				Note If one variable includes more than one of the above factors, only the first detected factor is recorded.

7-1 Execution Logs

7

7-1-6 Format of Records

Category name	Log code (Decimal)	Log name	Meaning of log name	Details
SERVER (continued)	0110	NumOf-Vari-ables	Number of OPC UA public variables	Format: Variables=xxxx, Values=xxxx, DataTypes=xxxx • Variables: Total number of OPC UA public variables • Values: Total number of value attributes of OPC UA public variables • DataTypes: Total number of structure definitions of OPC UA public variables
	0111	Pub-lished-Variable	Details of OPC UA public variables	Format: **VarName**<tab>**VarSize**<tab>**NumOfVal-ues**<tab>**NumOfMembers** • VarName: Variable name published to OPC UA clients (Up to 60 bytes to be displayed) Note In the case of multi-byte characters, the last character may not be displayed correctly. • VarSize: Variable size (decimal number, unit is byte) • NumOfValues: Number of value attributes of variable (decimal, unit is attribute but is not recorded) • NumOfMembers: When the data type of the variable is structure, number of members of the structure (decimal, unit is member but is not recorded) Note When the data type of the variable is not structure, this is *0* (zero).

AUTH	0001	Applica-tion	Application authen-tication	- When connected
				• In normal status
				  Format:
				OPEN<tab>**SessionID**<tab>**IP address of connecting cli-ent**<tab>**Host information of client certificate**
				• In error status
				  Format:
				  ERROR<tab>**Error message**
				Note Refer to [2] below this table for a list of the error messages.
				- When disconnected
				  Format:
				  CLOSE<tab>**SessionID**

	0002	User	User authentication	• In normal status:
				  Format: Success<tab>**SessionID**<tab>**User name**
				• In error status
				  Format: ERROR<tab>User name<tab>**Error message**
				Note Refer to [3] below this table for a list of the error messages.

	0100	Update	Security settings updated	None

Cate-gory name	Log code (Deci-mal)	Log name	Meaning of log name	Details	
CERT	0001	Update_Sever	Server certificate updated	Format: **Distinguished name (common name) of certifi-cate**<tab>**Expiration date of certificate** • Distinguished name (common name) of certificate: Up to 60 bytes maximum from the beginning is output. • Expiration date of certificate: YYYY-MM-DDThh:mm:ssZ (The expiration date of the certificate is expressed in UTC. When it is recorded in the Details, it is recorded in UTC as well.)	
	0002	Notify_-Server	Notice of expiration of server certificate		
	0003	Expired_Server	Server certificate expired		
	0004	Mis-match_Host	Server certificate mismatch		

	0100	Add	Certificate added	Format:
				Distinguished name (com-mon name) of certifi-cate<tab>**Expiration date of certificate**<tab>**Details 1**
				
				• Distinguished name (com-mon name) of certificate: Up to 60 bytes maximum from the beginning is out-put.
				• Expiration date of certifi-cate: YYYY-MM-DDThh:mm:ssZ
				  (The expiration date of the certificate is expressed in UTC. When it is recorded in the details, it is recorded in UTC.)
				• Details 1
				  Refer to the right.
					Details 1:
					Type of certifi-cate<tab>**Store location**
					• Type of certificate: CLI-ENT: Client certificate
					• Store location: TRUSTED: Trusted certificate list
					ISSUER: CA certificate list

	0101	Delete	Certificate deleted		Details 1: **Type of certifi-cate**<tab>**Store location** • Type of certificate: CLI-ENT: Client certificate • Store location: TRUSTED: Trusted certificate list ISSUER: CA certificate list REJECTED: Rejected certifi-cate list
	0102	Move	Certificate moved		Details 1: **Type of certifi-cate**<tab>**Store loca-tion**->**Store location** • Type of certificate: CLI-ENT: Client certificate • **Store location**->**Store location**: REJECTED ->TRUSTED (Fixed)

7-1 Execution Logs

7

7-1-6 Format of Records

Category name	Log code (Decimal)	Log name	Meaning of log name	Details	
CERT (continued)	0103	Discard	Certificate discarded		Details 1: **Type of certificate**<tab>**Store location** • Type of certificate: CLIENT: Client certificate • Store location: REJECTED: Rejected certificate list (Fixed) Note In the following cases, the *Certificate discarded* Execution Log is not recorded (it is recorded in the event log) • Memory all cleared • Unsupported OPC UA project downloaded • Unsupported OPC UA project restored
	0200	Add_Crl	Certificate Revocation List added	Format: **File name**<tab>**Distinguished name (common name) of CA**<tab>**Expiration date of revocation list**<tab>**Type of revocation list**<tab>**Store location** • File name: Up to 65 bytes maximum from the beginning is output. • Distinguished name (common name) of CA: Up to 60 bytes maximum from the beginning is output. • Expiration date of revocation list: YYYY-MM-DDThh:mm:ssZ • Type of revocation list: CLIENT: Client certificate revocation list • Store location: TRUSTED: Certificate Trust List ISSUER: Root certificate / intermediate certificate list Note: Revocation list deleted only: In the following cases, the *Revocation list deleted* Execution Log is not recorded (it is recorded in the event log) • Memory all cleared • Unsupported OPC UA project downloaded • Unsupported OPC UA project restored	
	0201	Delete_Crl	Certificate Revocation List deleted		

*1 HaltError (OPC UA Server Error) Error Message List

Error message	Meaning
Configuration Error	Reading of the OPC UA Settings file failed.
	Cause There is no OPC UA Settings file. Or the file is damaged.
	Measure Download the OPC UA Settings file.
Server Start Error	Preparing of address space failed.
	Cause TCP port number is duplicated.
	Measure Change the TCP port number and download the settings.
OPC UA System Error	A fatal error was detected.
	Cause An error occurred in the software.
	Measure Turn the power OFF and then back on.

*2 Application (Application Authentication) Error Message List

Error message	Meaning
BadCertificateIssuerRev-ocationUnknown	Whether the client certificate can be trusted is unknown because the CA certificate revocation list cannot be accessed.
BadCertificateInvalid	The certificate signature is invalid. The certificate may have been tampered with.
BadCertificateUntrusted	The certificate was issued by an untrusted CA.
BadCertificateRevoked	The certificate was issued by a CA but it has been revoked.
BadTooManySessions	The number of sessions is excessive.

*3 User (User Authentication) Error Message List

Error message	Meaning
BadUserAccessDenied	The user name or password is incorrect.
BadIdentityTokenRe-jected	An anonymous login was requested when anonymous logins are prohibited.

7-1-7 Examples of Records in Execution Log File

The following shows examples of records in an Execution Log file.

- Example of when the power is turned ON and the OPC UA Server is started.

```
0   2017-10-17   14:52:50   747   SERVER   0001   Start
1   2017-10-17   14:52:50   749   SERVER   0004   Prepaire
2   2017-10-17   14:52:50   877   SERVER   0111   PublishedVariable   Var1   2Byte    1   0
3   2017-10-17   14:52:50   878   SERVER   0111   PublishedVariable   Var2   6Byte    3   3
4   2017-10-17   14:52:50   878   SERVER   0111   PublishedVariable   Var3   2Byte    1   0
5   2017-10-17   14:52:50   878   SERVER   0111   PublishedVariable   Var4   10Byte   5   0
6   2017-10-17   14:52:50   878   SERVER   0110   NumOfVariables      Variables=4, Values=10, Data-
                                                                     Types=1
7   2017-10-17   14:52:50   878   SERVER   0005   Run
```

- Example of when an error occurs after a connection request from a client

```
8   2017-10-17   14:54:11   822   AUTH   0001   Application   ERRORBadCertificateUn-
                                                              trusted
9   2017-10-17   14:54:11   844   CERT   0103   Discard       UaClient_1@SamplePC
2022-10-03T08:19:54.000ZCLIENTREJECTED
```

- Example of when the user moved a client certificate from the Rejected Certificate List to the Trusted Certificate List:

```
10   2017-10-17   14:54:28   929   CERT   0102   Move   UaClient_1@SamplePC
2022-10-03T08:19:54.000ZCLIENTREJECTED->TRUSTED
```

• Example of when user authentication and application authentication end successfully, following a reconnection request from a client.

11   2017-10-17   14:54:39   250   AUTH   0002   User   SUCCESS0x2ADA356B
Anonymous
12   2017-10-17   14:54:39   251   AUTH   0001   Application   OPEN 0x2ADA356B
192.168.255.2UaClient_1@SamplePC

• Example of when the user shut down the OPC UA Server:

60   2017-10-17   16:05:45   323   SERVER0006 Shutdown

7-2   Checking the Execution Log

This section describes how to check Operation Logs stored in the SD Memory Card mounted in the CPU Unit.

7-2-1   How to Check the Execution Log

You can use any of the following methods to check the Execution Log.

- Checking logs in the Operation Log Window in the Sysmac Studio
- Checking logs with the SD Memory Card
- Checking logs by transferring data using FTP client software

Precautions for Correct Use

Execution Log file is encoded in UTF-8.

7-2-2   Checking Logs in the Operation Log Window in the Sysmac Studio

You can use the following method to check the Execution Logs stored in the SD Memory Card from the Operation Log Window of the Sysmac Studio.

The Operation Log Window is available for operation only when the CPU Unit has an SD Memory Card mounted and is connected online.

1   Go online with the CPU Unit from the Sysmac Studio, right-click **OPC UA Settings** under **Configurations and Setup** in the Multiview Explorer, and select **Show Operation Logs**.
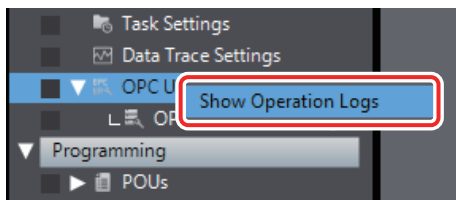
The following Operation Log Window is displayed.
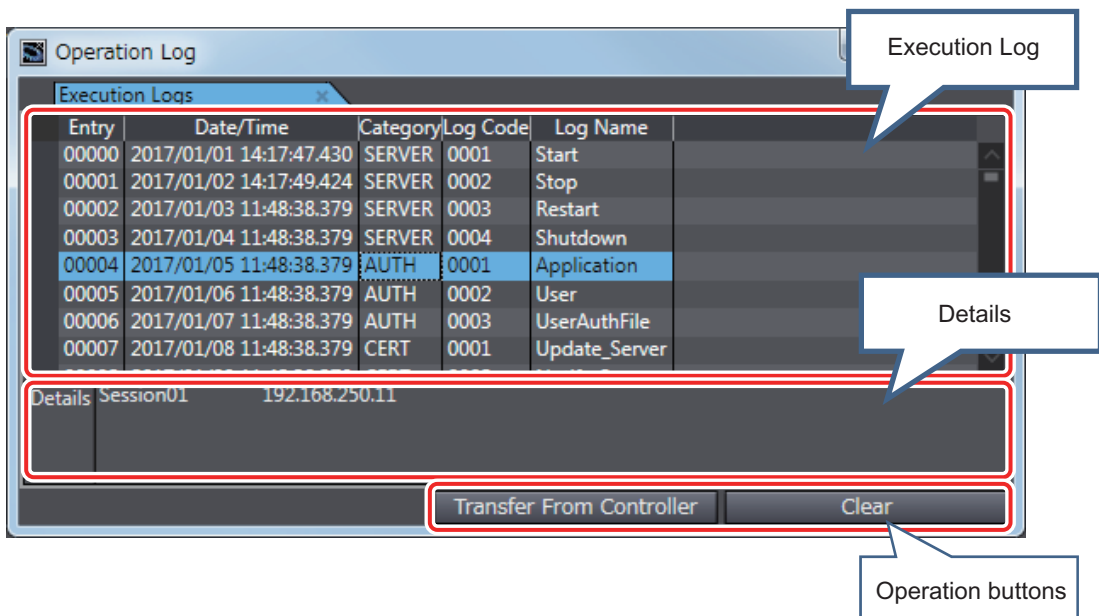
The following information is displayed.

Category	Item	Description
Execution Logs		Displays a list of log records.
		Displays the Entry, Date/Time, Category, Log Code, Operation and Log Name columns.
		The default data is displayed in the ascending order of entries. Clicking each column header sorts the list according to the name of the corresponding item. Each click switches between ascending and descending order.
	Entry	Displays a serial number.
	Date/Time	Displays a date and time in the *Year/Month/Day/Hour:Minute:Second.ms* format.
	Category	Displays a category.
	Log Code	Displays a log code.
	Log Name	Displays a log name.
Details		Displays the details of the log.
Operation buttons	**Transfer From Controller** Button	Acquires the log files. Refer to *Acquiring Log Files* on page 7-14 below for details.
	Clear Button	Clears the log files. Refer to *Clearing the Execution Logs* on page 7-15 below for details.

● **Acquiring Log Files**

Acquire the log files in the SD Memory Card inserted in the CPU Unit

1 Click the **Transfer From Controller** Button to acquire the log files from the Controller and display a list of the log files in the following **Operation Log** Dialog Box.
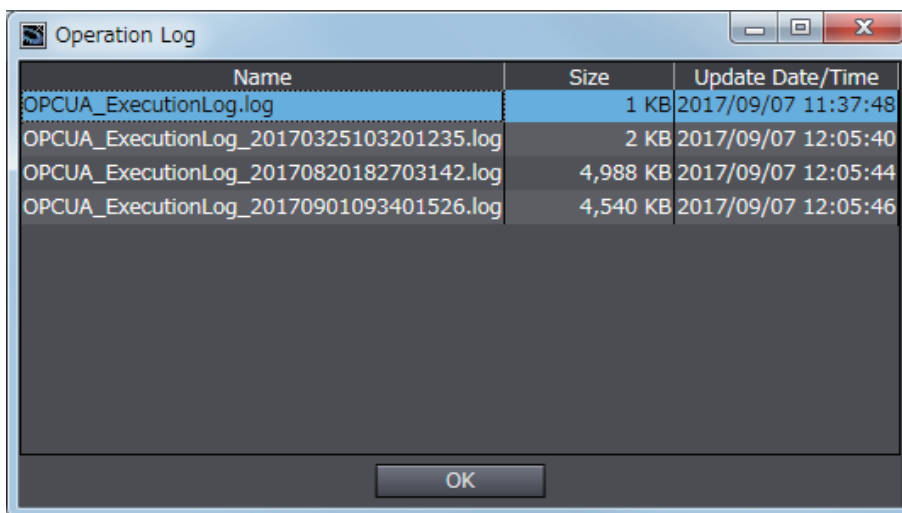
2 Select a log file to display and click the **OK** Button. The log file is uploaded.

Note1. If a log file of the same name exists on the computer, the following message is displayed.
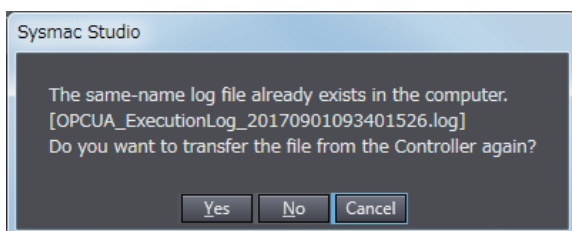
Select from the following options.
Yes: Acquires the specified file from the Controller and then displays it.
No: Displays the contents of the file that already exists on the computer without acquiring the selected file from the Controller.
Cancel: The file list is displayed again.

Note2. If the selected log file is bigger than 10 MB, the following message is displayed.
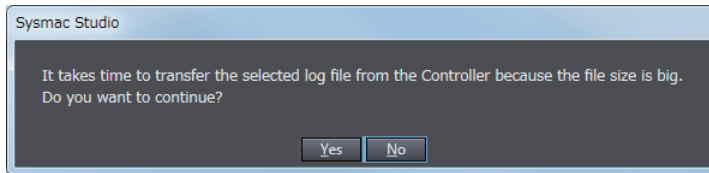
Select from the following options.
Yes: Acquires the specified file from the Controller and displays it.
No: Goes back to the list again.

● **Clearing the Execution Logs**

Clear the log files in the SD Memory Card inserted in the CPU Unit.

1 Click the **Clear** Button. The following confirmation message is displayed.
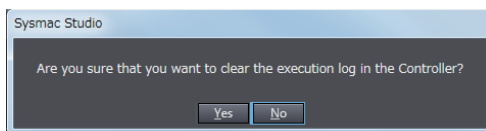
2 Click the **Yes** Button to clear the log files in the SD Memory Card inserted in the CPU Unit.

