

Programmable Controller KV-8000 Series

OPC UA Server Function User's Manual

Read this manual before using the product.
Keep this manual in a safe place for later reference.

Chapter 1	Overview of the OPC UA Server Function
Chapter 2	OPC UA Server and CPU Unit Settings
Chapter 3	Security Feature
Chapter 4	Settings for OPC UA Communication
Chapter 5	Monitoring Feature
Chapter 6	Connecting from the OPC UA Client and Reading and Writing Variables

• CA-signed Client Certificates

Preface

This manual describes the features related to OPC UA communications on the "KV-8000(A)" and how to use them.

Be sure to thoroughly read and fully understand this manual before installing. In addition, store this manual in a safe place so that you can retrieve it whenever necessary.

Related manuals

All the following PDF manuals can be found and opened in the help file of KV STUDIO. The latest version of PDF manuals can be downloaded from the Keyence web site.

Name	Description
KV-8000 OPC UA Server function User's Manual	This manual. It describes how to use the OPC UA communications features on the "KV-8000 Series".
KV-8000 Series User's Manual	Explains the system configuration, specifications, and methods for creating ladder programs for the "KV-8000 series".
KV STUDIO User's Manual	Explains the operation methods for "KV STUDIO".
KV Series EtherNet/IP Function User's Manual	Explains connections/specifications, and methods for creating ladder programs for the "EtherNet/IP functions built into the CPU unit".
KV-8000/7000/5500/5000/3000/1000 Series KV Nano Series Instructional Reference Manual	Explains each instruction that can be used in ladder programming.
KV-8000 Series ST Language Programming Manual	This document describes how to create an ST language program and the Operators, Control Statements, and Functions that can be used.
KV-8000/7000/5500/5000/3000/1000 Series KV Nano Series Script Programming Manual	Explains the script program creation method and possible operators, control statements, and functions.

About KV-8000(A) CPU Function Version

The functions of the KV-8000 Series differ depending on the CPU function version.

The CPU function version can be checked from "Tools" → "Check CPU Function Version" → "PLC" in the KV STUDIO menu (* KV STUDIO Ver.11.1 or later is required).

In addition, the CPU function version can be updated from "Tools" → "Check CPU Function Version" → "PLC" → "System Program Update" in the KV STUDIO menu.

(* KV STUDIO Ver.11.1 or later is required.)








Differences in CPU function by CPU function version

Release	2023/3	2022/6	2021/11
CPU function version	2.602	2.5	2.3
Maximum number of public network variables	200,000	200,000	10,000
Number of sessions	20	8	8





Safety information

Symbols

The following symbols alert you to important messages. Be sure to read these messages carefully.

	Indicates a hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.
	Indicates a situation which, if not avoided, could result in product damage as well as property damage.
	Indicates cautions and limitations that must be followed during operation.
	Indicates additional information on proper operation.
	Indicates tips for better understanding or useful information.

General Precautions

	<ul style="list-style-type: none"> Do not use the device with the purpose of protecting human beings. This device is not intended for use as an explosion-proof product. Do not use this device in a hazardous location or in a location that has a potentially explosive atmosphere. Do not use this product in an application that may cause death, serious injury or serious property damage due to a failure with this product should occur, such as nuclear power plants, on aircraft, trains, ships, or vehicles, used within medical equipment, playground equipment, roller coasters and other rides, etc.
	<ul style="list-style-type: none"> Output circuit and internal circuit malfunctions sometimes prevent control from being performed normally. Be sure to provide a safety circuit in control systems where circuit malfunctions may lead to fire or other serious accidents. Provide a safety circuit that bypasses the PLC to enable failsafe operation of the entire system in the event that the PLC fails. You must perform a sufficient risk assessment for the machine where this product is to be installed prior to installing this product. Provide appropriate protective fail-safe measures on the machine independent from this product in case a failure with this product should occur.
	<ul style="list-style-type: none"> Before you use this device, verify its functionality and performance at startup and during operation. If the equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.
	<ul style="list-style-type: none"> Proceed with care when modifying the device, or when using it in a manner that falls outside of the ranges indicated in its specifications, since KEYENCE is unable to guarantee device functionality or performance in such situations. Use this device in combination with other devices only after careful consideration, since the device may fail to satisfy its functionality and performance capabilities as a result of factors such as its usage conditions and the environment in which it is used.

CE and UKCA Marking/UL Standards

For restrictions related to CE and UKCA Marking, and restrictions to comply with UL Standards, see the "KV-8000" Instruction Manual.

How to Use This Manual

This section describes the terminology/symbols used in this manual.


Terminology

The following terminologies are used for descriptions except for some contents in this manual.

Terminology	Description
CPU Unit	This refers to KEYENCE "KV-8000(A)" programmable controllers.
KV-8000(A)	It may represent CPU unit "KV-8000" only, or the generic name of "KV-8000(A)".
Expansion unit	This refers to the I/O expansion unit and special expansion unit other than the CPU unit.
PLC	This refers to the Programmable Logic Controller.
"KV STUDIO"	"KV STUDIO" Ladder Support Software
Ladder program	The program made with Ladder Support Software.
OPC UA	This is an international standard created by the OPC Foundation. It is an industrial communications protocol designed to transmit data safely with a high level of trust.
OPC UA server	Refers to an application that uses OPC UA to transmit data. In this manual, the "KV-8000(A)" functions as an OPC UA server and reads and writes variable values.
OPC UA client	Refers to an application that connects to the OPC UA server and requests that data be read and written.
Endpoint URL	This is a physical OPC UA server address required for OPC UA client access. Format: opc.tcp:// [IP address] : [Port No.] Example: opc.tcp://192.168.0.10:4840
Application authentication	Refers to the process in which the OPC UA server and OPC UA client exchange electronic certificates to authenticate each other.
User authentication	Refers to the process in which the OPC UA server authenticates an OPC UA client using a user name and password.
Server certificate	An electronic certificate used to prove the identity of the OPC UA server when application authentication is performed. Identity is proven by registering the server certificate on the OPC UA client.
Client certificate	An electronic certificate used to prove the identity of the OPC UA client when application authentication is performed. Identity is proven by registering the client certificate on the OPC UA server.
CA (Certification Authority)	This is an entity that issues and revokes digital certificates.
Private key	This is used in tandem with certificates to prevent identity theft. If it is lost, the certificate must be reissued. It must be stored in such a way that it is not leaked to prevent identity theft.

Symbols

Menus and buttons in this manual are indicated using the following symbols.

Symbol	Description
" "	Menu items, which can be selected from the menu bar.
[]	Names of dialog boxes and items.
" "	Buttons with text descriptions in dialog boxes for various operations, such as executing and canceling.
	Keys on the keyboard.

Chapter 1 Overview of the OPC UA Server Functions

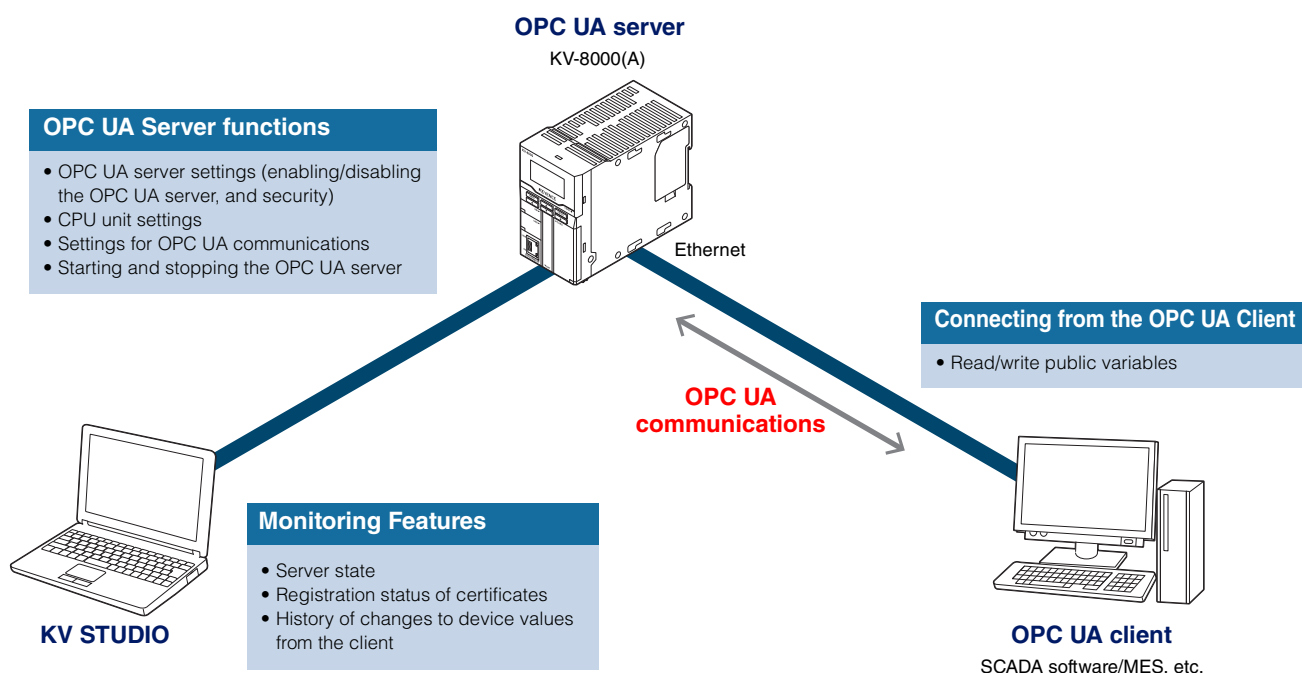
This chapter describes an overview of the features related to OPC UA communications on the "KV-8000(A)", the workflow from setup to connections, and the specifications of the features.

1-1 Overview of the Features

In terms of the OPC UA server functions on the "KV-8000(A)", the CPU unit functions as an OPC UA server providing a series of features from connecting with a client using OPC UA communications to reading and writing public variables.

For details about workflow from setup to connections, see ["1-2 Workflow from Setup to Connections"](#) (Page 1-3).

For details about CPU units and "KV STUDIO" versions that support OPC UA communications, and the specifications of the features, see ["1-3 Specifications of Features"](#) (Page 1-4).



OPC UA Server functions

The OPC UA server functions enable the CPU unit to function as an OPC UA server. Enable the OPC UA server and set the security mode or set to read and write from the OPC UA client.

OPC UA server and CPU unit settings

These are the settings for the CPU unit to function as an OPC UA server.

- OPC UA server settings: Set the OPC UA server functions to enable or disable, and configure the security settings for connections from an OPC UA client.
- CPU unit settings: Set the IP address and port number for the CPU unit that will serve as the OPC UA server endpoint URL.