● **Failure of Execution Log Saving**

Saving of the Execution Logs will fail in the following cases.
• The OPC UA Server is started while an SD Memory Card is not mounted.
• The OPC UA Server is started while an SD Memory Card is mounted but the type or format is invalid, write protection is set, there is insufficient space, or a failure has occurred.

When this happens, an *Execution Log Save Failed* event log (event code: 15000000 hex) will be registered.

7-2-3   Checking Logs with the SD Memory Card

Remove the SD Memory Card from the CPU Unit and insert it into a computer. Then, check the contents of the logs in Microsoft Excel or a text editor or any other application.

For the conditions for saving execution log files to the SD Memory Card and the method of replacing the SD Memory Card, refer to *7-4 SD Memory Card Operations* on page 7-19.

7-2-4   Checking Logs by Using FTP Client Software

You can transfer the log files using the FTP Server function via the Ethernet network and check the contents in Microsoft Excel or a text editor or any other application.

Use the following procedure.

Use the FTP server function of the built-in EtherNet/IP port.

1   Select the *Use* Option for the **FTP server** in the **FTP Settings**, which is displayed following **Built-in EtherNet/IP Port Settings** - **Configurations and Setup** in the Multiview Explorer of the Sysmac Studio.

For details on how to make the settings, refer to the *NJ/NX-series CPU Unit Built-in EtherNet/IP Port User's Manual* (Cat. No. W506).

2   Using the FTP client software, input the FTP login name and password that you set in the Built-in EtherNet/IP Port Settings to log into the CPU Unit.

3   Move to the folder where the execution log files are stored.

cd \MEMCARD1\packages\OPCUA_Server\ExecutionLog\

4   Acquire the Execution Log files.

For example, to acquire multiple log files to which writing has been completed, specify a wild card with the mget command as shown below.

mget OPCUA_ExecutionLog*.log

5   Disconnect the FTP client software from the CPU Unit.

6   Open the acquired Execution Log files in Microsoft Excel or a text editor or any other application to check the contents.

7-3 OPC UA Server Shutdown Function

This section describes the shutdown function of the OPC UA Server for preventing Execution Log data loss.

Refer to *4-2 Checking the Status of the OPC UA Server* on page 4-5 for details on the operating statuses of the OPC UA Server.

7-3-1 Overview

The OPC UA Server shutdown function (hereinafter called *shutdown function*) is used to shut down the OPC UA Server after saving the execution files to the SD Memory Card.

Execute the shutdown function before turning OFF the power supply to the CPU Unit. You can prevent Execution Log data loss by executing the shutdown function.

Precautions for Correct Use

If the power supply to the CPU Unit is turned OFF without executing the shutdown function while the OPC UA Server is running, the contents of the Execution Logs cannot be guaranteed. The Execution Log files may be corrupted or the data may be lost.

Additional Information

To prevent data loss due to an unexpected power interruption, we recommend that you take measures against power interruptions such as the installation of an uninterruptible power supply system.

7-3-2 Shutdown System

The following figure shows the shutdown system.
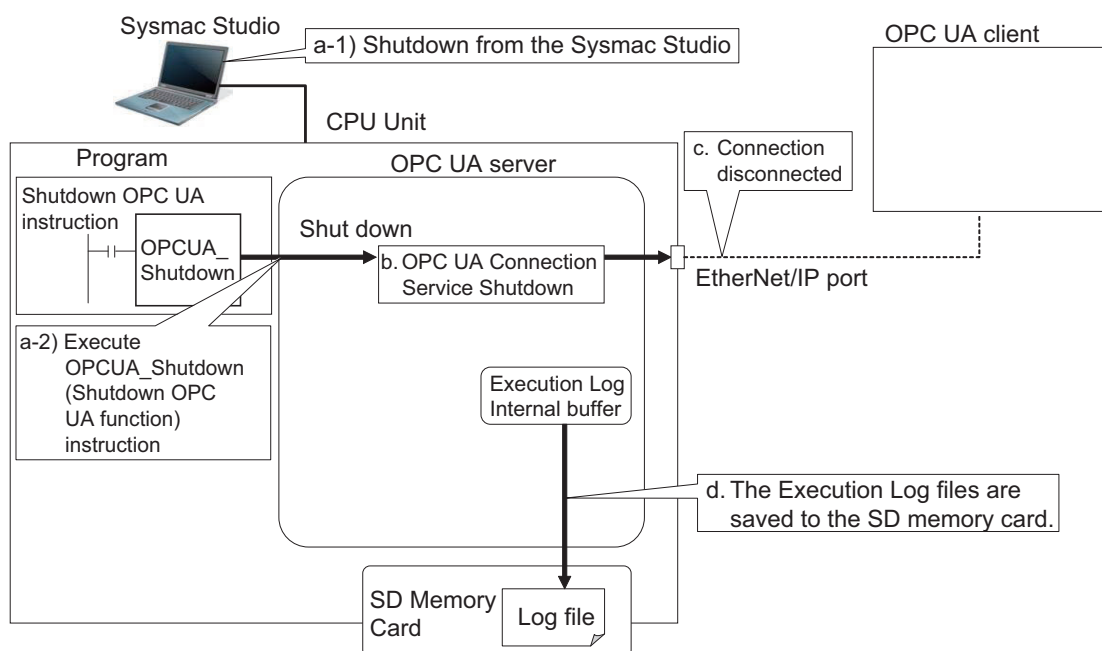
a) The OPC UA Server is shut down by one of the followings:
   (1) Using the Sysmac Studio
   Or
   (2) Executing the OPCUA_Shutdown (Shutdown OPC UA Function) instruction

b) The OPC UA Server shuts down.

c) The connection is closed.

d) The Execution Log files are saved to the SD memory card.

7-3-3   How to Execute the Shutdown Function

You can execute the shutdown function by performing either of the following operations.
- Sysmac Studio operation
- Instruction execution

Sysmac Studio Operation

1   Right-click **OPC UA Server Settings** from **OPC UA Settings** under **Configurations and Setup** in the Multiview Explorer of the Sysmac Studio and select **Server Status** while connecting online with an NJ/NX-series CPU Unit. The **Service Status** Tab Page is displayed.

2   Click the **Server shutdown** Button.
For details on the procedure, refer to the *Shutting Down the Server Function* on page 4-6.

Additional Information

When you execute the Reset Controller operation on the Sysmac Studio, the OPC UA server shutdown function is automatically executed before resetting the Controller.

Instruction Execution

Execute the OPCUA_Shutdown (Shutdown OPC UA Function) instruction.

Refer to *A-2 OPC UA Instruction* on page A-7 for details on the OPC UA instruction.

7-3-4   How to Check the Shutdown of the OPC UA Server

Confirm that the OPC UA Server has been shut down by the following method before turning OFF the power supply to the CPU Unit.
- Checking with OPC UA Server Status of the Sysmac Studio

  Confirm that the Server operating status in **Operation Information** is *Shutdown* in the **Server Status** Tab Page.
- Checking by executing an instruction

  For details of the procedure, refer to *4-2-1 Checking Based on OPC UA Server Status of the Sysmac Studio* on page 4-5.

  Confirm that the *Done* output variable of the OPCUA_Shutdown (Shutdown OPC UA Function) instruction is TRUE.

  Refer to *A-2 OPC UA Instruction* on page A-7 for details on the OPC UA instruction.

7-4   SD Memory Card Operations

In the OPC UA Server, the SD Memory Card mounted in the CPU Unit is used for the Execution Log function.

The Execution Log files are stored in the SD Memory Card.

This section describes how to save the Execution Log files in the SD Memory Card and precautions for replacing the SD Memory Card.

Refer to the *NJ/NX-series CPU Unit Software User's Manual* (W501) for details on the SD Memory Card functions.

7-4-1   Conditions for Saving Execution Log Files to the SD Memory Card

Execution Log files are saved to the SD Memory Card under the following condition.

Operation to use the function	Conditions for saving log files on SD Memory Card
Set **Execution Log** to **Record** in **OPC UA Server Settings** of the Sysmac Studio.	Constantly saved while the OPC UA Server is running [1].

*1   If the power supply to the CPU Unit is turned on while no SD Memory Card is mounted in the CPU Unit, an *Execution Log Save Failed* event (event code: 15000000 hex) is registered in the event log when an Execution Log is saved. Recording of the Execution Logs starts when an SD Memory Card is inserted into the CPU Unit.

Even while the Server operating status of the OPC UA Server is *preparing* or *running*, recording of the Execution Log files will just start at the point of time when an SD Memory Card is inserted.

7-4-2   Directories Used for the OPC UA Server

The OPC UA Server uses the directories under packages/OPCUA_Server in the SD Memory Card as shown in the following table.

Directory	Description
/packages/OPCUA_Server/ExecutionLog	Contains the Execution Log files.
/packages/OPCUA_Server/System	Contains the system files (log control file).

Precautions for Correct Use

Do not delete the following files in the SD Memory Card.

- OPCUA_ExecutionLog.log (latest log file)
- OPCUA_ExecutionLog.fjc (log control file)

If they are deleted, the log files will not be saved correctly; for example, the Execution Log data will be lost.

7-4-3   Execution Log Operation when Replacing the SD Memory Card

This section describes the Execution Log operation when the SD Memory Card is replaced while the OPC UA Server is running.

Status during SD Memory Card Replacement		
When the SD Memory Card power switch is pressed	When no SD Memory Card is mounted	When an SD Memory Card is inserted
Stopped. If Execution Logs are contained in the internal buffer of the CPU Unit, they are recorded in the SD Memory Card.	Execution logs are not recorded.	The Execution Logs that were temporarily saved in the internal buffer are automatically recorded in the SD Memory Card.

7-4-4   Approximate Work Time for SD Memory Card Replacement

If you replace the SD Memory Card while the OPC UA Service is running, replace the SD Memory Card within the following time frames, depending on the interval at which the Execution Log is recorded.

● Approximate Time for Replacement Work

Examples of Execution Log recording intervals		
50-ms interval	100-ms interval	500-ms interval
30 seconds	60 seconds	300 seconds (5 minutes)

Precautions for Correct Use

Please note the following for replacing the SD Memory Card.

- When a project is downloaded from the Sysmac Studio and when the OPC UA Server is being prepared again, a large number of Execution Logs are written to the internal buffer. Therefore, do not replace the SD Memory Card for approximately five minutes after the download or the OPC UA Server preparation. If it is replaced before five minutes pass, the Execution Logs recorded in the internal buffer may be lost.
- Use a formatted SD Memory Card when replacing the SD Memory Card.
- When you replace the SD Memory Card while Execution Logs are being recorded, press the SD Memory Card power switch and insert a new SD Memory Card within the corresponding approximate time for replacement work after the SD PWR indicator turns off.

  If it takes longer than the corresponding approximate time for replacement work, the Execution Logs recorded in the internal buffer may be lost.

  If the internal buffer space becomes full before inserting the SD Memory Card, an *Execution Log Save Failed* event (event code: 15000000 hex) is registered in the event log.

7-4-5   Replacement Timing of SD Memory Card

● How to Know the Replacement Timing of the SD Memory Card

You can know the replacement timing of the SD Memory Card by checking the *SD Memory Card Life Exceeded* Event or the SD Memory Card Life Warning Flag (*_Card1Deteriorated* system-defined variable).

8

Other Functions

This section describes other functions of the OPC UA Server.

8

8-1   The Sysmac Studio Operation Authority Verification Related to the OPC UA Server

This section describes the Sysmac Studio operation authority verification related to the OPC UA Server.

This function is used to restrict online operations on the CPU Unit via the Sysmac Studio based on the granted authority.

Refer to the *NJ/NX-series CPU Unit Software User's Manual* (Cat. No. W501) and the *Sysmac Studio Version 1 Operation Manual* (Cat. No. W504) for the details and operating procedure of the operation authority verification function.

The following table indicates online operations related to the OPC UA Server based on the authority level.

OP: Operation possible, NP: Operation not possible

Function		Administrator	Designer	Maintainer	Operator	Observer	Reference
Server certificate	Display and update	OP	OP	OP	OP	NP	*3-2-5 Setting and Displaying the Certificate on page 3-9*
	Export	OP	NP	NP	NP	NP	
	Regenerate	OP	NP	NP	NP	NP	
Client authentication	Display and update	OP	OP	OP	OP	NP	
	Add certificate	OP	NP	NP	NP	NP	
	Delete certificate	OP	NP	NP	NP	NP	
	Move certificate	OP	NP	NP	NP	NP	
	View certificate details	OP	OP	OP	OP	NP	
	Add certificate revocation list	OP	NP	NP	NP	NP	*A-3 When CA-signed Client Certificates Supported* on page A-11
	Delete Certificate Revocation List	OP	NP	NP	NP	NP	
	View Certificate Revocation List details	OP	OP	OP	OP	NP	
Issuer authentication	Display and update	OP	OP	OP	OP	NP	*A-3 When CA-signed Client Certificates Supported* on page A-11
	Add certificate	OP	NP	NP	NP	NP	
	Delete certificate	OP	NP	NP	NP	NP	
	Move certificate	OP	NP	NP	NP	NP	
	View certificate details	OP	OP	OP	OP	NP	
	Add Certificate Revocation List	OP	NP	NP	NP	NP	
	Delete Certificate Revocation List	OP	NP	NP	NP	NP	
	View Certificate Revocation List details	OP	OP	OP	OP	NP	

Function		Admin-istrator	Design-er	Main-tainer	Opera-tor	Observ-er	Reference
Security settings (user authentica-tion settings, anonymous login, and security pol-icy)	Display and edit	OP	OP	OP	OP	NP	*3-2-6 Security Set-tings* on page 3-20
	Transfer security settings	OP	NP	NP	NP	NP	
Service status	Display and update	OP	OP	OP	OP	NP	*4-2-1 Checking Based on OPC UA Server Status of the Sysmac Studio* on page 4-5
	Shut down server	OP	OP	NP	NP	NP	
Execution Logs	Display	OP	OP	OP	OP	NP	*Section 7 Execu-tion Log Functions*
	Clear	OP	OP	OP	NP	NP	

8-2   Backup and Restore Functions Related to the OPC UA Server

This section describes the functions for backing up and restoring data in the NJ/NX-series CPU Unit that are related to the OPC UA Server.

There are four types of features for backup and restoration. Refer to the *NJ/NX-series CPU Unit Software User's Manual* (Cat. No. W501) for details on each function.

Function	Description	Backup function	Restore function
SD Memory Card backups	This function allows you to save various settings data in the NJ/NX-series CPU Unit to the SD Memory Card and restore the settings data in the CPU Unit by performing an operation on the CPU Unit.	Available	Available
The Sysmac Studio Controller Backup Function	This function allows you to save various settings data in the NJ/NX-series CPU Unit to a PC and restore the settings data in the CPU Unit by using the Sysmac Studio.	Available	Available
Program transfer from SD Memory Card	With the _Card1PrgTransferCmd (SD Memory Card Program Transfer Command) system-defined variable, you can transfer a program stored in the SD Memory Card mounted in the CPU Unit to the Controller.	Unavailable	Available
Automatic transfer from SD Memory Card	This function automatically transfers the data of the backup file in the */autoload* directory of the SD Memory Card in the CPU Unit to the Controller when the power is turned on.	Unavailable	Available

> **Precautions for Correct Use**
>
> The server certificate is not target for backup and restore because it is information belonging to individual CPU Units. If you replace the CPU Unit hardware, you cannot use the same server certificate for the new CPU Unit after the replacement.
>
> Even if you set the IP address of the built-in EtherNet IP port to the same value as the one for the previous CPU Unit, be sure to export the server certificate of the new CPU Unit and then perform installation again on the OPC UA clients.
>
> Refer to *3-2-5 Setting and Displaying the Certificate* on page 3-9 for how to export the server certificate.

8-2-1 Backup Function

The following table indicates OPC UA Server-related data to be backed up by the CPU Unit backup function.

Data	Data group for back up	Save location	Backed up by one of the following • SD Memory Card backup • Sysmac Studio Controller backup
OPC UA Server Settings	*User program and settings*	Non-volatile memory	Applicable
Server certificate	*OPC UA server certificate*	Non-volatile memory	Not applicable
Client certificate	*OPC UA security profile*	Non-volatile memory	Applicable [1]
CA certificate		Non-volatile memory	Applicable [1]
Certificate Revocation List		Non-volatile memory	Applicable [1]
Security settings (user authentication settings, anonymous login, and security policy)		Non-volatile memory	Applicable [1]
Execution logs	---	SD Memory Card	Not applicable
Event logs	*Event logs*	Backup memory	Applicable

*1. Not to be backed up by the backup function when the file is being exported or imported via the Sysmac Studio.