["Chapter 2 OPC UA Server and CPU Unit Settings"](#) (Page 2-1)

["Chapter 3 Security Features"](#) (Page 3-1)

Settings for OPC UA communications

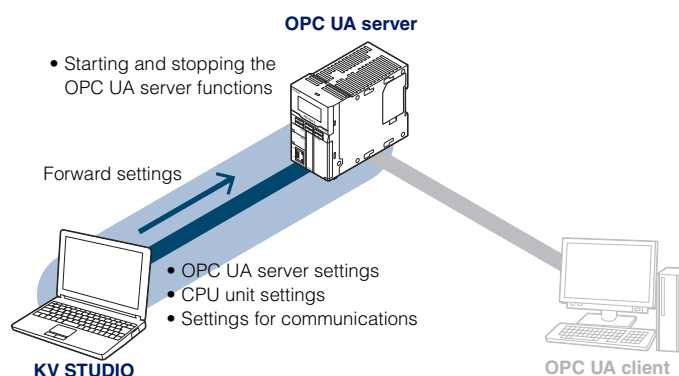
Create variables to read and write from the OPC UA client and set the targets for OPC UA communications. Variables set at the target of communications are assigned to the OPC UA address space and are read and written from the OPC UA client.

Only global variables can be set as communications targets. They support BOOL/UINT/INT/UDINT/DINT/REAL/LREAL/STRING data types and are also compatible with array and structure types.

["Chapter 4 Settings for OPC UA Communications"](#) (Page 4-1)

Starting and stopping the OPC UA server functions

Enabling the feature with the OPC UA server settings and forwarding the settings to the CPU unit will start the OPC UA server functions. The OPC UA server functions will also operate when the CPU unit is in the PROG state. Disabling the settings and forwarding them to the CPU unit will stop the OPC UA server functions.



Monitoring Features

The OPC UA server status and revision history for the device values can be checked by using the "KV STUDIO" monitoring features.

- OPC UA server monitor: The operation status for the OPC UA server, connection status from the OPC UA client, and other server statuses.

☞ "5-1 Checking the Server Status" (Page 5-1)

Additionally, the registration details of server certificates, client certificates, and certificate revocation list saved on the CPU unit (CPU memory/memory card).

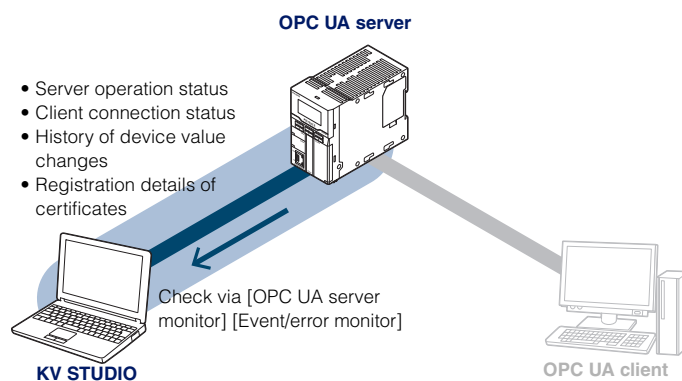
☞ "3-3 Server Certificates" (Page 3-4)

☞ "3-4 Client Certificates" (Page 3-9)

☞ "A-1 CA-signed Client Certificates" (Page A-1)

- Event/error monitor: The write status from the client to the variables set as communications targets can be checked as the device value changes.

☞ "5-2 Checking the History of Device Value Changes for Variables" (Page 5-2)

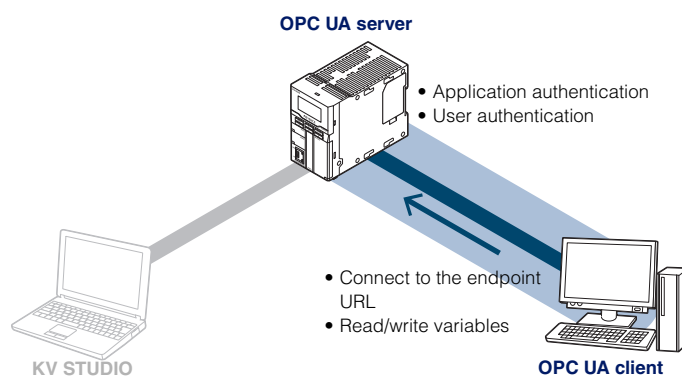


Connecting from the OPC UA Client and Reading and Writing Variables

Specify the OPC UA server URL (endpoint URL) to connect from the OPC UA client.

Reading and writing to variables set as the targets of communications will be performed according to the OPC UA address space.

☞ "Chapter 6 Connecting from the OPC UA Client and Reading and Writing Variables" (Page 6-1)



1-2 Workflow from Setup to Connections

This section describes workflow of the settings configured on the OPC UA server and OPC UA client respectively.

To use the security features, server and client certificates must be exchanged.

For details about the security policy, see ["3-2 Security Policy"](#) (Page 3-3).

For details about the server certificate, see ["3-3 Server Certificates"](#) (Page 3-4).

For details about the client certificate, see ["3-4 Client Certificates"](#) (Page 3-9).

This section describes how to use self-signed SSL certificates.

To use CA-signed certificates, see ["A-1 CA-signed Client Certificates"](#) (Page A-1).

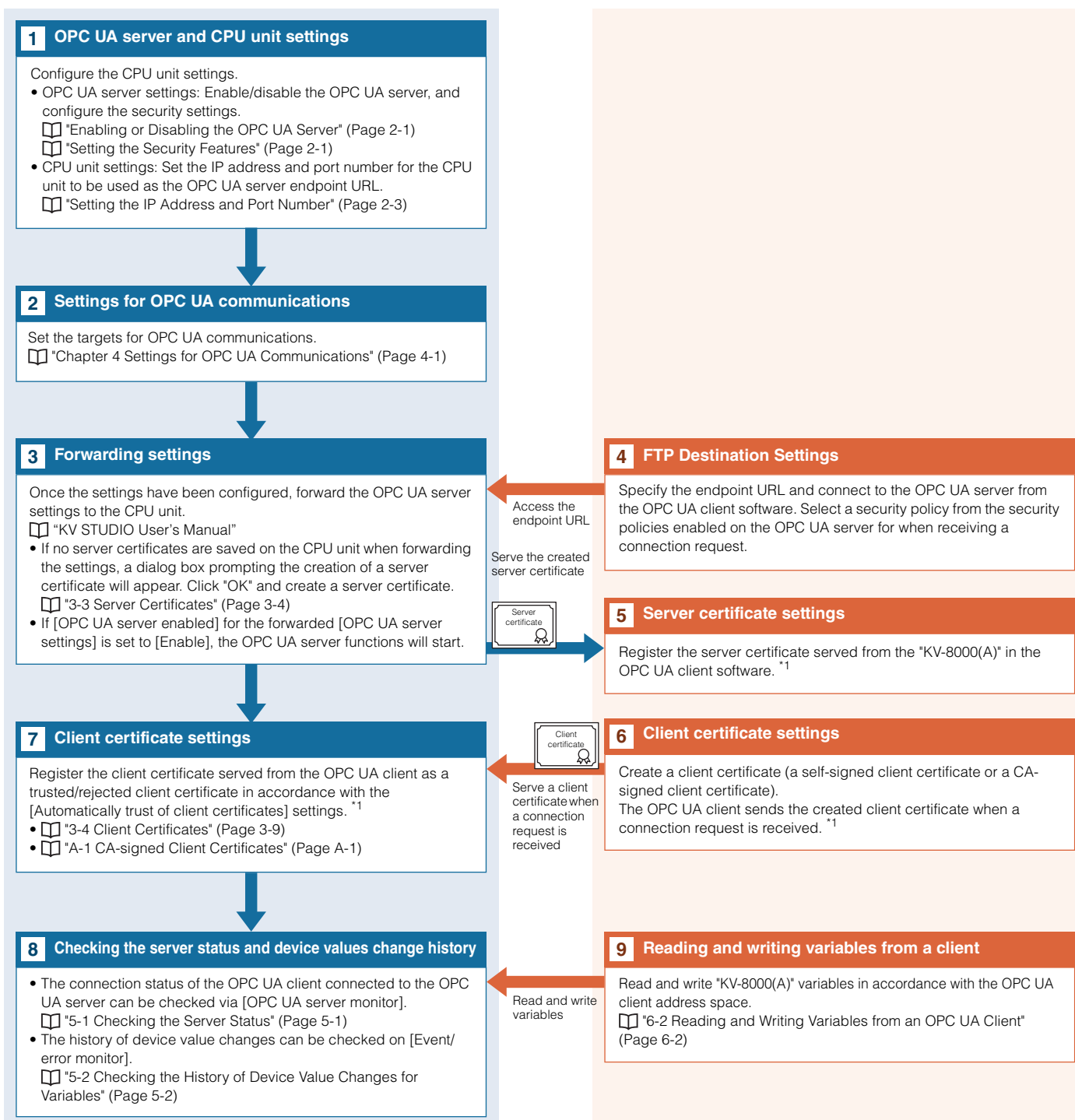
Workflow from Setup to Connections

OPC UA server side setup

Configure the OPC UA server settings using "KV STUDIO".

OPC UA client side setup

For details about configuring the OPC UA client settings, see the instruction manual for the applicable OPC UA client.



^{*1} If [None] is selected for the security policy, communications are possible even without exchanging the server and client certificates.

1-3 Specifications of Features

This section describes the CPU unit that the OPC UA features support, the supported version of KV STUDIO, and the specifications of the OPC UA server functions.

Supported CPU Unit and KV STUDIO Versions

CPU unit model	CPU unit supported versions	KV STUDIO supported versions
KV-8000(A)	Ver. 2.4 or later	Ver. 11.4 or later

OPC UA Server function Specifications

Item		Description
Supported model		KV-8000(A)
Connection port		Ethernet port* ¹ built-in to the CPU unit (can be used the same as other Ethernet communications)
Supported features		OPC UA server functions
Transport/data encoding method		UA TCP binary
URL (endpoint URL) specification method		opc.tcp://[IP address]:[Port No.] E.g.) opc.tcp://192.168.0.10:4840
Maximum number of sessions (clients)		20
Number of monitored items* ²		Up to 2,000
Supported sampling cycle		50 ms to 10 s* ³
Maximum number of public network variables		Max. 200,000* ⁴
OPC UA security mode and policy		<ul style="list-style-type: none"> Signature and encryption required: SignAndEncrypt Signature required: Sign Both signature and encryption not required: None
Signature and encryption algorithms		Basic128Rsa15 / Basic256 / Basic256Sha256 / Aes128Sha256RsaOaep / Aes256Sha256RsaPss
Application authentication	Certificate authentication methods	<ul style="list-style-type: none"> Authentication using trusted certificates Authentication using CA-signed certificates
	Supported certificate standards	X.509 compliant
User authentication	User authentication methods	<ul style="list-style-type: none"> User name/Password Anonymous

*¹ The OPC UA server functions can be used in combination with other Ethernet features.

*² The number of monitored items is the number of elements to be set as targets for cyclic communications on the OPC UA client. The number of monitored items counts the actual number of variables regardless of the size of the variable. Even if the registered variable data type is structure or array, the number of monitor items is counted as 1. When monitoring the maximum number of Public network variables, it is possible to define the target data as a variable of the structure type.

*³ The sampling cycle is set on the OPC UA client.

KV-8000 OPC UA server operates at an integer multiple of 50 ms regardless of the sampling cycle set on the client.

*⁴ Includes the number of structural members and array elements.

For details about variables, see □ "Chapter 4 Settings for OPC UA Communications" (Page 4-1).