Precautions for Correct Use

• When you import the data of a backup file created with the SD Memory card backup function to a Sysmac Studio project and when you export the data of a Sysmac Studio project to a backup file, *client certificates*, *security settings*, and *Execution Logs* cannot be imported/exported. Please note that only *OPC UA Server Settings* can be imported/exported.

Additional Information

The Execution Log is not covered by the backup/restore function.

If you want to keep the Execution Log data after replacement of the CPU Unit, insert the SD Memory Card used for the previous CPU Unit into the new CPU Unit for restoration, after the restore completes.

8-2-2   Restoration and Verification

The following table shows OPC UA Server data items to be restored and verified by the CPU function.

Data	Data group of the backup function for each data	Save loca-tion	Restoration		Verification
			Restored by one of the fol-lowing • SD Memory Card Restore Function • The Sysmac Studio Con-troller back-ups	**Restored by one of the fol-lowing** • Automatic transfer from SD Memory Card • Program transfer from SD Memory Card	**Verified by one of the following** • SD Memory Card backups • The Sysmac Studio Con-troller back-ups
OPC UA Server Set-tings	*User program and settings*	Non-vola-tile memory	Applicable	Applicable	Applicable
Server certificate	*OPC UA server certificate*	Non-vola-tile memory	Not applicable	Not applicable	Not applicable
Client certificate	*OPC UA secu-rity profile*	Non-vola-tile memory	Depends on the selection [*]1		
CA certificate					
Certificate Revocation List					
Security settings (user authentication set-tings, anonymous login, and security policy)					
Execution logs	---	SD Mem-ory Card	Not applicable		
Event logs	*Event logs*	Backup memory	Not applicable		

*1. You can select whether or not to allow these types of data to be restored by the function. Refer to the next sec-
   tion *How to Select Whether or Not to Set OPC UA Security Profile as a Restore Target* on page 8-7 for the
   selection procedure.

How to Select Whether or Not to Set OPC UA Security Profile as a Restore Target

For restoring using the SD Memory Card Restore Function or the Sysmac Studio Controller Backup Function, you can select whether or not to restore the client certificates, CA certificates, Certificate Revocation List, and security settings together as the *OPC UA Security Profile*.

The selection procedures are as follows.

● SD Card Memory Restoration Function

There are two ways as below:

- When using the CPU Unit front panel switches and turning the power on
  You can select whether or not to restore the *OPC UA Security Profile* by setting the restore command file (RestoreCommand.ini) as shown below.

Contents (defaults when the file is created)	Description
[Restore]	Refer to the *NJ/NX-series CPU Unit Software User's Manual* (Cat. No. W501) for an explanation.
; --- User Program and Configuration. ---	
; Always select "yes".	OPC UA security profile
UserProgram=yes	yes/no: Restore/Do not restore.
: :	
; --- OPC UA Security Profile. ---	
; "yes":will be restored, "no":will not be restored	
OpcuaSPF=yes	

- When using system-defined variables

  You can use the *_Card1RestoreCmdTargetOpcuaSPF* (OPC UA Security Profile Transfer Flag) system-defined variable, as shown in detail below.

Variable name	Name	Function	Data type	Range of values
_Card1RestoreCmd TargetOpcuaSPF	OPC UA Security Profile Transfer Flag	When restoring *OPC UA security profile* in the SD Memory Card to the Controller, set this to *TRUE*.	BOOL	TRUE, FALSE

● When Using the Sysmac Studio Controller Backup Function

You can select whether or not to restore the *OPC UA Security Profile* by setting the *Restore Target File* in the **Restore** Dialog Box on the Sysmac Studio.

8-2-3   Compatibility between Backup-related Files

Refer to *Compatibility between Backup-related Files* in the *NJ/NX-series CPU Unit Software User's Manual* (Cat. No. W501) for details on compatibility between backup files.

8-2-4   How to Replace the CPU Unit in Relation to the OPC UA Server

The following shows how to replace the CPU Unit in relation to the OPC UA Server.

1 Using the Controller backup functions (i.e., SD Memory Card backup function or the Sysmac Studio Controller backup function), back up the settings data other than the server certificate in the CPU Unit to the SD Memory Card or the computer as a backup file.

2 Remove the SD Memory Card and insert it into the newly-installed CPU Unit.

3 Using the Controller restore functions (i.e., SD Memory Card restore function or the Sysmac Studio Controller backup function), restore the backed-up file to the new CPU Unit[*1].

   *1. You can select whether to restore the OPC UA security profile (i.e., client certificate, CA certificate, Certificate Revocation List, Security Settings) in the target data.

4 Cycle the power supply to the new CPU Unit, or reset the Controller.

   A new server certificate will be automatically generated.

   If the newly-installed CPU Unit has ever used the OPC UA Server, the event of *Server Certificate Mismatch* (event code: 15020000 hex) may be registered in the event log. If it is registered, connect online to the CPU Unit and regenerate a server certificate in the **Server Certificate** Tab Page.

5 Connect online to the new CPU Unit from the Sysmac Studio, right-click **OPC UA Server Settings**, and then click the **Export** Button in the **Server Certificate** Tab Page to export the server certificate.

6 Import the exported X.509 certificate file to the OPC UA client.

7 If you have not restored the OPC UA security profile, connect online to the new CPU Unit from the Sysmac Studio and reconfigure the security settings, the client certificate, and if necessary the CA certificate and Certificate Revocation List.

8-3   Clear All Memory Function Related to the OPC UA Server

This section describes the function for clearing all memory in the NJ/NX-series CPU Unit from the Sysmac Studio that is related to the OPC UA Server.

Clear All Memory is an operation to initialize the data in the CPU Unit from the Sysmac Studio.

The following table shows whether or not each data of the OPC UA Server is target for the Clear All Memory function.

Data		To be cleared or not
OPC UA Server Settings		Cleared
Server certificate		Whether cleared or not cleared can be selected
OPC UA security profile	Client certificates, CA certificates, and Certificate Revocation List	
	Security settings (user authentication settings, anonymous login, and security policy)	
Execution Logs		Not cleared

The Sysmac Studio Operation

The Clear All Memory operation can be performed on the Sysmac Studio only when the Controller is in PROGRAM mode. Before you clear All Memory, change the operating mode of the Controller to PROGRAM mode.

1   Connect the Sysmac Studio to the CPU Unit online, and select **Clear All Memory** from the **Controller** Menu. The following **Clear All Memory** Window is displayed.
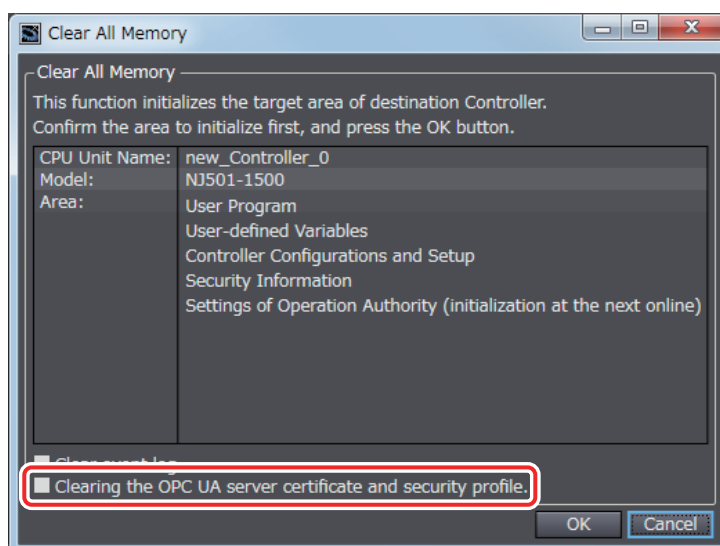
2 Select the following check box as needed.

Check box	Description
Clearing the OPC UA server certificate and security profile.	If you select this check box, the *OPC UA server certificate* and *OPC UA security profile* are cleared.
	If you deselect this check box, the *OPC UA server certificate* and *OPC UA security profile* are not cleared.

3 Click the **OK** Button. The following dialog box is displayed.

- When the **Clearing the OPC UA server certificate and security profile** Check Box is selected
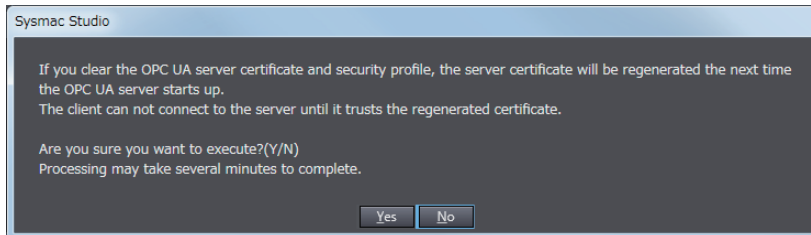
- When the **Clearing the OPC UA server certificate and security profile** Check Box is not selected
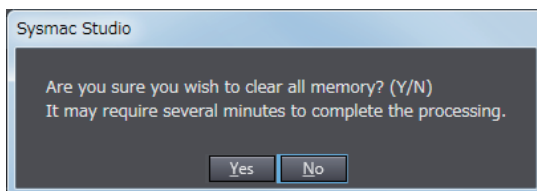
4 Click the **Yes** Button to clear all memory. All memory is cleared.

- When **OPC UA Server** in **OPC UA Server Settings** under **OPC UA Settings** is set to *Use* for the connected CPU Unit:
  The Controller must be reset. The following dialog box is displayed.
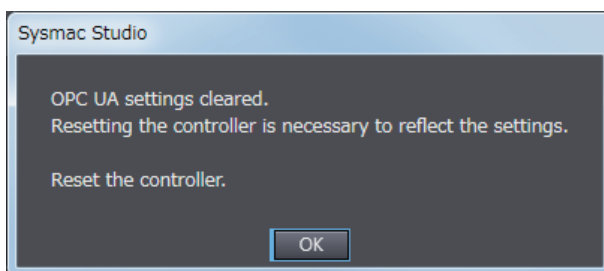
Click the **OK** Button. The Controller reset will be executed.

The following dialog box is displayed.
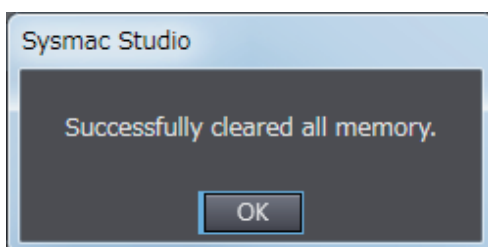
Click the **OK** Button.

- When **OPC UA Server** in **OPC UA Server Settings** under **OPC UA Settings** is set to *Do not use* for the connected CPU Unit:
  There is no need to cycle the power supply to the Controller, or reset the Controller. The following dialog box is displayed.
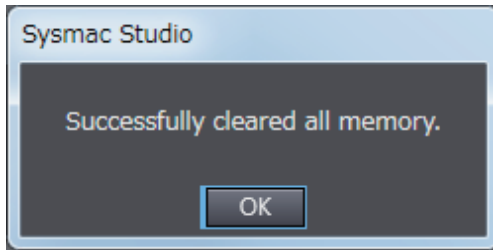
Click the **OK** Button.

Reconfiguring Procedures After Clear All Memory

After Clear All Memory, reconfigure the settings that are related to the OPC UA Server using the following procedures.

● When Not Clearing the Server Certificate And OPC UA Security Profile

1 Reconfigure the OPC UA Server Settings offline from the Sysmac Studio and download them to the CPU Unit.

2 Cycle the power supply to the Controller or reset the Controller.

● When Clearing the Server Certificate and OPC UA Security Profile

1 Reconfigure the OPC UA Server Settings offline from the Sysmac Studio and download them to the CPU Unit.

2 Cycle the power supply to the Controller or reset the Controller.

A server certificate will be created automatically.

3 Connect online from the Sysmac Studio to the CPU Unit, and set the Security Settings, client certificate, and if necessary the CA certificate and Certificate Revocation List.

4 Connect online from the Sysmac Studio to the CPU Unit, and click the **Export** Button in the **Server Certificate** Tab Page to export the server certificate.

5 Import the exported server certificate (X.509 certificate file) to the OPC UA client.

9

Troubleshooting

This section describes the error confirmation methods and corrections for errors that can occur with the OPC UA Server.

9

9-1 Overview of Errors

You manage all of the errors that occur on the NJ/NX-series Controller as events. The same methods are used for all events. This allows you to see what errors have occurred and find corrections for them with the same methods for the entire range of errors that is managed (i.e., CPU Unit, EtherCAT slaves [1], and CJ-series Units).

*1. Only the Sysmac devices are supported.
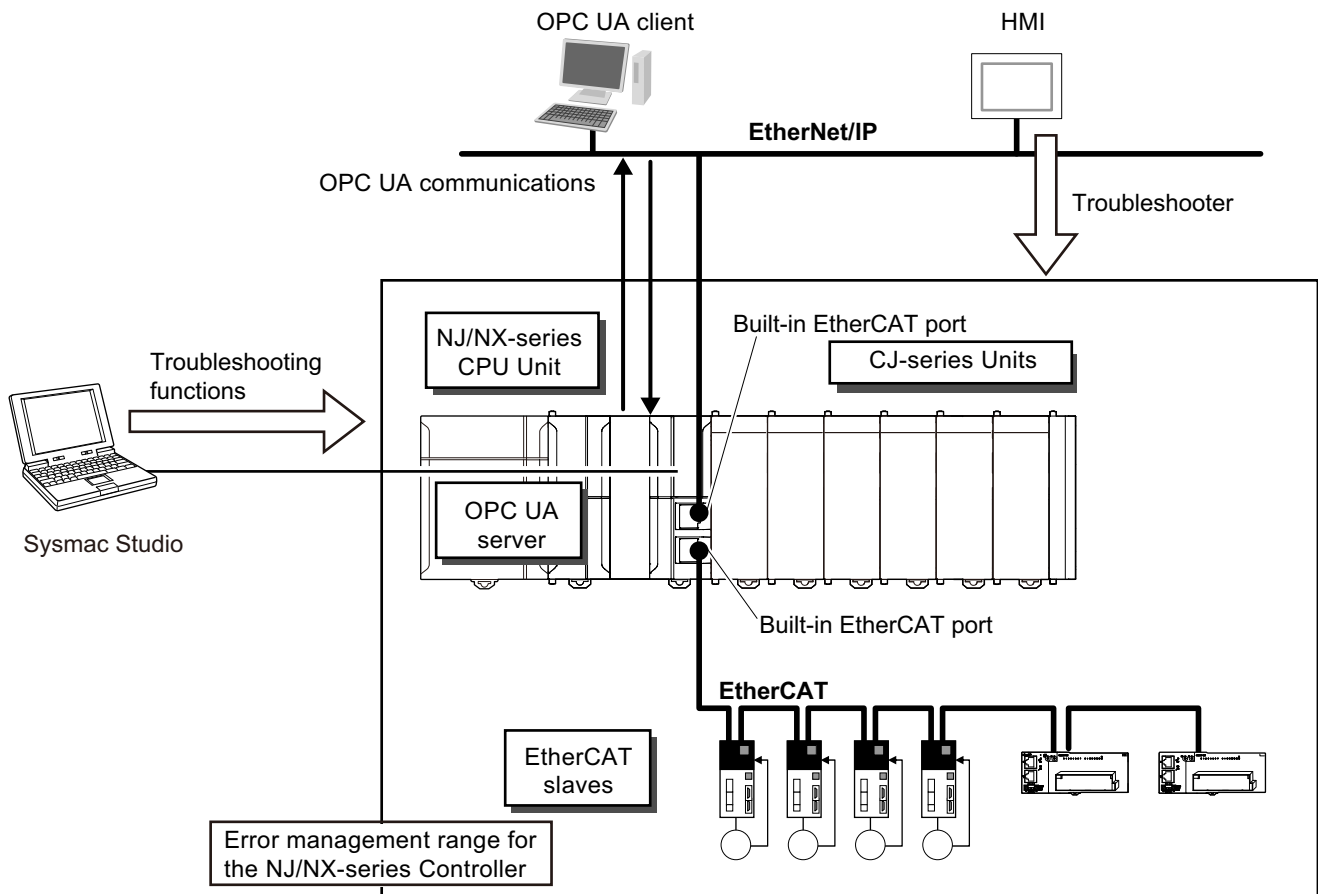
You can use the troubleshooting functions of the Sysmac Studio or the Troubleshooter of the HMI to quickly check for errors that have occurred and find corrections for them.

This manual describes the errors that originate from the OPC UA Server.

Refer to the *NJ/NX-series Troubleshooting Manual* (Cat. No. W503) for specific error corrections and for troubleshooting information on the entire NJ/NX-series Controller.

9-1-1 How to Check for Errors

You can check to see if an event has occurred with the following methods.