Chapter 2 OPC UA Server and CPU Unit Settings

This chapter describes the OPC UA server and CPU unit settings and the procedures to configure those settings.

2-1 OPC UA Server Settings

These are settings related to the security features and to enable or disable the OPC UA server functions.

Enabling or Disabling the OPC UA Server

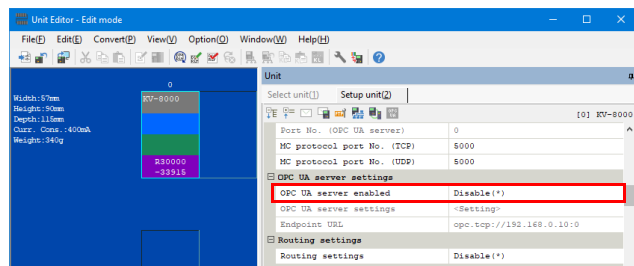
These are the settings for the CPU unit to function as an OPC UA server. Enabling these settings allows the settings for the security features described herein to be configured.

Reference Configuring this setting to [Enable] and forwarding the settings to the PLC automatically starts the OPC UA server function. Setting it to [Disable] and forwarding them will stop the OPC UA server functions. To change between enabling and disabling the OPC UA server, the system must be changed to PROGRAM mode.

1 Start the unit editor.

For details how to start and operate the unit editor, see ["KV STUDIO User's Manual"](#).

2 Select whether to enable or disable the OPC UA server with [OPC UA server enabled] under [OPC UA server settings].



Item	Description
OPC UA server settings	
OPC UA server enabled	Select whether to enable the OPC UA server functions (default setting: Disable).

If the setting is changed to [Enable], a confirmation message appears.

Reference If the setting is set to [Disable], a confirmation message does not appear. Clicking [Apply] in the unit editor completes the configuration of the settings.

3 Click [OK].

The OPC UA server functions have now been enabled.

Next, configure the security and endpoint URL settings.

- ["Setting the Security Features"](#) (Page 2-1)
- ["Setting the IP Address and Port Number"](#) (Page 2-3)

Setting the Security Features

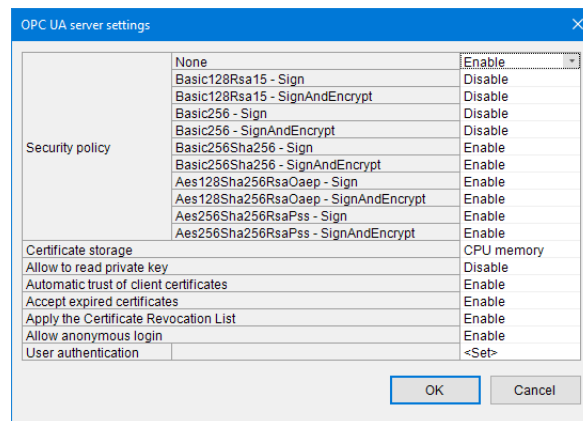
These are the security feature settings for the connections from an OPC UA client. The OPC UA server function has two types of authentication: application authentication to authenticate a connection with an electronic certificate and user authentication to authenticate a user with a user name and password. For details of the security features, see ["Chapter 3 Security Features"](#) (Page 3-1). Set the security features on the [OPC UA server settings] dialog box.

Important The security policy is set to [None] by default, so an OPC UA client can connect to the OPC UA server without using the security features by selecting [None] on the OPC UA client as well.


1 In the unit editor, select [OPC UA server settings] - [OPC UA server settings] and then click .


The [OPC UA server settings] dialog box will appear.

2 Set the security features for the connections from an OPC UA client.



Item	Description
Security	
Security policy	Set the security policy to [Enable] to apply the applicable setting to exchange messages in OPC UA communications. <ul style="list-style-type: none"> • None (default setting: Enable) • Basic128Rsa15 - Sign (default setting: Disable) • Basic128Rsa15 - SignAndEncrypt (default setting: Disable) • Basic256 - Sign (default setting: Disable) • Basic256 - SignAndEncrypt (default setting: Disable) • Basic256Sha256 - Sign (default setting: Enable) • Basic256Sha256 - SignAndEncrypt (default setting: Enable) • Aes128Sha256RsaOaep - Sign (default setting: Enable) • Aes128Sha256RsaOaep - SignAndEncrypt (default setting: Enable) • Aes256Sha256RsaPss - Sign (default setting: Enable) • Aes256Sha256RsaPss - SignAndEncrypt (default setting: Enable) For details of the security policy, see "3-2 Security Policy" (Page 3-3).
Certificate storage	Select the storage to save the certificates (server certificates, client certificates, and certificate revocation list). <ul style="list-style-type: none"> • CPU memory (default setting) • Memory card
Allow to read private key ^{*1}	Select whether to allow to read private key saved in storage. <ul style="list-style-type: none"> • Enable: Allow to read private key. • Disable (default setting): Reject to read private key.

Item	Description
Automatic trust of client certificates	<p>Select whether to trust a client certificate when a request to connect is received with a client certificate that is not saved in certificate storage.</p> <ul style="list-style-type: none"> • Enable (default setting): Add the certificate to the [Trusted] folder and allow the client to connect. • Disable: Add the certificate to the [Rejected] folder and deny connecting.
Accept expired certificates	<p>Select whether to allow connecting when a request to connect is received with a client certificate in the [Trusted] folder even if the certificate has expired.</p> <ul style="list-style-type: none"> • Enable (default setting): Trust the certificate and allow the client to connect. • Disable: Do not trust and deny connecting.
Apply the Certificate Revocation List	<p>Select whether to reject connecting from a client certificate in the certificate revocation list when a certificate revocation list is registered.</p> <ul style="list-style-type: none"> • Enable (default setting): Reject a connection request by a client certificate in the certificate revocation list. • Disable: Do not authenticate using the certificate revocation list. As long as the client certificate is in the [Trusted] folder, connecting is allowed even if the connection request is from a client in the certificate revocation list.
Allow anonymous login	<p>Select whether to allow anonymous login.</p> <ul style="list-style-type: none"> • Enable (default setting): Allow anonymous login. • Disable: Reject anonymous login.
User authentication	<p>Set a user name and password to perform authentication with a user name and password.</p> <p>For details about how to configure the settings, see  "3-5 User Authentication" (Page 3-13).</p>

*1 This setting is only configurable when [Certificate storage] is set to [CPU memory]. When [Memory card] is selected, only [Enable] is available. When replacing the CPU unit, copying the private key in the CPU memory beforehand and storing it in the KV-8000 enables communications with the OPC UA client without having to regenerate a server certificate. For details about server certificates, see  "3-3 Server Certificates" (Page 3-4).

3 To apply the settings, click "OK".

The [OPC UA server settings] dialog box closes and the unit editor appears.

2-2 CPU Unit Settings

This section describes the CPU unit settings related to the OPC UA communications.

For details about the CPU unit settings not related to the OPC UA communications, see "KV STUDIO User's Manual."

Setting the IP Address and Port Number

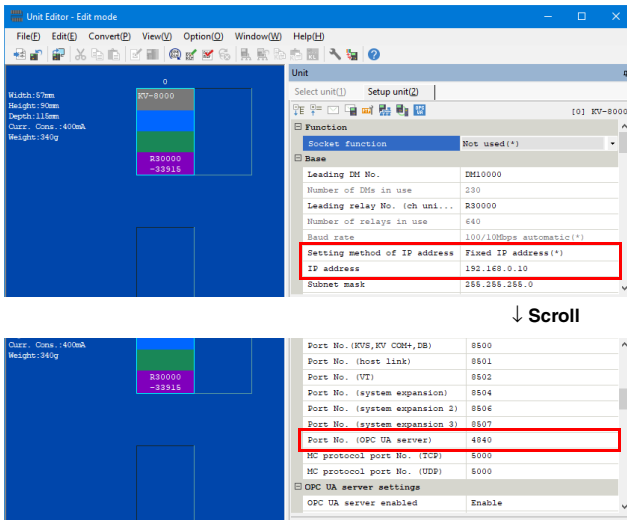
Set an IP address for the CPU unit and a port number for OPC UA communications. The IP address and port number for the CPU unit is contained in the endpoint URL specified when connecting from the OPC UA client.

Format: opc.tcp://[IP address]:[Port No.]

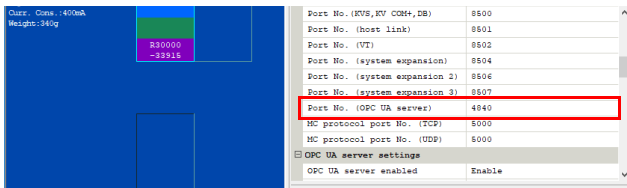
1 Start the unit editor.

For details how to start and operate the unit editor, see "KV STUDIO User's Manual".

2 Set an IP address and a port number for the OPC UA communications.

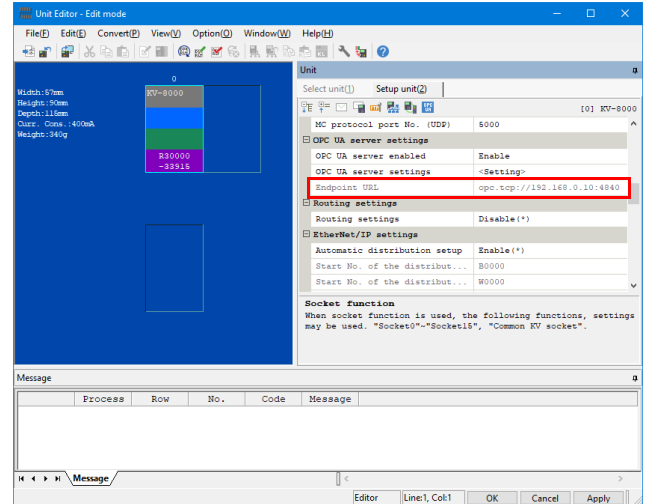


↓ Scroll



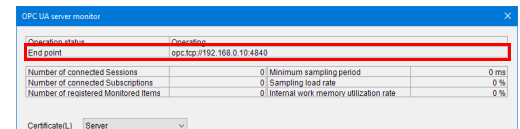
3 Click "Apply".

The endpoint URL is set with the set IP address and port number.



Reference

The endpoint URL can also be checked via [OPC UA server monitor].



"5-1 Checking the Server Status" (Page 5-1)

Item	Description
Base	
Setting method of IP address	Select how to set the IP address. <ul style="list-style-type: none"> Fixed IP address (default setting) BOOTP -> automatic switching of fixed IP BOOTP
IP address	If the IP address setting method is set to "Fixed IP Address," the port IP address used in the OPC UA communications (default setting: 192.168.0.10) is set.
Port No.	
Port No. (OPC UA server)*1	Set the port number to use for the OPC UA communications (default setting: 4840, setting range: 1 to 65535).

*1 The setting can be configured only when [OPC UA server enabled] is set to [Enable].

Point

Make sure that [Port No. (OPC UA server)] is not duplicated with a port number used by another communications service. For details about the port numbers used by the other services, see "KV Series EtherNet/IP Function User's Manual".