Checking method	What you can check
Checking indicators	CPU Unit operating status
Checking with the troubleshooting function of the Sysmac Studio	You can check for current Controller errors, a log of past Controller errors, error sources, error causes, corrections, and error log of CJ-series Special Units.[*1]
Checking with the troubleshooter of an HMI [*2]	You can check for current Controller errors, a log of past Controller errors, error sources, error causes, and corrections.
Checking with an instruction that reads the function module error status	You can check the highest-level status and highest-level event code in the current Controller errors.
Checking with system-defined variables	You can check the current Controller error status for each function module.

*1. Detailed information such as error causes and corrections are not displayed.

*2. To perform troubleshooting from an HMI, connect the HMI to the built-in EtherNet/IP port on the CPU Unit.

This section describes the above checking methods.

● Checking Indicators

You can use the PWR indicator on the Power Supply Unit and the RUN and ERROR indicators on the CPU Unit to determine the event level for an error. The following table shows the relationship between the Controller's indicators and the event level.

LED			CPU Unit operating status	The Sysmac Studio / HMI
PWR	RUN	ERROR		
Not lit	Not lit	Not lit	Power supply error	Not possible:
Lit	Not lit	Not lit	CPU Unit reset [*1]	Refer to the *NJ/NX-series Troubleshooting Manual* (Cat. No. W503).
Lit	Flashing	Lit	Incorrect power supply unit connected	
Lit	Not lit	Lit	CPU Unit watchdog timer error [*2]	
Lit	Not lit	Lit	Major fault level [*2]	Possible:
Lit	Lit	Flashing	Partial fault level	Connect the Sysmac Studio or an HMI and check the cause of and correction for the error with the troubleshooting functions of the Sysmac Studio or the Troubleshooter of the HMI.
Lit	Lit	Flashing	Minor fault level	
Lit	Lit	Not lit	Observation	
Lit	Lit	Not lit	Normal operation in RUN mode	---
Lit	Not lit	Not lit	Normal operation in PROGRAM mode [*1]	---
Lit	Flashing	Not lit	Normal operation in startup state	---

*1. If you can go online with the CPU Unit from the Sysmac Studio with *Direct connection via USB*, the CPU Unit is in PROGRAM mode. If you cannot go online, a CPU Unit Reset has occurred. [*3]

*2. If you can go online with the CPU Unit from the Sysmac Studio with *Direct connection via USB*, a major fault level error has occurred. If you cannot go online, a CPU Unit Watchdog Timer error has occurred. [*3]

*3. If you cannot go online with the CPU Unit from the Sysmac Studio, it is also possible that the USB cable is faulty or that the **Connection Type** setting on the Sysmac Studio is not set to *Direct connection via USB*. Refer to the *NJ/NX-series Troubleshooting Manual* (Cat. No. W503) if you cannot go online with the CPU Unit.

Checking with the Troubleshooting Function of the Sysmac Studio

When an error occurs, you can connect the Sysmac Studio online to the Controller to check current Controller errors and the log of past Controller errors.

You can also check error causes and corrections.

Refer to the *NJ/NX-series Troubleshooting Manual* (Cat. No. W503) for the procedures to check for errors with the Sysmac Studio.

Checking with the Troubleshooter of an HMI

If a connection is established between an HMI and the Controller when an error occurs, you can check for current Controller errors and the log of past Controller errors.

You can also check the cause of the error and corrections.

Refer to the *NJ/NX-series Troubleshooting Manual* (Cat. No. W503) for the procedures to check for errors with an HMI.

● Checking with an Instruction That Reads the Error Status

You can use an instruction in the user program to check the error status of each function module.

The following table gives the instruction that is used to get the error information for the OPC UA Server.

Instruction	Name	Function
GetPLCError	Get PLC Error Status	The **GetPLCError** instruction gets the highest level status (partial fault or minor fault) and highest level event code of the current Controller errors in the PLC Function Module.

For details on the instruction that gets the error status, refer to the *NJ/NX-series Instructions Reference Manual* (Cat. No. W502).

9-1-2 Error Checking Methods

This section describes errors related to the OPC UA Server.

Classification

The source of OPC UA Server errors is described below.

Detection loca-tion	Event source	Event source details	Event log category		
			System log	Access log	User-defined event log
OPC UA Server	PLC function module	OPC UA Server	Yes	No	No

Event Levels

This section describes the operation of the OPC UA Server for each event level.

Event level of the error	Operation
Major fault	All NJ/NX-series Controller control operations stop for errors in this event level.
Partial fault	All control operations for one of the function modules in the NJ/NX-series Controller stop for errors in this event level.
	If a partial fault level error occurs on the OPC UA Server, all functions of the OPC UA Server stop.
Minor fault	Some of the control operations for one of the function modules in the NJ/NX-series Controller stop for errors in this event level.
Observation	Errors in the observation level do not affect the NJ/NX-series Controller control operations.
	Observations are reported in order to prevent them from developing into errors at the minor fault level or higher.
Information	Events that are classified as information provide information that does not indicate errors.

OPC UA Server Errors

The following tables list error events by event level.

● OPC UA Server Errors

Error event level	Error name
Major fault	None
Partial fault	None
Minor fault	• Execution Log Save Failed • OPC UA Server Setting Error • Server Certificate Expired • OPC UA System Processing Error
Observation	• Server Certificate Mismatch • Notice of Expiration of Server Certificate • Too Many Public Variables • Unsupported Data Type • Too Many Public Value Attributes • Too Many Structure Definitions • OPC UA Client Connection Rejected
Information	• OPC UA Server Started • OPC UA Server Stopped • Server Certificate Generated • Client Certificate Discarded • OPC UA Server Certificate and Security Profile Cleared

9-2   Troubleshooting

This section describes the errors that can occur in the OPC UA Server and the corrections for them.

9-2-1   Error Table Related to the OPC UA Server

The errors (i.e., events) related to the OPC UA Server are given on the following pages.

The following abbreviations and symbols are used in the event level column.

Abbreviation	Name
Maj	Major fault level
Prt	Partial fault level
Min	Minor fault level
Obs	Observation
Info	Information

Symbol	Meaning
S	Event levels that are defined by the system.
U	Event levels that can be changed by the user.[1]

*1. This symbol appears only for events for which the user can change the event level.

Refer to the *NJ/NX-series Troubleshooting Manual* (Cat. No. W503) for all NJ/NX-series event codes.

Errors Related to the OPC UA Server

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
15000000 hex	Execution Log Save Failed	Failed to save the Execution Log to the SD Memory Card.	• An SD Memory Card is not inserted. • The SD Memory Card type is not correct. • The format of the SD Memory Card is not correct. • The SD Memory Card is write protected. • The SD Memory Card does not have sufficient available space. • The SD Memory Card is damaged.			S	U		P. 9-12

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
15020000 hex	Server Certificate Mismatch	The IP address of the server certificate in the CPU Unit is not the same as that of the built-in EtherNet/IP port on the CPU Unit.	The IP address of the built-in EtherNet/IP port of the CPU Unit was changed when the OPC Server Use Option is set to *Use*. • The IP address was changed by the **ChangeIPAdr** (Change IP Address) instruction. • If the IP address setting method was *Obtain from BOOTP server*, the IP address was changed when the power is turned ON. • A project containing a different IP address for the built-in EtherNet/IP port of the CPU Unit was downloaded to the CPU Unit.				S		P. 9-13
35D00000 hex	OPC UA Server Setting Error	The OPC UA Server Settings are incorrect.	• The power supply to the Controller was interrupted while the OPC UA Server Settings were being transfered. • The power supply to the Controller was interrupted during a Clear All Memory operation. • The OPC UA Server settings are not correct because the Controller was interrupted during a restore operation. • TCP port number is duplicated.			S			P. 9-14
35D10000 hex	Server certificate Expired	The server certificate expired.	• The period that is set in the server certificate expired.			S	U		P. 9-14
35D20000 hex	Server Certificate Expiration Notice	The server certificate is close to expiring.	• The period that is set in the server certificate is close to expiring.			U	S		P. 9-15
35D30000 hex	Too Many Public Variables	The number of variables that can be published to the OPC UA client exceeded the upper limit when the OPC UA Server was prepared.	• When the OPC UA Server prepared the address space, the number of OPC UA variables exceeded the upper limit.				S		P. 9-15
35D40000 hex	Unsupported Data Type	When the OPC UA Server was prepared, the network-published global variables included a data type variable that cannot be published to the OPC UA client.	The OPC UA Server had an unsupported data type in the network-published global variables. Unsupported data types are as follows. • Multidimensional array specified structure • Structure containing multidimensional array(s) as member(s) • Structure whose nesting number exceeds the limit value • Union • Array whose start number is not 0; e.g., Array[2..5] • Variable whose size exceeds the limit value • Array whose number of elements exceeds the limit value • Structure whose number of members exceeds the limit value				S		P. 9-16

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
35D50000 hex	Too Many Public Value Attributes	The number of value attributes to be published to the OPC UA client exceeded the upper limit when the OPC UA Server was prepared.	• When the OPC UA Server prepared the address space, the number of OPC UA value attributes has exceeded the upper limit.				S		P. 9-17
35D60000 hex	Too Many Structure Definitions	The number of structure definitions to be published to the OPC UA client exceeded the upper limit when the OPC UA Server was prepared.	• When the OPC UA Server prepared the address space, the number of structure definitions has exceeded the upper limit.				S		P. 9-17
44180000 hex	OPC UA System Processing Error	A fatal error was detected in the OPC UA Server.	• A software error occurred.			S			P. 9-18
85600000 hex	OPC UA Client Connection Rejected	A connection request from an OPC UA client was rejected.	• User authentication information was incorrect. • The client certificate was incorrect. • The client certificate was registered in the Rejected Certificate List. • The CA certificate is not registered in the Trusted Certificate List for Client authentication or Issuer authentication. • The number of sessions has exceeded the maximum number of connectable sessions.				S		P. 9-19
95D00000 hex	OPC UA Server Started	The OPC UA Server started.	• The OPC UA Server started.					S	P. 9-20
95D10000 hex	OPC UA Server Stopped	The OPC UA Server stopped.	• The OPC UA Server stopped.					S	P. 9-20
95D20000 hex	Server Certificate Generated	A server certificate was generated. • The server certificate is automatically generated when there is no server certificate. • The server certificate is generated when Regenerate certificate is performed.	• A server certificate was generated.					S	P. 9-21
95D30000 hex	Client Certificate Discarded	Received client certificates were discarded	• The maximum number of client certificates that can be registered in the Rejected Certificate List has been exceeded.					S	P. 9-21

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
95D40000 hex	OPC UA Server Certificate and Security Profile Cleared	The OPC UA Server certificate and Security Profile have been cleared.	• A restore was executed using a backup file created by a CPU Unit whose version does not support the OPC UA Server. • A project was downloaded from a CPU Unit without the OPC UA Server. • Checked *Clearing the OPC UA server certificate and security profile.* and performed Clear All Memory operation.					S	P. 9-22

Errors Related to the OPC UA Instructions

The lower four digits of an event code give the error code for the instruction. For details of error codes, refer to the description of the corresponding event code. For example, for an error code, 16#5000, refer to the description for event code 54015000 hex.

Event code	Event name	Meaning	Assumed cause	Level					Reference
				Maj	Prt	Min	Obs	Info	
54015000 hex	OPC UA Server Shutdown or Shutting Down	The OPC UA Server was already shut down or was being shut down.	• The OPCUA_Shutdown (Shutdown OPC UA Function) instruction was executed while the OPC UA Server was already shut down. • The OPCUA_Shutdown (Shutdown OPC UA Function) instruction was executed while the OPC UA Server was being shut down.				S		P. 9-23
54015001 hex	OPC UA Server Being Initialized	The OPCUA_Shutdown (Shutdown OPC UA Function) instruction could not be executed because the OPC UA Server was being initialized.	• The OPCUA_Shutdown (Shutdown OPC UA Function) instruction was executed while the OPC UA Server was being initialized.				S		P. 9-24
54015002 hex	OPC UA Server Not Started	The relevant instruction could not be executed because the OPC UA Server had not been started.	• When the Server Use Option is set to *Do not use*, the relevant instruction was executed.				S		P. 9-24

9-2-2   OPC UA Server Error Description

This section describes the information that is given for individual errors.

How to Read Error Descriptions

The items that are used to describe individual errors (events) are described in the following copy of an error table.

Event name	Gives the name of the error.			Event code	Gives the code of the error.
Meaning	Gives a short description of the error.				
Source	Gives the source of the error.	Source details	Gives details on the source of the error.	Detection timing	Tells when the error is detected.
Error attributes	Level	Tells the level of influence on control.[1]		Log category	Tells which log the error is saved in.[2]
	Recovery	Gives the recovery method.[3]			
Effects	User program	Tells what will happen to execution of the user program.[4]	Operation	Provides special information on the operation that results from the error.	
System-defined variables	Variable		Data type		Name
	Lists the variable names, data types, and meanings for system-defined variables that provide direct error notification, that are directly affected by the error, or that contain settings that cause the error.				
Cause and correction	Assumed cause		Correction		Prevention
	Lists the possible causes, corrections, and preventive measures for the error.				
Attached information	This is the attached information that is displayed by the Support Software or an HMI.				
Precautions/Remarks	Provides precautions, restrictions, and supplemental information. If the user can set the event level, the event levels that can be set, the recovery method, operational information, and other information are also provided.				

*1. One of the following:
    Major fault: Major fault level
    Partial fault: Partial fault level
    Minor fault: Minor fault level
    Observation
    Information

*2. One of the following:
    System: System event log
    Access: Access event log

*3. One of the following:
    Automatic recovery: Normal status is restored automatically when the cause of the error is removed.
    Cycle the power supply: Normal status is restored when the power supply to the Controller is turned OFF and then back ON after the cause of the error is removed.
    Controller reset: Normal status is restored when the Controller is reset after the cause of the error is removed.
    Depends on cause: The recovery method depends on the cause of the error.

*4. One of the following:
    Continues: Execution of the user program will continue.
    Stops: Execution of the user program stops.
    Starts: Execution of the user program starts.

Errors Related to the OPC UA Server

Event name	Execution Log Save Failed			Event code	15000000 hex
Meaning	Failed to save the Execution Log to the SD Memory Card.				
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	Continuously
Error attributes	Level	Minor fault		Log category	System
	Recovery	Automatic recovery			
Effects	User program	Continues	Operation	Not affected	
System-defined variables	Variable		Data type		Name
	None		---		---

Cause and correction	Assumed cause	Correction	Prevention
	An SD Memory Card is not inserted.	Insert an SD Memory Card.	Insert an SD Memory Card.
	The SD Memory Card type is not correct.	Replace the SD Memory Card with an SD or SDHC card.	Use an SD or SDHC card.
	The format of the SD Memory Card is not correct.	Format the SD Memory Card with the Sysmac Studio.	Use a formatted SD Memory Card. Also, do not remove the SD Memory Card or turn OFF the power supply while the SD BUSY indicator is lit.
	The SD Memory Card is write protected.	Remove write protection from the SD Memory Card.	Make sure that the SD Memory Card is not write protected.
	The capacity of the SD Memory Card is insufficient.	Replace the SD Memory Card for one with sufficient available capacity.	Replace the SD Memory Card for one with sufficient available capacity.
	The SD Memory Card is damaged.	Replace the SD Memory Card.	Do not remove the SD Memory Card or turn OFF the power supply while the SD BUSY indicator is lit.
			Replace the SD Memory Card periodically according to the write life of the SD Memory Card.
			Do not remove the SD Memory Card while the SD PWR indicator is lit.

Attached information	Attached information 1: Error Details
	0001 hex: An SD Memory Card is not inserted
	0002 hex: The SD Memory Card is faulty, the format of the SD Memory Card is not correct, or the SD Memory Card type is not correct.
	0003 hex: The SD Memory Card is write protected.
	0005 hex: There is not sufficient space available on the SD Memory Card.
	0302 hex: A file was not successfully saved to the SD Memory Card due to other factors, or the SD Memory Card is damaged.
Precautions/Remarks	None

Event name	Server Certificate Mismatch		Event code	15020000 hex	
Meaning	The IP address of the server certificate in the CPU Unit is not the same as that of the built-in EtherNet/IP port on the CPU Unit.				
Source	PLC Function Module		OPC UA Server	Detection timing	At CPU Unit power ON, at Controller reset, at Download, or Periodically (every 24 hours)
		Source details			
Error attributes	Level	Observation		Log category	System
	Recovery	---			
Effects	User program	Continues	Operation	Not affected	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and correction	Assumed cause		Correction		Prevention
	The IP address of the built-in EtherNet/IP port of the CPU Unit was changed when the OPC UA Server Use Option is set to *Use*. • The IP address was changed by the **ChangeIPAdr** (Change IP Address) instruction. • If the IP address setting method was *Obtain from BOOTP server*, the IP address was changed when the power is turned ON. • A project containing a different IP address for the built-in EtherNet/IP port of the CPU Unit was downloaded to the CPU Unit.		Restore the IP address of the built-in EtherNet/IP port on the CPU Unit, or regenerate the server certificate.		Regenerate the server certificate after changing the IP address of the built-in EtherNet/IP port on the CPU Unit.
Attached information	Attached Information 1: The IP address of the server certificate				
Precautions/Remarks	This event will not be registered in duplicate until the power supply to the Controller is cycled or the Controller is reset or the Server certificate is regenerated.				