Important

- The IP address information is included in the server certificate. Changing the IP address after generating the server certificate (Page 3-5) will cause the server certificate IP address and CPU unit IP address to no longer match and connecting from the OPC UA client may no longer be possible. To connect in that case, restore the IP address to its previous value or regenerate a server certificate (Page 3-7).
- If [BOOTP -> automatic switching of fixed IP] is selected for [Setting method of IP address], a BOOTP server must be set, an IP address obtained, and then a server certificate must be generated.

Chapter 3 Security Features

This chapter describes the security features for the OPC UA server function.

3-1 Overview of the Security Features

OPC UA enables the security for the connections to be set.

This section describes these security features.

Set the communications security policy to prevent theft and the tampering of messages exchanged in the OPC UA communications.

The security policy specifies whether to sign and encrypt messages and the algorithm combinations.

- **Signature:** Information that is encrypted and appended to guarantee the integrity of the certificates and the messages.
- **Encrypt:** Messages are converted into ciphertext using a certain technique (algorithms) when they are transmitted to prevent them being stolen or modified during transmissions by a third party.

For details, refer to ["3-2 Security Policy"](#) (Page 3-3).

Authenticating Connections

The OPC UA server function ensures security with two-factor authentication for OPC UA client connections using application authentication and user authentication.

Application Authentication

Application authentication is a method in which the OPC UA server and OPC UA client exchange electronic certificates to authenticate each other's identity.

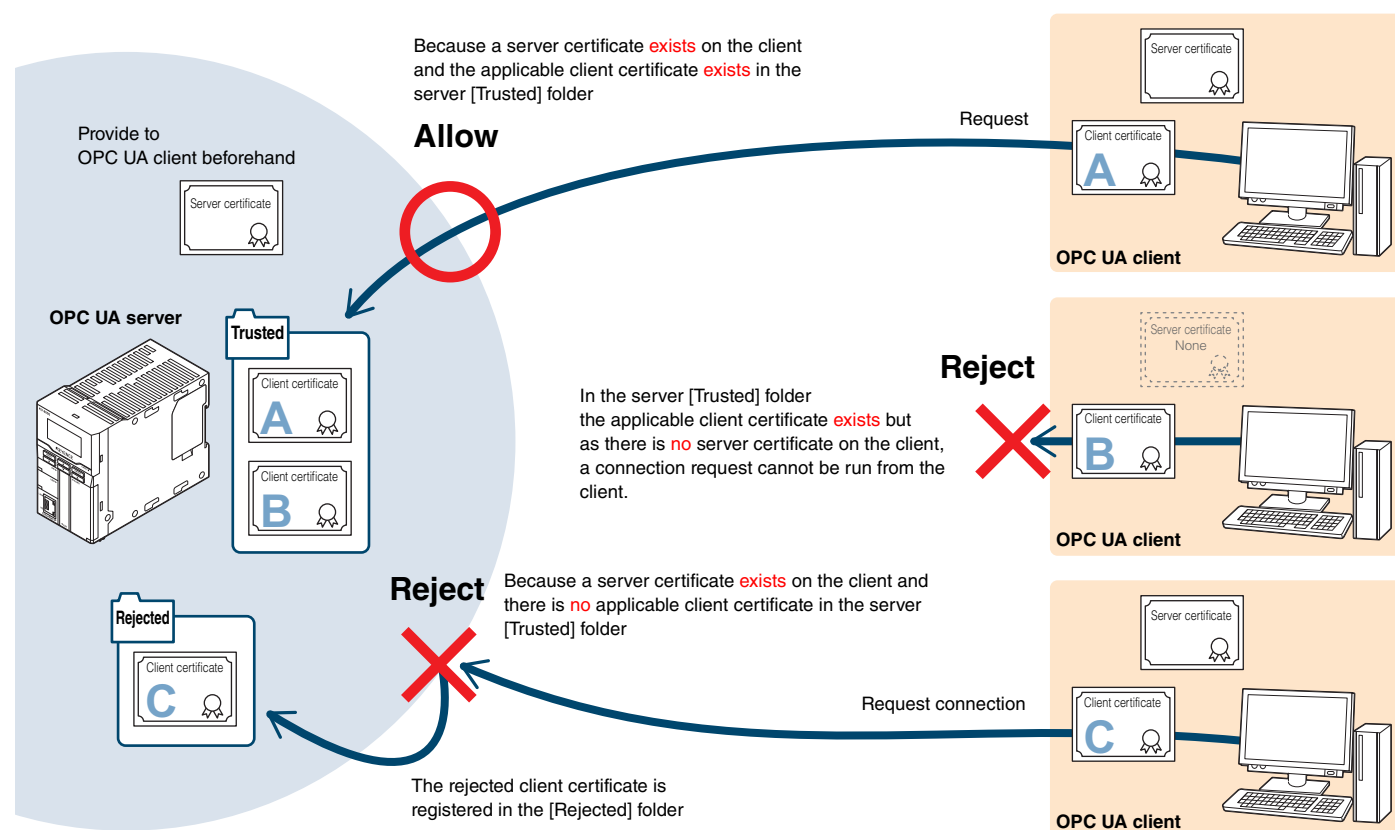
The "KV-8000(A)" application authentication supports X.509 standard certificates.

How authentication works

The OPC UA server function exchanges a server certificate and a client certificate with the OPC UA client to authenticate each other.

Registering a server certificate generated by "KV STUDIO" on an OPC UA client and registering a client certificate provided by the OPC UA client as a KV-8000(A) "trusted client certificate" enables connecting.

Reference This is how authentication works using a self-signed client certificate. For details about authentication using a CA-signed client certificate, see ["A-1 CA-signed Client Certificates"](#) (Page A-1).



Point Setting the security policy to [None] enables communications without having to exchange certificates. Therefore, security is not ensured.