Event name	OPC UA Server Setting Error		Event code	35D00000 hex	
Meaning	The OPC UA Server Settings are incorrect.				
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	At Download, at CPU Unit power ON, at Controller reset
Error attributes	Level	Minor fault	Log category	System	
	Recovery	Automatic recovery			
Effects	User program	Continues	Operation	• The OPC UA Server cannot be started. • The operating status of the OPC UA Server will move to the *Halt error* state.	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and correction	Assumed cause		Correction		Prevention
	• The power supply to the Controller was interrupted while the OPC UA Server Settings were being transfered. • The power supply to the Controller was interrupted during a Clear All Memory operation. • The OPC UA Server settings are not correct because the Controller was interrupted during a restore operation.		Transfer the OPC UA Server Settings again with the Sysmac Studio.		None
	TCP port number is duplicated.		Do not set the same port number as that of the socket communications instructions or FTP server settings.		Do not set the same port number as that of the socket communications instructions or FTP server settings.
Attached information	None				
Precautions/Remarks	None				

Event name	Server certificate Expired		Event code	35D10000 hex	
Meaning	The server certificate expired.				
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	At Download, at CPU Unit power ON, at Controller reset, or Periodically (every 24 hours)
Error attributes	Level	Minor fault	Log category	System	
	Recovery	Automatic recovery			
Effects	User program	Continues	Operation	Not affected	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and correction	Assumed cause		Correction		Prevention
	The period that is set in the server certificate expired.		Regenerate the server certificate.		Consider the expiration date of the server certificate.
Attached information	Attached Information 1: The expiration date of the server certificate "YYYY-MM-DD HH:MM:SS"				
Precautions/Remarks	This event will not be registered in duplicate until the power supply to the Controller is cycled or the Controller is reset or the Server certificate is regenerated.				

Event name	Server Certificate Expiration Notice		Event code	35D20000 hex	
Meaning	The server certificate is close to expiring.				
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	At CPU Unit power ON, at Controller reset, or Periodically (every 24 hours)
Error attributes	Level	Observation	Log category	System	
	Recovery	---			
Effects	User program	Continues	Operation	Not affected	
System-defined variables	Variable		Data type	Name	
	None		---	---	
Cause and correction	Assumed cause	Correction	Prevention		
	The period that is set in the server certificate is close to expiring.	Regenerate the server certificate.	Consider the expiration date of the server certificate.		
Attached information	Attached Information 1: The expiration date of the server certificate "YYYY-MM-DD HH:MM:SS"				
Precautions/Remarks	This event will not be registered in duplicate until the power supply to the Controller is cycled or the Controller is reset or the Server certificate is regenerated.				

Event name	Too Many Public Variables		Event code	35D30000 hex	
Meaning	The number of variables that can be published to the OPC UA client exceeded the upper limit when the OPC UA Server was prepared.				
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	At CPU Unit power ON, at Controller reset, restore operation, at download, or online editing
Error attributes	Level	Observation	Log category	System	
	Recovery	---			
Effects	User program	Continues	Operation	Not affected	
System-defined variables	Variable		Data type	Name	
	None		---	---	
Cause and correction	Assumed cause	Correction	Prevention		
	When the OPC UA Server prepared the address space, the number of OPC UA variables has exceeded the upper limit.	Make the number of the network-published global variables less than the maximum number that can be published to the OPC UA client.	Keep the number of the network-published global variables below the maximum number that can be published to the OPC UA client.		
Attached information	None				
Precautions/Remarks	This event does not occur if the OPC UA Server Use Option is set to *Do not use* or when you use a project not compatible with the OPC UA Server.				

Event name	Unsupported Data Type		Event code	35D40000 hex	
Meaning	When the OPC UA Server was prepared, the network-published global variables included a data type variable that cannot be published to the OPC UA client.				
Source	PLC Function Module	**Source details**	OPC UA Server	**Detection timing**	At CPU Unit power ON, at Controller reset, restore operation, at download, or online editing
Error attributes	Level	Observation		Log category	System
	Recovery	---			
Effects	User program	Continues	**Operation**	Not affected	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and correction	**Assumed cause**		**Correction**		**Prevention**
	The OPC UA Server had an unsupported data type in the network-published global variables. Unsupported data types are as follows. • Multidimensional array specified structure • Structure containing multidimensional array(s) as member(s) • Structure whose nesting number exceeds the limit value • Union • Array whose start number is not 0; e.g., Array[2..5] • Variable whose size exceeds the limit value • Array whose number of elements exceeds the limit value • Structure whose number of members exceeds the limit value		Set global variables of the following data types to be not published. • Multidimensional array specified structure • Structure containing multidimensional array(s) as member(s) • Structure whose nesting number exceeds the limit value • Union • Array whose start number is not 0; e.g., Array[2..5] • Variable whose size exceeds the limit value • Array whose number of elements exceeds the limit value • Structure whose number of members exceeds the limit value		Set global variables of the following data types to be not published. • Multidimensional array specified structure • Structure containing multidimensional array(s) as member(s) • Structure whose nesting number exceeds the limit value • Union • Array whose start number is not 0; e.g., Array[2..5] • Variable whose size exceeds the limit value • Array whose number of elements exceeds the limit value • Structure whose number of members exceeds the limit value.

Attached information	Attached Information 1: Error Details
	
	        Bit 00: Multidimensional array specified structure
	
	        Bit 01: Structure containing multidimensional array(s) as member(s)
	
	        Bit 02: Structure whose nesting number exceeds the limit value.
	
	        Bit 03: Union
	
	        Bit 04: Array whose start number is not 0; e.g., Array[2..5]
	
	        Bit 05: Variable whose size exceeds the limit value
	
	        Bit 06: Array whose number of elements exceeds the limit value
	
	        Bit 07: Structure whose number of members exceeds the limit value				

Precautions/Remarks	None				

Event name	Too Many Public Value Attributes			Event code	35D50000 hex	
Meaning	The number of value attributes to be published to the OPC UA client exceeded the upper limit when the OPC UA Server was prepared.					
Source	PLC Function Module		Source details	OPC UA Server	Detection timing	At CPU Unit power ON, at Controller reset, restore operation, at download, or online editing
Error attributes	Level	Observation		Log category	System	
	Recovery	---				
Effects	User program		Operation	Not affected		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	When the OPC UA Server prepared the address space, the number of OPC UA value attributes has exceeded the upper limit.		Check the number or data type of the network-published global variables and make it less than the maximum number of value attributes.		Check the number or data type of the network-published global variables and make it less than the maximum number of value attributes.	
Attached information	None					
Precautions/Remarks	None					

Event name	Too Many Structure Definitions			Event code	35D60000 hex	
Meaning	The number of structure definitions to be published to the OPC UA client exceeded the upper limit when the OPC UA Server was prepared.					
Source	PLC Function Module		Source details	OPC UA Server	Detection timing	At CPU Unit power ON, at Controller reset, restore operation, at download, or online editing
Error attributes	Level	Observation		Log category	System	
	Recovery	---				
Effects	User program	Continues	Operation	Not affected		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and correction	Assumed cause		Correction		Prevention	
	When the OPC UA Server prepared the address space, the number of structure definitions has exceeded the upper limit.		Check the data type of the network-published global variables and make sure that the number of structure definitions does not exceed the upper limit.		Check the data type of the network-published global variables and make sure that the number of structure definitions does not exceed the upper limit.	
Attached information	None					
Precautions/Remarks	None					

Event name	OPC UA System Processing Error		Event code	44180000 hex	
Meaning	A fatal error was detected in the OPC UA Server.				
Source	PLC Function Module		Source details	OPC UA Server	Detection timing	---
Error attributes	Level	Minor fault		Log category	System
	Recovery	---			
Effects	User pro-gram	Continues	Operation	Not affected	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and cor-rection	Assumed cause		Correction		Prevention
	An error occurred in the software.		Cycle the power supply to the Controller, or reset the Con-troller.		---
Attached infor-mation	None				
Precau-tions/Remarks	None				

Event name	OPC UA Client Connection Rejected		Event code	85600000 hex	
Meaning	A connection request from an OPC UA client was rejected.				
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	When receiving a connection request from a OPC UA client
Error attributes	Level	Observation		Log category	System
	Recovery	---			
Effects	User program	Continues	Operation	The OPC UA client cannot connect to the OPC UA Server.	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and correction	Assumed cause		Correction		Prevention
	User authentication information was incorrect.		Use the correct user name and password.		Set the correct user name and password for OPC UA client.
	The client certificate was incorrect.		Check that the client certificate registered in the CPU Unit is correct.		Register the correct client certificate in the CPU Unit.
			Make sure the client certificate used by the OPC UA client is correct.		Register the correct client certificate in the CPU Unit.
	The client certificate was registered in the Rejected Certificate List.		Register the client certificate to the Trusted Certificate List, and then reconnect.		Register to the Trusted Client List the certificate of the client to be connected
	The CA certificate is not registered in the Trusted Certificate List for Client authentication or Issuer authentication.		Register the CA certificate to the Trusted Certificate List for Client authentication or Issuer authentication, and then reconnect.		Register the CA certificate to the Trusted Certificate List for Client authentication or Issuer authentication.
	The number of sessions has exceeded the maximum number of connectable sessions.		Make sure the number of sessions is below the maximum connectable sessions.		Reconsider the configuration to make sure that the number of sessions is less than the maximum number of sessions that can be connected.
Attached information	Attached information 1: Reasons for connection rejected				
	01 hex: Incorrect user authentication information				
	02 hex: Untrusted certificate				
	04 hex: Maximum connectable sessions exceeded				
	Attached information 2: Details				
	User name if the reason for connection rejected is set to 01 hex, as described above.				
Precautions/Remarks	None				

Event name	OPC UA Server Started			Event code	95D00000 hex	
Meaning	The OPC UA Server started.					
Source	PLC Function Module		Source details	OPC UA Server	Detection timing	At start of OPC UA Server
Error attributes	Level	Information		Log category	System	
	Recovery	---				
Effects	User pro-gram	Continues	Operation	Not affected		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and cor-rection	Assumed cause		Correction		Prevention	
	The OPC UA Server started.		None		None	
Attached infor-mation	None					
Precau-tions/Remarks	None					

Event name	OPC UA Server Stopped			Event code	95D10000 hex	
Meaning	The OPC UA Server stopped.					
Source	PLC Function Module		Source details	OPC UA Server	Detection timing	At OPC-UA_Shutdown (Shutdown OPC UA Func-tion) instruc-tion execution, shutdown operation from the Sysmac Studio
Error attributes	Level	Information		Log category	System	
	Recovery	---				
Effects	User pro-gram	Continues	Operation	The OPC UA Server stopped.		
System-defined variables	Variable		Data type		Name	
	None		---		---	
Cause and cor-rection	Assumed cause		Correction		Prevention	
	The OPC UA Server stopped.		None		None	
Attached infor-mation	None					
Precau-tions/Remarks	This event is not registered when the OPC UA Server stops due to power OFF. To start the OPC UA Server, cycle the power supply to the Controller or reset the Controller.					

Event name	Server Certificate Generated		Event code	95D20000 hex
Meaning	A server certificate was generated. • The server certificate is automatically generated when there is no server certificate. • The server certificate is generated when Regenerate certificate is performed.			
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	When a server certificate is generated
Error attributes	Level	Information		Log category	System
	Recovery	---			
Effects	User program	Continues	Operation	Not affected	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and correction	Assumed cause		Correction		Prevention
	A server certificate was generated.		None		None
Attached information	None				
Precautions/Remarks	None				

Event name	Client Certificate Discarded		Event code	95D30000 hex
Meaning	Received client certificates were discarded.			
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	When receiving a connection request from a OPC UA client
Error attributes	Level	Information		Log category	System
	Recovery	---			
Effects	User program	Continues	Operation	Not affected	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and correction	Assumed cause		Correction		Prevention
	The maximum number of client certificates that can be registered in the Rejected Certificate List has been exceeded.		Delete registered client certificates from the Rejected Certificate List.		Delete unnecessary client certificates from the Rejected Certificate List
Attached information	Attached information 1: The IP address of the discarded client certificate				
Precautions/Remarks	None				

Event name	OPC UA Server Certificate and Security Profile Cleared		Event code	95D40000 hex	
Meaning	The OPC UA Server certificate and Security Profile have been cleared.				
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	At Download, restore operation, Clear All Memory operation with the relevant checkbox checked
Error attributes	Level	Information	Log category	System	
	Recovery	---			
Effects	User program	Continues	Operation	Not affected	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and correction	Assumed cause		Correction		Prevention
	• A restore was executed using a backup file created by a CPU Unit whose version does not support OPC UA Server. • A project was downloaded from a CPU Unit without OPC UA Server. • Checked *Clearing the OPC UA server certificate and security profile.* and performed Clear All Memory operation.		---		---
Attached information	None				
Precautions/Remarks	None				

Errors Related to the OPC UA Instructions

This section provides a table of errors (events) that occur for the following instruction.

The lower four digits of the event code give the error code for the instruction.

OPC UA instruction	Name
OPCUA_Shutdown	Shutdown OPC UA Server

Event name	OPC UA Server Shutdown or Shutting Down		Event code		54015000 hex
Meaning	The OPC UA Server was already shut down or was being shut down.				
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	At instruction execution
Error attributes	Level	Observation		Log category	System
	Recovery	---			
Effects	User program	Continues	Operation	The relevant instruction will end according to specifications.	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and correction	Assumed cause	Correction		Prevention	
	• The OPCUA_Shutdown (Shutdown OPC UA Function) instruction was executed while the OPC UA Server was already shut down. • The OPCUA_Shutdown (Shutdown OPC UA Function) instruction was executed while the OPC UA Server was being shut down.	Cycle the power supply to the Controller and start the OPC UA Server before executing the relevant instruction.		When you write the user program, make sure that an OPC-UA_Shutdown (Shutdown OPC UA Function) instruction cannot be repeated after the same instruction is executed, or that the shutdown instruction cannot be executed after the same instruction is performed from the Sysmac Studio.	
Attached information	Attached Information 1: Error Location Attached Information 2: Error Location Details (Rung Number). For a program section, the rung number from the start of the section is given. For ST, the line number is given. Attached Information 3: Names of the Instruction and Instruction Instance Where the Error Occurred. If there is more than one possible instruction, information is given on all of them. Nothing is given If the instruction cannot be identified.				
Precautions/Remarks	If a program is changed after an error occurs, the attached information may not be correctly displayed.				

Event name	OPC UA Server Being Initialized		Event code	54015001 hex	
Meaning	The OPCUA_Shutdown (Shutdown OPC UA Function) instruction could not be executed because the OPC UA Server was being initialized.				
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	At instruction execution
Error attributes	Level	Observation		Log category	System
	Recovery	---			
Effects	User pro-gram	Continues	Operation	The relevant instruction will end according to specifications.	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and cor-rection	Assumed cause		Correction		Prevention
	The OPCUA_Shutdown (Shutdown OPC UA Function) instruction was executed while the OPC UA Server was being initialized.		Execute the relevant instruc-tion again.		Execute the relevant instruction again.
Attached infor-mation	Attached Information 1: Error Location Attached Information 2: Error Location Details (Rung Number). For a program section, the rung num-ber from the start of the section is given. For ST, the line number is given. Attached Information 3: Names of the Instruction and Instruction Instance Where the Error Occurred. If there is more than one possible instruction, information is given on all of them. Nothing is given If the instruction cannot be identified. Attached Information 4: Expansion Error Code (ErrorIDEx)				
Precau-tions/Remarks	If a program is changed after an error occurs, the attached information may not be correctly displayed.				

Event name	OPC UA Server Not Started		Event code	54015002 hex	
Meaning	The relevant instruction could not be executed because the OPC UA Server had not been started.				
Source	PLC Function Module	Source details	OPC UA Server	Detection timing	At instruction execution
Error attributes	Level	Observation		Log category	System
	Recovery	---			
Effects	User pro-gram	Continues	Operation	The relevant instruction will end according to specifications.	
System-defined variables	Variable		Data type		Name
	None		---		---
Cause and cor-rection	Assumed cause		Correction		Prevention
	When the OPC UA Server Use Option is set to *Do not use*, the rele-vant instruction was executed.		Set the OPC UA Server Use Option to *Use* and cycle the power supply to the Controller before executing the relevant instruction.		Set the OPC UA Server Use Option to *Use* and cycle the power supply to the Controller before executing the relevant instruction.
Attached infor-mation	Attached Information 1: Error Location Attached Information 2: Error Location Details (Rung Number). For a program section, the rung num-ber from the start of the section is given. For ST, the line number is given. Attached Information 3: Names of the Instruction and Instruction Instance Where the Error Occurred. If there is more than one possible instruction, information is given on all of them. Nothing is given If the instruction cannot be identified. Attached Information 4: Expansion Error Code (ErrorIDEx)				
Precau-tions/Remarks	If a program is changed after an error occurs, the attached information may not be correctly displayed.				

9-3   OPC UA Server-specific Troubleshooting

This section shows the problems, causes, corrections, related event logs, and Execution Logs for OPC UA server-specific troubleshooting.

Symptom	Cause 1	Cause 2	Correction	Related logs	
				Event log	Execution Log (Category, log code, and log name)
Cannot connect	The connection destination is incorrect.	The IP address is different.	Specify the same value as set for **OPC UA Server Settings - End point** for the URL.	---	---
	The connection destination is incorrect.	The communications port (PORT) number is incorrect.	Connect to the communications port 1 (PORT 1).	---	---
	The connection destination is incorrect.	The IP address has been changed by BOOTP.	Specify the same value as set for **OPC UA Server Settings - End point** for the URL.	Server Certificate Mismatch (15020000 hex)	Server Certificate Mismatch (CERT, 0004, Mismatch_Host)
	The connection destination is incorrect.	The port number is different or is duplicated with that of another communications service.	Specify the same value as set for **OPC UA Server Settings - End point** for the URL.	---	---
	The connection destination is incorrect.	The IP address has been changed by the Sysmac Studio, NetworkConfigurator, or instruction.	Change the connection setting of the OPC UA client with a correct IP address. Regenerate the server certificate manually in the Sysmac Studio. After that, export the server certificate and import it into the OPC UA client.	Server Certificate Mismatch (15020000 hex)	Server Certificate Mismatch (CERT, 0004, Mismatch_Host)
	The Ethernet/IP cable is not connected.	The cable is disconnected. A relay device is faulty, etc.	Check the network environment.	---	---
	OPC UA server setting error	The OPC UA server settings are corrupted.	Execute downloading using the Sysmac Studio.	OPC UA Server Setting Error (35D00000 hex)	OPC UA Server Error (SERVER, 0007, HaltError)

Symp-tom	Cause 1	Cause 2	Correction	Related logs	
				Event log	Execution Log (Category, log code, and log name)
Cannot connect (cont.)	The OPC UA Server Use setting is incorrect.	**OPC UA Server** of **OPC UA Server Settings** is set to *Do not use*.	Set **OPC UA Server** to *Use*.	---	---
	The OPC UA Server Use setting is incorrect.	The project is downloaded from a CPU Unit with an old version.	Replace the CPU Unit with one which supports OPC UA functionality and then transfer the project to the Controller.	---	---
	The OPC UA Server is in the *shutdown* state.	The OPCUA_Shutdown (Shutdown OPC UA Function) instruction was issued and then the OPC UA server was shut down from the Sysmac Studio.	Cycle the power supply to the Controller, or reset the Controller.	OPC UA Server Stopped (95D10000 hex)	OPC UA Server Shutdown (SERVER, 0006, Shutdown)
	The OPC UA Server is in the *Preparing* state.	The OPC UA function is being used during downloading, clearing all memory, or restoring.	Wait until the state of the OPC UA function becomes *Running* and then connect.	---	---
	The client certificate is invalid.	The client certificate or CA certificate is not registered in the Trusted Certificate List for client authentication.	Add the client certificate to the Trusted Certificate List. Add the CA certificate to the Trusted Certificate Lits for client authentication. Add the revoked certificate to the Certificate Revocation Lists for client authentication.	Client Connection Rejected (85600000 hex)	Application Authentication (AUTH, 0001, Application)
	The client certificate is invalid.	The client certificate is corrupted.	Set the correct client certificate for the OPC UA client.	Client Connection Rejected (85600000 hex)	Application Authentication (AUTH, 0001, Application)
	The client certificate is invalid.	The client certificate is not registered in the Trusted Certificate List for client authentication. Or the CA certificate is not registered in the Trusted Certificate List for client authentication or the Trusted Certificate List for issuer authentication.	Add the client certificate to the Trusted Certificate List for client authentication. Or add the CA certificate to the Trusted Certificate List for client authentication or the Trusted Certificate List for issuer authentication.	Client Connection Rejected (85600000 hex)	Application Authentication (AUTH, 0001, Application)

Symp-tom	Cause 1	Cause 2	Correction	Related logs	
				Event log	Execution Log (Category, log code, and log name)
Cannot con-nect (cont.)	The CA-signed client certifi-cate has been revoked.	The CA-signed client certificate has been revoked.	Update all CA certificate revocation lists up to the root certificate.	Client Connec-tion Rejected (85600000 hex)	Application Authentica-tion (AUTH, 0001, Applica-tion)
	The CA cer-tificate has been revoked	The CA certificate itself or the CA certifi-cates up to the root have been revoked.	Update all CA certificate revocation lists up to the root certificate.	Client Connec-tion Rejected (85600000 hex)	Application Authentica-tion (AUTH, 0001, Applica-tion)
	The server certificate is invalid.	The IP address spec-ified in the server cer-tificate does not match the IP address of the Controller.	Regenerate the server certifi-cate and install it on the OPC UA client.	Server Certifi-cate Mismatch (15020000 hex)	Server Certifi-cate Mismatch (CERT, 0004, Mis-match_Host)
	The server certificate is invalid.	The server certifi-cate has expired.	Set an appropriate server certificate expiration date and then regenerate the server certificate.	Server Certifi-cate Expired (35D10000 hex)	Server Certifi-cate Expired (CERT, 0003, Expired_-Server)
	Security pol-icy mis-match	The security policy set on the OPC UA client is outside of the allowable range of the server security policy.	Check the consistency of the security policies between the server and client. Add the security policy sup-ported by OPC UA client to the security policy settings of the server.	---	---
	Security pol-icy mis-match	The OPC UA client does not support the encryption method of the server certificate.	Check the consistency of the security policies between the server and client.	---	---
	Self-signed certificate acceptance rejected	The OPC UA client does not accept the self-signed certifi-cate of the OPC UA server.	Consult with the system administrator to make sure that the self-signed certificate is accepted.	---	---
	Server cer-tificate mis-match	The OPC UA server certificate was cleared when all memory was cleared.	Reinstall the server certifi-cate on the OPC UA client.	OPC UA Server Certifi-cate and OPC UA Security Profile Deleted (95D40000 hex)	Server Certifi-cate Updated (CERT, 0001, Update_-Sever)
	Server cer-tificate mis-match	The server certifi-cate has been regen-erated.	Reinstall the server certifi-cate on the OPC UA client.	---	Server Certifi-cate Updated (CERT, 0001, Update_-Sever)
	Error occurs when a ses-sion is cre-ated.	The number of sup-ported sessions is exceeded.	Make sure that more than five sessions are not created.	---	Application Authentication (AUTH, 0001, Application)

Symp-tom	Cause 1	Cause 2	Correction	Related logs	
				Event log	Execution Log (Category, log code, and log name)
Cannot con-nect (cont.)	Error occurs when a ses-sion is cre-ated.	The specified data encoding method is not supported by the OPC UA server.	Set **Data Encoding** of the OPC UA client to UA Binary.	---	---
	Error occurs when a ses-sion is cre-ated.	The specified trans-port protocol is not supported by the OPC UA server.	Set **Transport Protocol** of the OPC UA client to UA TCP.	---	---
	Error occurs when a ses-sion is cre-ated.	The user name or password entered on the OPC UA client does not match the corresponding authentication set-ting on the server.	Check the consistency of the user name and password between the server and cli-ent.	OPC UA Client Connection Rejected (85600000 hex)	User Authenti-cation (AUTH, 0002, User)
	Error occurs when a ses-sion is cre-ated.	The user of the OPC UA client is not regis-tered in the user authentication set-tings.	Set the user authentication settings correctly.	OPC UA Client Connection Rejected (85600000 hex)	User Authenti-cation (AUTH, 0002, User)
	Error occurs when a ses-sion is cre-ated.	The user authentica-tion settings have been changed.	Set the user authentication settings correctly.	OPC UA Client Connection Rejected (85600000 hex)	Security Set-tings Updated (AUTH, 0100, Update)
	Error occurs when a ses-sion is cre-ated.	The OPC UA client is requesting authenti-cation with user cer-tificate.	Select the *Permit* Option for **Anonymous login** in the **Security Settings** Dialog Box for the OPC UA Server. Or connect with the OPC UA client settings configured for user name and password authentication.	OPC UA Client Connection Rejected (85600000 hex)	Application Authentica-tion (AUTH, 0001, Applica-tion)
	Error occurs when a ses-sion is cre-ated.	The settings of the OPC UA server are set for user name and password authentication but the OPC UA client is requesting to connect anonymously.	Select the *Permit* Option for **Anonymous login** in the **Security Settings** Dialog Box for the OPC UA Server. Or connect with the OPC UA client settings configured for user name and password authentication.	OPC UA Client Connection Rejected (85600000 hex)	User Authenti-cation (AUTH, 0002, User)
	The client certificate cannot be moved to the Trusted Certificate List.	The maximum num-ber of client certifi-cates is already registered in the Trusted Certificate List.	More than 32 client certifi-cates cannot be registered in the Trusted Certificate List. Delete the client certificate of a client that is not connected and then add the client certif-icate to the Trusted Certifi-cate List.	---	---

Symp-tom	Cause 1	Cause 2	Correction	Related logs	
				Event log	Execution Log (Category, log code, and log name)
Cannot con-nect (cont.)	The client certificate cannot be moved as it is not included in the Rejected Certificate List.	The maximum num-ber of client certifi-cates is already registered in the Rejected Certificate List.	More than 32 client certifi-cates cannot be registered in the Rejected Certificate List. Delete unnecessary client cer-tificates from the Rejected Cer-tificate List to reconnect from the client. After the client certif-icate is added to the Rejected Certificate List, move it to the Trusted Certificate List.	Client Certifi-cate Discarded (95D30000 hex)	Certificate Discarded (CERT, 0102, Discard_Cli-ent)
A vari-able can-not be viewed from an OPC UA client.	A global vari-able of the CPU Unit is not displayed correctly on the OPC UA client.	The publish attribute of the global variable is set to *Do not pub-lish*.	Set the publish attribute of the global variable of the CPU Unit to *Publish Only*, *Input*, or *Output*.	---	---
	A sys-tem-defined variable of the CPU Unit is not displayed correctly on the OPC UA client.	---	A system-defined variable cannot be published. Copy it to a network-pub-lished variable in a user pro-gram.	---	---
	A global variable of the CPU Unit is not displayed correctly on the OPC UA client.	The variable is a vari-able that cannot be published.	The following variables can-not be published by the OPC UA Server. Change the variable to a data type that can be published with the OPC UA Server. - Multidimensional array specified structure - Structure containing multi-dimensional array(s) as member(s) - Structure whose nesting number exceeds the limit value. - Union - Array whose start number is not 0 - Variable whose size exceeds the limit value - Array whose number of elements exceeds the limit value - Structure whose number of members exceeds the limit value	Unsupported Data Type (35D40000 hex)	Variable Including Unsupported Data Type (SERVER, 0101, Invalid-DataType)

Symptom	Cause 1	Cause 2	Correction	Related logs	
				Event log	Execution Log (Category, log code, and log name)
A variable cannot be viewed from an OPC UA client. (cont.)	No node for structure member.	The structure member cannot be deployed.	Refer to the value attributes for details on the members of structure variables.	---	---
	A variable of the CPU Unit is not displayed correctly on the OPC UA client.	The number of variables that can be published is exceeded.	Set the number of public variables of the OPC UA Server to no more than the upper limit. Set the publish attribute of any global variable for which network publishing is not necessary to *Do not publish*.	Too Many Public Variables (35D30000 hex)	Maximum Number of Variables That Can Be Published Is Exceeded (SERVER, 0100, Max-Variables)
	A variable of the CPU Unit is not displayed correctly on the OPC UA client.	The maximum number of value attributes that can be published is exceeded.	Make sure that the number of public attributes for the OPC UA Server does not exceed the upper limit. Set *Do not publish* for global variables which do not need to be published	Too Many Public Value Attributes (35D50000 hex)	Maximum Number of Variables That Can Be Published Is Exceeded (SERVER, 0100, Max-Variables)
	A variable of the CPU Unit is not displayed correctly on the OPC UA client.	The maximum number of structure definitions that can be published is exceeded.	Make sure that the number of structure definitions that can be published for the OPC UA Server does not exceed the upper limit.	Too Many Structure Definitions (35D60000 hex)	Maximum Number of Variables That Can Be Published Is Exceeded (SERVER, 0100, Max-Variables)
A variable cannot be read or written.	Read/write error	The variable is not published to OPC UA.	Set the publish attribute of the variable to *Publish Only*, *Input*, or *Output*.	---	---
	Read/write error	OPC UA is in a shutdown state.	Cycle the power supply to the Controller, or reset the Controller.	OPC UA Server Stopped (95D10000 hex)	OPC UA Server Shutdown (SERVER, 0006, Shutdown)
	Read/write error	OPC UA is in the *Preparing* state.	Read/write after the state becomes *Running*.	---	---
	Read/write error	The variable cannot be accessed because an element in its array is specified.	Specify the entire array.	---	---
	Read/write error	The variable cannot be accessed because its structure member is specified.	Specify the entire structure.	---	---

Symp-tom	Cause 1	Cause 2	Correction	Related logs	
				Event log	Execution Log (Category, log code, and log name)
A variable cannot be read or written. (cont.)	Read/write error	The EtherNet/IP cable has become disconnected, communications has been cut off, or other communications failure has occurred.	Check the network environment.	---	Application Authentication (AUTH, 0001, Application)
The subscription settings cannot be configured.	Subscription error	The maximum value for subscriptions is exceeded.	Make sure that the number of OPC UA subscriptions does not exceed 100.	---	---
	Subscription error	The maximum value for MoniterdItem is exceeded.	Make sure that the number of OPC UA client MoniterdItems does not exceed 2,000.	---	---
	Subscription error	OPC UA is in a shut-down state.	Cycle the power supply to the Controller, or reset the Controller and then execute.	OPC UA Server Stopped (95D10000 hex)	OPC UA Server Shutdown (SERVER, 0006, Shutdown)
	Subscription error	OPC UA is in the *Preparing* state.	Execute after the state becomes *Running*.	---	---
	Subscription error	The EtherNet/IP cable has become disconnected, communications has been cut off, or other communications failure has occurred.	Check the network environment.	---	Connection from OPC UA client (AUTH, 0001, Application)
Execution logs are not recorded.	An SD card is not inserted.	An SD card is not inserted correctly in the CPU Unit. - The SD card is damaged. - The SD card is not supported. - The SD card is not formatted.	Insert an SD Memory Card into the CPU Unit correctly.	Execution Log Save Failed (15000000 hex)	---
	SD card is write-protected	The write protection switch of the SD card is set to the *write-protected* position.	Change the position of the write protection switch of the SD card to enable writing.	Execution Log Save Failed (15000000 hex)	---
	The settings are incorrect.	The *Do not record* Option is selected for **Execution Log** in the **OPC UA Server Settings** Tab Page.	Select the *Record* Option for **Execution Log** in the **OPC UA Server Settings** Tab Page.	---	---

*1. Refer to *9-2 Troubleshooting* on page 9-7 for details on the event logs.

*2. Refer to *Section 7 Execution Log Functions* for details on execution logs.

A

A

Appendices

This section describes the error confirmation methods and corrections for errors that can occur with the OPC UA Server.

A-1 Task Design Procedure

This section describes the task design procedure for the OPC UA Server.

Refer to the *NJ/NX-series CPU Unit Software User's Manual* (Cat. No. W501) for the task and system service operation specifications of the NJ/NX-series Controllers.

A-1-1 Startup Time of the OPC UA Server (Reference Values)

The time required to get the OPC UA Server ready for operation after turning on the power of the CPU Unit (hereinafter called "startup time") varies depending on the number of network-published variables and the task execution time ratio.

The following graphs show reference values given when the data type of all network-published variables is INT type.

Please design your system by reference to these graphs.

NJ501-1□00

● **Change in Startup Time Depending on Number of Network-published Variables**
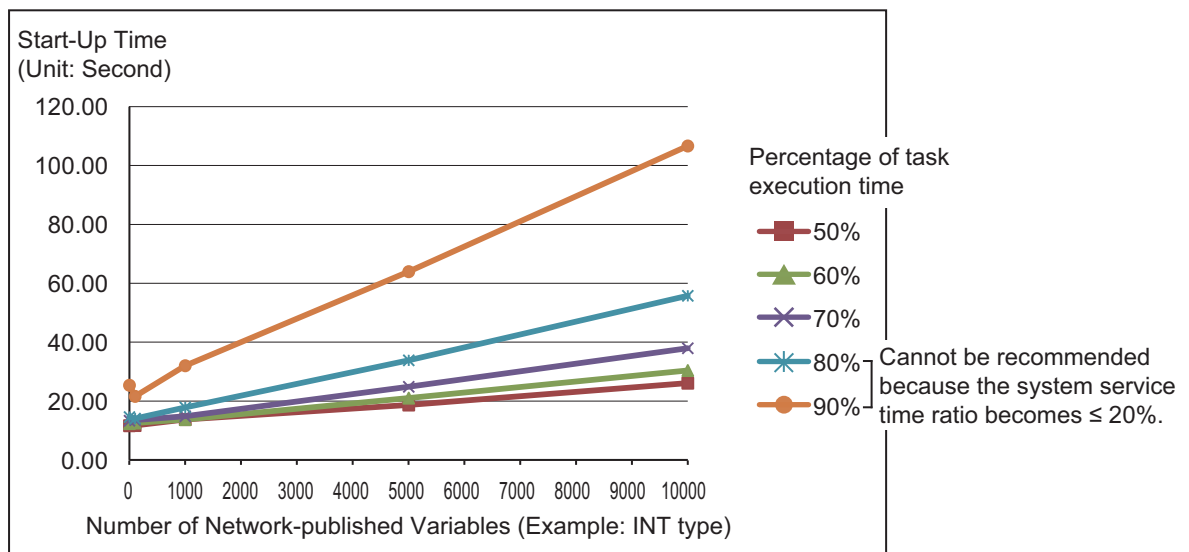
● **Change in Startup Time Depending on Task Execution Time Ratio**

Start-Up Time (Unit: Second)

Number of Network-published Variables (Example: INT type)
- 0
- 100
- 1000
- 5000
- 10000

Percentage of task execution time
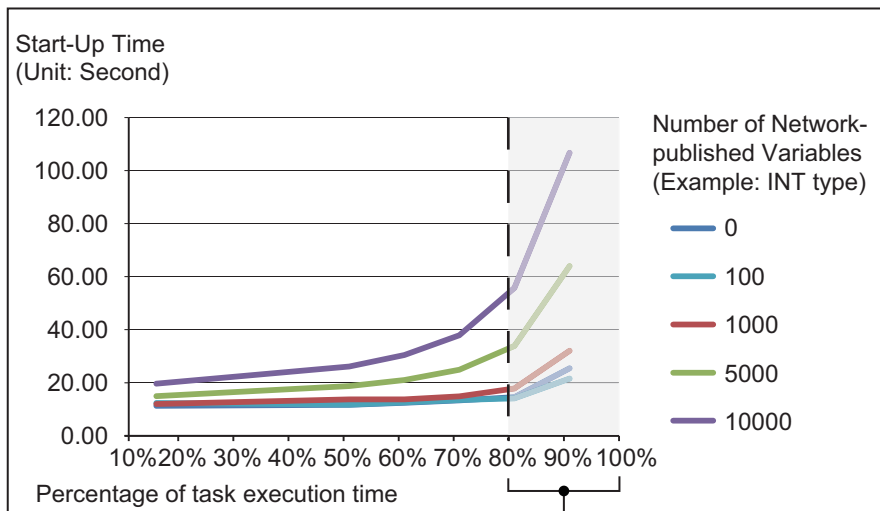
Cannot be recommended because the system service time ratio becomes ≤ 20%.

NX102-□□□□

● **Change in Startup Time Depending on Number of Network-published Variables**

Start-Up Time (Unit: Second)

Number of Network-published Variables (Example: INT type)
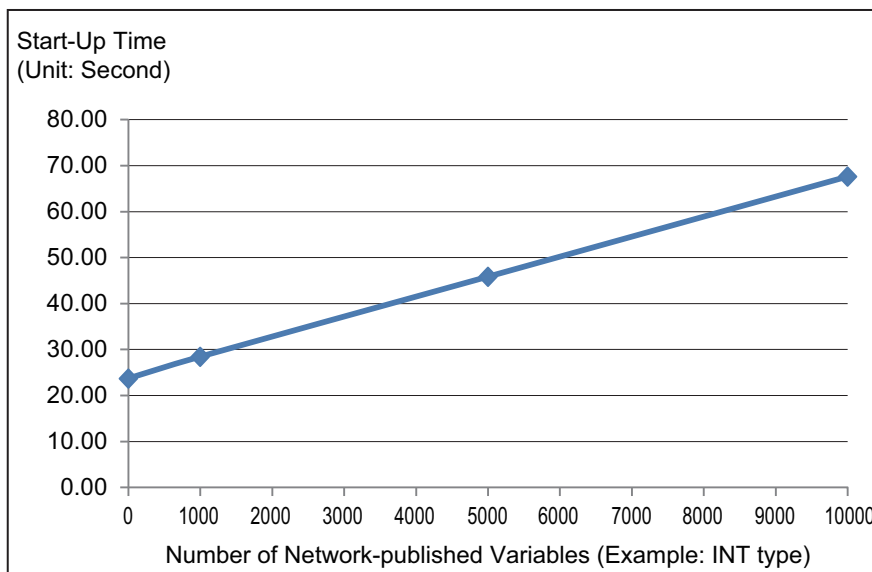
📝 **Precautions for Correct Use**

The OPC UA Server is executed as a system service.

Accordingly, if other system services are executed while the OPC UA Server is starting up, they may take longer.

A-1-2 Guidelines for System Service Execution Time Ratio

The OPC UA Server is executed as a system service.

When the OPC UA Server is used, the OPC UA Server executes the processing as a system service.

The method of executing the system service depends on the CPU Unit model.

● NJ501-1□00

For NJ501-1□00, if sufficient system service execution time cannot be secured, the OPC UA Server may be slow in responding to requests from OPC UA clients, including reading/writing variables.

As a target to perform a satisfactory level of response to requests from OPC UA clients, design tasks to make sure that the system service execution time ratio exceeds 20%.

Precautions for Safe Use

The system service execution time ratio (CPU usage) of 20% or greater is just a numerical target. The appropriate system service execution time ratio depends on the CPU usage of other services executed on the system.

Before starting actual operation, you must test performance under all foreseeable conditions on the actual system and make sure that the OPC UA Server operates with appropriate system service execution time.

Precautions for Correct Use

- If the system service execution time ratio is reduced, operation failures or communications errors may occur when each operation is executed from the Sysmac Studio. If an operation failure or communications error occurs when you execute an operation from the Sysmac Studio, retry the operation after doing the following:
  - Check the cable connections.
  - Check the communications settings.
  - Increase the response monitoring time in the communications settings.
  - Start up in safe mode.
  - If the Sysmac Studio cannot go online, refer to the *NJ/NX-series Troubleshooting Manual* (Cat. No. W503).
- If the time set for system service monitoring cannot be secured for system services, an *Insufficient System Service Time Error* will occur. The error is classified as a major fault level Controller error. When the error occurs, user programs will be stopped. Set the System Service Monitoring Settings to the minimum values that are required to meet the response performance of the system services so that sufficient time can be allocated to the system services and task execution. The System Service Monitoring Settings are used to monitor whether the specified system service execution time can be obtained. System services will not necessarily be executed for the specified time.
- The system service execution time is affected by task execution time and tag data links. Refer to the *NJ/NX-series CPU Unit Software User's Manual* (Cat. No. W501) for details of task specifications, tag data link service, and system services.

● NX102-□□□□

For NX102-□□□□, the system services are executed without being affected by the tasks. However, during execution of the tag data link service, system services are not executed.

A-1-3 Checking the System Service Execution Time Ratio

When you design tasks, confirm that sufficient execution time can be allocated to system services by the following methods.

● Desktop Calculation

This is an example for a project that consists of one primary periodic task.

Refer to the *NJ/NX-series CPU Unit Software User's Manual* (Cat. No. W501) to make a rough estimate of the *average task execution time* on paper.

- For NJ501-1□00

Average task execution time < Task period x 0.8

Design the task based on the above calculation.

● Calculating with the Simulator in the Sysmac Studio

Check the value of *Estimated CPU usage rate* with the *Task Execution Time Monitor* for the Simulator on the Sysmac Studio.

Refer to the *NJ/NX-series CPU Unit Software User's Manual* (Cat. No. W501) for the procedure to check the operation on the Simulator.

- For NJ501-1□00

Estimated CPU usage rate - System service execution time ratio < 80%

Design the task based on the above calculation.

The *Estimated CPU usage rate* shows how much of the task period is used by the total of the maximum estimated task processing time, the tag data link service execution time ratio, and the system service processing time.

The value obtained by subtracting the *System service execution time ratio* from the *Estimated CPU usage rate* is the percentage for the execution time of processing other than system services.
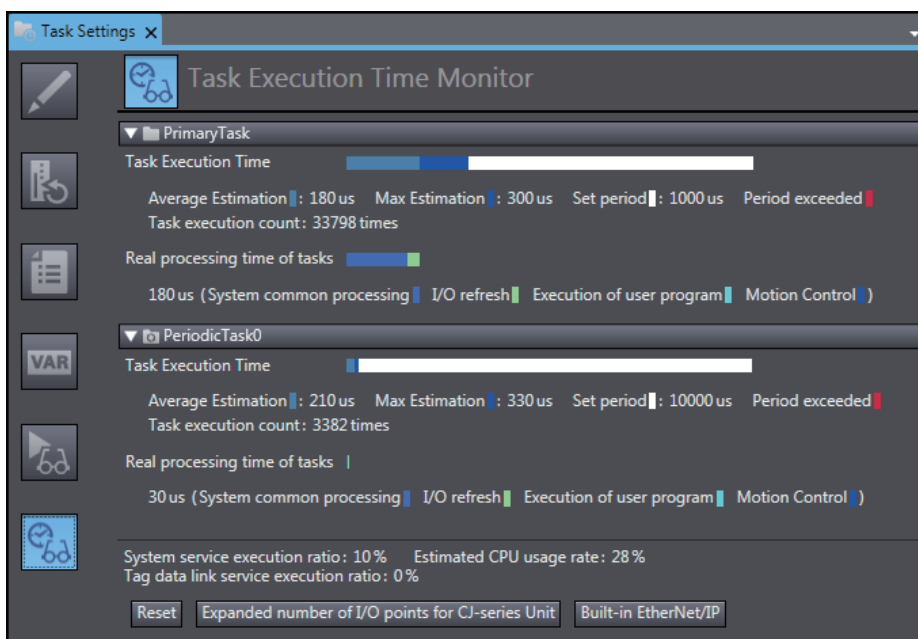
● **Calculating Times on the Actual Controller**

When the project consists of one primary periodic task, check the *average task execution time* using the *Task Execution Time Monitor function* on the Sysmac Studio connected online with the actual Controller.

• For NJ501□00

Average task execution time < *Task period* x 0.8

Design the task based on the above calculation.

When the project consists of multiple tasks, test the performance under all foreseeable conditions using the actual Controller to make sure that the OPC UA clients operate within the appropriate execution time.

A-2 OPC UA Instruction

This section describes the OPC UA instructions.

Refer to the *NJ/NX-series Instructions Reference Manual* (Cat. No. W502) for details on the variables common to the NJ/NX-series instructions.

A-2-1 OPCUA_Shutdown (Shutdown OPC UA Function)

The OPCUA_Shutdown (Shutdown OPC UA Function) instruction requests the termination of the OPC UA functions so that the controller power supply can be safely turned OFF.

Instruction	Name	FB/FUN	Graphic expression	ST expression
OPCUA_Shutdown	Shutdown OPC UA Server	FB	OPCUA_Shutdown_instance OPCUA_Shutdown Execute — — Done — Busy — Error — ErrorID	OPCUA_Shutdown_instance (Execute, Done, Busy, Error, ErrorID);

Note The OPCUA_Shutdown_instance is an instance of OPCUA_Shutdown (Shutdown OPC UA Function) instruction, which is declared as a variable.

A-2-2 Variables

Input Variables

Input variable	Meaning	Data type	Valid range	Unit	Default	Description
Execute	Execute	BOOL	TRUE or FALSE	---	FALSE	Specify the execution condition.

Output Variables

Output variable	Meaning	Data type	Valid range	Unit	Description
Done	Done	BOOL	TRUE or FALSE	---	TRUE when the instruction is normally completed.
Busy	Executing	BOOL	TRUE or FALSE	---	TRUE when the instruction is being executed.
Error	Error	BOOL	TRUE or FALSE	---	TRUE when the instruction is terminated due to an error.
ErrorID	Error Code	WORD	16#0000 to 16#FFFF	---	Contains the error code when an error occurs.

A-2-3   Related System-defined Variables

None

A-2-4   Related Error Codes

Error code	Error name	Description
16# 041D	Too Many Instructions Executed at the Same Time	More than 32 OPC UA instructions were executed at the same time.
16# 5000	OPC UA Server Shutdown or Shutting Down	The instruction was executed after the OPC UA Server was shut down or while the OPC UA Server was being shut down.
16# 5001	OPC UA Server Being Initialized	The instruction cannot be executed because the OPC UA Server is being initialized.
16# 5002	OPC UA Server Not Started	While the *Do not use* Option was selected for the OPC UA Server, the instruction was executed after a power-on or reset of the controller.

For details on errors, refer to *Errors Related to the OPC UA Server* in *9-2-2 OPC UA Server Error Description* on page 9-11.

A-2-5   Function

The OPCUA_Shutdown (Shutdown OPC UA Function) instruction requests the shutdown of the OPC UA Server so that the controller power supply can be safely turned OFF.

At this time, in order to set the OPC UA Server to the shutdown state, record *OPC UA server shutdown completed* in the Execution Log, and stop access to the SD memory card.

Before turning OFF the power supply to the controller, make sure this instruction has terminated normally (the value of *Done* has changed to TRUE).

This instruction operates separately from the function of accessing the SD Memory Card for other instructions. If other than the OPC UA Server accesses the SD memory card during the execution of this instruction, this instruction will be executed asynchronously with respect to the SD memory card access, and therefore, the processing order will be optional.

A-2-6   Precautions for Correct Use

• Execution of this instruction is continued until processing is completed even if the value of *Execute* changes to FALSE or the execution time exceeds the task period. You can confirm that the processing normally ends by checking that the value of *Done* has changed to TRUE.

• Refer to *Using this Section* of the *NJ/NX-series Instructions Reference Manual* (Cat. No. W502) for a timing chart for *Execute*, *Done*, *Busy*, and *Error*.

• This instruction cannot be used on an event task. A compiling error will occur.

• OPC UA instructions cannot be executed during and after execution of this instruction. The execution of an OPC UA instruction will result in an error.

• Before turning OFF the power supply to the system, make sure this instruction has terminated normally by confirming that the value of *Done* has changed to TRUE.

• If the power supply is turned OFF without executing this instruction, the Execution Log will not be saved correctly.

A-2-7 Additional Information

If this instruction is executed on the simulator, no processing is performed, and the output variables are as shown below.

Output variable	Meaning	Data type	Execution results
Done	Done	BOOL	TRUE
Busy	Executing	BOOL	FALSE
Error	Error	BOOL	FALSE
ErrorID	Error Code	WORD	16#0000

A-2-8 Sample Programming

This section gives sample programming for shutting down the OPC UA Server when the trigger variable changes to TRUE.

Ladder Diagram

● **Main Variables**

Name	Data type	Initial value	Comment
OPCUA_Shutdown_instance	OPCUA_Shutdown	---	Instance of OPCUA_Shutdown (Shutdown OPC UA Function) instruction.
Trigger	BOOL	FALSE	Variable used as a trigger for shutting down the OPC UA Server.
Shutdown_OK	BOOL	FALSE	This variable changes to TRUE when the OPCUA_Shutdown (Shutdown OPC UA Function) instruction terminates normally.

● **Sample Programming**

• Shutdown the OPC UA Server.

Shutdown the OPC UA server by setting Trigger to TRUE.
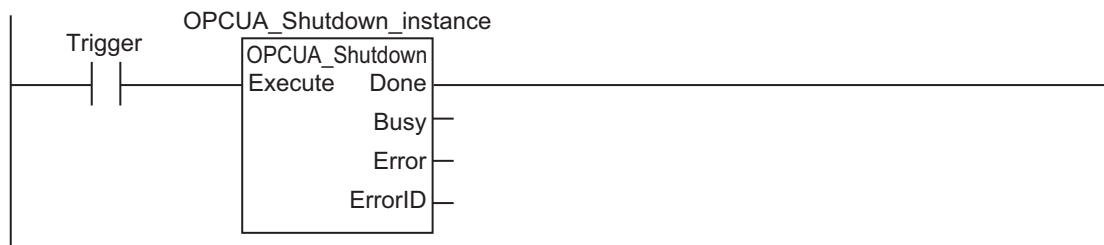
When the instruction is normally completed, the Shutdown_OK variable is changed to TRUE.

Structured Text (ST)

● Main Variables

Name	Data type	Initial value	Comment
OPCUA_Shutdown_instance	OPCUA_Shutdown	---	Instance of OPCUA_Shutdown (Shutdown OPC UA Function) instruction.
Trigger	BOOL	FALSE	Variable used as a trigger for shutting down the OPC UA Server.
LastTrigger	BOOL	FALSE	Variable to retain the trigger status of the previous execution.
Operating	BOOL	FALSE	The OPC UA Server is shutdown when this variable is TRUE.
OperatingStart	BOOL	FALSE	The initialization processing is executed when this variable is TRUE.
ShutdownOK	BOOL	FALSE	This variable changes to TRUE when the OPCUA_Shutdown (Shutdown OPC UA Function) instruction terminates normally.

● Sample Programming

```
(*------------------------------------------------------------------------------
    ◆Shutdown the OPC UA Server.
-------------------------------------------------------------------------------*)

// Start the sequence when the variable Trigger changes to TRUE.
IF ( (Trigger=TRUE) AND (LastTrigger=FALSE) ) THEN
    OperatingStart := TRUE;
    Operating := TRUE;
END_IF;
LastTrigger := Trigger;

// Sequence start processing
IF (OperatingStart=TRUE) THEN
    // Initialize the instruction instance.
    OPCUA_Shutdown_instance( Execute:=FALSE );

    OperatingStart := FALSE;
END_IF;

IF (Operating=TRUE) THEN
    // Shutdown OPC UA Server
    OPCUA_Shutdown_instance( Execute:=TRUE );

IF (OPCUA_Shutdown_instance.Done=TRUE) THEN
    // Normal end processing
    ShutdownOK := TRUE;
    Operating := FALSE;
  END_IF;
  IF (OPCUA_Shutdown_instance.Error=TRUE) THEN
    // Processing after error end
    Operating := FALSE;
  END_IF;
END_IF;
```

A-3 When CA-signed Client Certificates Supported

This Appendix describes an overview and settings of a CA-signed client certificate, as well as how to operate a CA-signed client certificate on the Sysmac Studio.

A-3-1 Overview

For a CA-signed client certificate, you must make the settings from the **Client Authentication** Tab Page and the **Issuer Authentication** Tab Page in the OPC UA settings (online) from the Sysmac Studio.

The internal mechanism of the CPU Unit is as shown below.

Note that both the CA-signed client certificate and the self-signed client certificate can also be used together [1].

[1]. Shown by a dotted line in the following diagram.
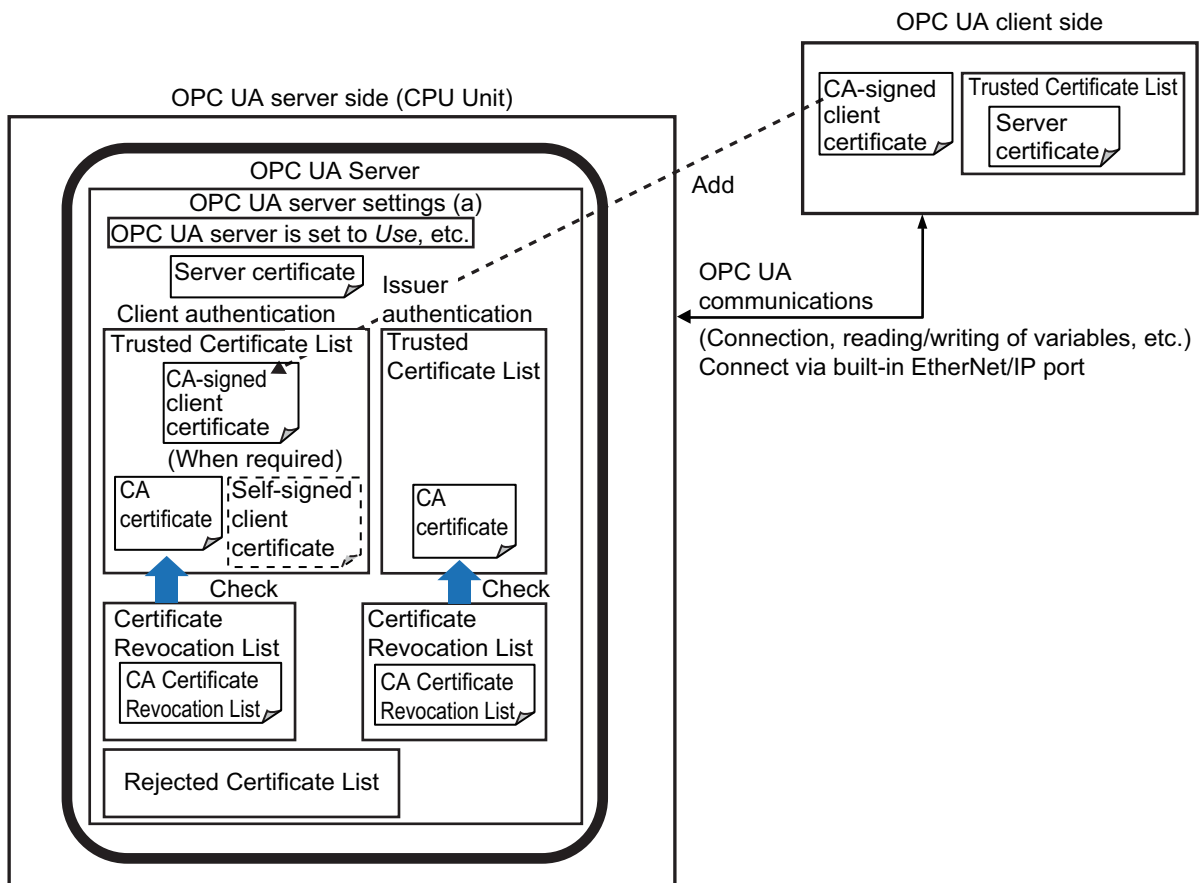
The CA Certificate Revocation List is a list in which issued client certificates are registered when they are revoked before the expiry of the valid period.

If a client certificate is registered in the CA Certificate Revocation List, the connection from the corresponding client certificate fails, and the client certificate is registered in the Rejected Certificate list.

A-3-2 Settings

For a CA-signed client certificate, you must make the following settings in the OPC UA settings (online) from the Sysmac Studio.

The certificates that must be registered differ depending on the authentication means and the type of CA certificate.

Authentication means of CA-signed client certificate	Type of corresponding CA certificate a	OPC UA settings (online)			
		Client Authentication Tab Page		Issuer Authentication Tab Page	
		Trusted certificate	Certificate Revocation List	Trusted certificate	Certificate Revocation List
When authentication is performed only by the CA certificate (CA Certificate a) that signs the client certificate	A root certificate	Register only the CA certificate a	Register the revocation list containing the CA certificate a	Registration not required	Registration not required
	An intermediate certificate			Register all CA certificates up to the root certificate	Register the group of revocation lists containing all CA certificates specified on the left
When authentication is performed by the client certificate (Client Certificate b) and the CA certificate (CA Certificate a) that signs the client certificate	A root certificate	Register both certificates below: • Corresponding client certificate b • Corresponding CA certificate a	Register the revocation list containing the CA certificate a	Registration not required	Registration not required
	An intermediate certificate			Register all CA certificates up to the root certificate, except the CA certificate a	Register the group of revocation lists containing all CA certificates specified on the left
	Or				
	A root certificate	Register only the client certificate b	Registration not required	Register the root certificate	Register the revocation list containing the root certificate
	An intermediate certificate		Registration not required	Register all CA certificates up to the root certificate including the CA certificate a	Register the group of revocation lists containing all CA certificates specified on the left

A-3-3 Related Operations Performed from OPC UA Settings in the Sysmac Studio

For a CA-signed client certificate, make the following settings from **Client Authentication** and **Issuer Authentication** in the **OPC UA Settings** of the Sysmac Studio.

Client Authentication

Display and perform client authentication for a CPU Unit connected online.

1 Place the Sysmac Studio online with the CPU Unit, right-click **OPC UA Server Settings** under **Configurations and Setup** - **OPC UA Settings** in the Multiview Explorer, and then select **Client Authentication**.
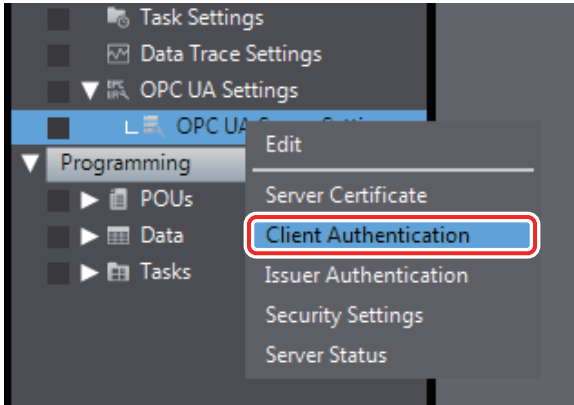
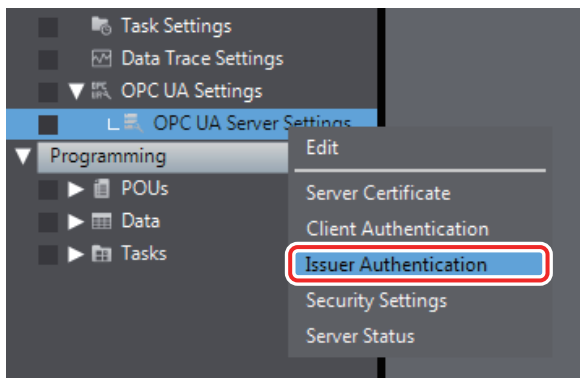The following **Client Authentication** Tab Page appears.

(A) Trusted Certificate List

(B) Certificate Revocation List

(C) **Update** Button

The following information is displayed.

Item	Description
(A) Trusted Certificate List	The Trusted Client Certificate List in the CPU Unit is displayed. • Common name, expiration of validity period, organization, domain name are displayed. • The default display order is ascending order of common names. You can sort the list by the name of each item by clicking each column header. Ascending and descending order are switched each time you click. • **Add** Button (+): Adds the certificate selected in the **Add Certificate** Dialog Box to the Trusted Certificate List in the CPU Unit. • **Delete** Button (🗑): Deletes the selected certificate from the Trusted Certificate List in the CPU Unit.
(B) Certificate Revocation List	The Certificate Revocation List in the CPU Unit is displayed. • The File Name, Issuer, Effective Start Date, and Next Update Date are displayed. • The default display order is the ascending order of the file name. You can sort the list by the name of each item by clicking each column header. Ascending and descending order are switched each time you click. • **Add** Button (+): Adds the certificate selected in the **Add Certificate** Dialog Box to the Trusted Certificate List in the CPU Unit. • **Delete** Button (🗑): Deletes the selected certificate from the Trusted Certificate List in the CPU Unit.
(C) **Update** Button	The display in the **Client Authentication** Tab Page is updated with the data in the CPU Unit.

Issuer Authentication

Perform display and operations of issuer authentication in the CPU Unit placed online.

1 Place the Sysmac Studio online with the CPU Unit, right-click **OPC UA Server Settings** under **Configurations and Setup** - **OPC UA Settings** in the Multiview Explorer, and then select **Issuer Authentication**.

The following **Issuer Authentication** Tab Page is displayed.

The following information is displayed.

Item	Description
(A) Trusted Certificate List	The Trusted CA Certificate List in the CPU Unit is displayed. • Common name, expiration of validity period, organization, domain name are displayed. • The default display order is ascending order of common names. You can sort the list by the name of each item by clicking each column header. Ascending and descending order are switched each time you click.
	• **Add** Button (+): Adds the certificate selected in the **Add Certificate** Dialog Box to the Trusted Certificate List in the CPU Unit. • **Delete** Button (🗑): Deletes the selected certificate from the Trusted Certificate List in the CPU Unit.
(B) Certificate Revocation List	The Certificate Revocation List in the CPU Unit is displayed. • The File Name, Issuer, Effective Start Date, and Next Update Date are displayed. • The default display order is the ascending order of the file name. You can sort the list by the name of each item by clicking each column header. Ascending and descending order are switched each time you click. • **Add** Button (+): Adds the certificate selected in the **Add Certificate** Dialog Box to the Trusted Certificate List in the CPU Unit. • **Delete** Button (🗑): Deletes the selected certificate from the Trusted Certificate List in the CPU Unit.
(C) **Update** Button	The display in the **Issuer Authentication** Tab Page is updated with the data in the CPU Unit.

A-4 List of Related System-defined Variables

This section lists the system-defined variables related to the OPC UA Server.

A-4-1 System-defined Variables for the Overall NJ/NX-series Controller (No Category)

● **Functional Classification: SD Memory Card Related**

Variable name	Name	Function	Data type	Range of values
_Card1RestoreCmd TargetOpcuaSPF	OPC UA Security Profile Transfer Flag	When restoring *OPC UA security profile* in the SD Memory Card to the Controller, set this to TRUE.	BOOL	TRUE, FALSE

A-5   Version Information

This section describes the relationship between unit versions of CPU Units, OPC UA standard versions, and the Sysmac Studio versions.

A-5-1   Relationship between Unit Versions and OPC UA Standard Versions

The following table gives the relationship between the unit versions of CPU Units and OPC UA standard versions.

CPU Unit model	Unit version of CPU Unit	OPC UA standard version
NJ501-1300 NJ501-1400 NJ501-1500	Ver.1.17	Ver.1.02
NX102-9000 NX102-1000 NX102-1100 NX102-1200	Ver.1.30	Ver.1.02

A-5-2   Relationship between Unit Versions and the Sysmac Studio Versions

The following table gives the relationship between the unit versions of CPU Units and the Sysmac Studio versions.

Unit Versions and the Corresponding Sysmac Studio Versions

This following table gives the relationship between the unit versions of CPU Units and the corresponding Sysmac Studio versions.

CPU Unit model	Unit version of CPU Unit	Corresponding version of the Sysmac Studio
NJ501-1300 NJ501-1400 NJ501-1500	Ver.1.17 or later	Ver.1.21 or higher
NX102-9000 NX102-1000 NX102-1100 NX102-1200	Ver.1.30 or later	Ver.1.23 or higher

Index

Index

U

V

I

OMRON Corporation   **Industrial Automation Company**

Kyoto, JAPAN

Contact: www.ia.omron.com

Regional Headquarters
OMRON EUROPE B.V.
Wegalaan 67-69, 2132 JD Hoofddorp
The Netherlands
Tel: (31)2356-81-300/Fax: (31)2356-81-388

OMRON ELECTRONICS LLC
2895 Greenspoint Parkway, Suite 200
Hoffman Estates, IL 60169 U.S.A.
Tel: (1) 847-843-7900/Fax: (1) 847-843-7787

OMRON ASIA PACIFIC PTE. LTD.
No. 438A Alexandra Road # 05-05/08 (Lobby 2),
Alexandra Technopark,
Singapore 119967
Tel: (65) 6835-3011/Fax: (65) 6835-2711

OMRON (CHINA) CO., LTD.
Room 2211, Bank of China Tower,
200 Yin Cheng Zhong Road,
PuDong New Area, Shanghai, 200120, China
Tel: (86) 21-5037-2222/Fax: (86) 21-5037-2200

Authorized Distributor:

Cat. No. W588-E1-03   0719