Types of certificates

There are three types of certificates that the OPC UA server functions supports.

Certificate	Description
Server certificate	This is a certificate that authenticates the OPC UA server. A self-signed server certificate ^{*1} and a CA-signed server certificate ^{*2} can be used. The connected client must provide the certificates.
Client certificate	This is a certificate that authenticates an OPC UA client. Both a self-signed client certificate and a CA-signed client certificate ^{*3} can be used. Although the connected client must provide a certificate, a certificate sent from the OPC UA client can also be automatically registered when a connection request is received.
CA certificate and Certificate revocation list ^{*3}	A CA certificate is a certificate to authenticate the certificate chain when using a CA-signed certificate. A certificate revocation list is a list of certificates that were revoked due to certificates being leaked, the company name changing, or some other reason. Clients authenticated by a CA authority can be authenticated all at once.

*1 Server certificates generated by "KV STUDIO" are self-signed server certificates.

*2 This is a server certificate issued by a certification authority (CA). Import the certificate into the CPU unit to use it (Page 3-8). In addition to a CA-signed server certificate, a CA certificate and certificate revocation list must be provided to the OPC UA client and registered in advance. For details of how to register certificates, see the manual for the applicable OPC UA client application.

*3 This is a client certificate issued by a certification authority (CA). Register a combination of a CA-signed certificate, CA certificate, and certificate revocation list in accordance with the authentication pattern. For details, see "A-1 CA-signed Client Certificates" (Page A-1).

Managing certificates

The OPC UA server function can perform the following processing on certificates.

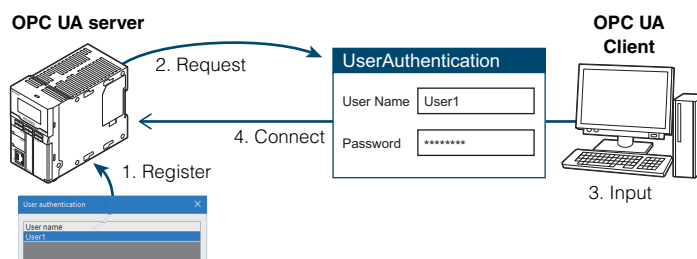
Certificate	Description
Server certificate	<ul style="list-style-type: none"> Generate server certificates (Page 3-5) Display server certificate information deployed on the CPU unit (Page 3-11) Regenerate server certificates (Page 3-7) Export server certificates from the CPU unit (Page 3-5) Import server certificates to the CPU unit (Page 3-8)
Client certificate	<ul style="list-style-type: none"> Authenticate client certificates when connecting (Page 3-9) Configure settings to trust or reject client certificates (Page 2-1) Display client certificate information registered on the CPU unit (Page 3-11) Add client certificates (Page 3-10) Allow rejected client certificates (Page 3-12) Delete client certificates (Page 3-12)
CA certificate and certificate revocation list	These are used only with CA-signed client certificates. "A-1 CA-signed Client Certificates" (Page A-1)

User authentication

This is a method in which the OPC UA server authenticates an OPC UA client that accesses the OPC UA server using a user name and password. Register a user name and password for the user to be allowed to connect in the OPC UA server.

A user name and password must be entered when connecting from an OPC UA client to authenticate the client.

For details, refer to "3-5 User Authentication" (Page 3-13).




3-2 Security Policy

The security policy defines the combination of settings required to maintain security including whether to sign and encrypt messages exchanged in the communications and the applicable algorithm.

Set a message security policy to ensure secure communications.

Communications are enabled by setting the same security policy between the OPC UA server and the OPC UA client that connect to the server.


Configure the security policy in the OPC UA server settings. For details, refer to  "Setting the Security Features" (Page 2-1).


- Configurable security policy

The configurable security policy is shown below. Multiple security policies can be set to enable connections with an OPC UA client that has a different security policy.

Security policy	Signature	Encryption	Integrity (Measures to prevent tampering)	Confidentiality (Measures to prevent theft)
None	-	-	-	-
Basic128Rsa15 – Sign	Basic128Rsa15	-	○	-
Basic128Rsa15 – SignAndEncrypt	Basic128Rsa15	Basic128Rsa15	○	○
Basic256 – Sign	Basic256	-	○	-
Basic256 – SignAndEncrypt	Basic256	Basic256	○	○
Basic256Sha256 – Sign	Basic256Sha256	-	○	-
Basic256Sha256 – SignAndEncrypt	Basic256Sha256	Basic256Sha256	○	○
Aes128Sha256RsaOaep – Sign	Aes128Sha256RsaOaep	-	○	-
Aes128Sha256RsaOaep – SignAndEncrypt	Aes128Sha256RsaOaep	Aes128Sha256RsaOaep	○	○
Aes256Sha256RsaPss – Sign	Aes256Sha256RsaPss	-	○	-
Aes256Sha256RsaPss – SignAndEncrypt	Aes256Sha256RsaPss	Aes256Sha256RsaPss	○	○

For details about the security policy, see "OPC Unified Architecture Specification" created by the OPC Foundation.

 **[None] is a setting that allows the communications of messages that have not been signed or encrypted. If you are concerned about message security, set [None] for [Security policy] to [Disable].**

 The security policy is set to [None] by default, so an OPC UA client can connect to the OPC UA server without using the security features by selecting [None] on the OPC UA client as well.

3-3 Server Certificates

The server certificates that authenticate the identity of the OPC UA server.

If the security features have been set, connecting is possible by registering a server certificate on the OPC UA client.

This section describes the authentication and management of a server certificate.

- "Authenticating a Server Certificate" (Page 3-4)
- "Managing Server Certificate Information" (Page 3-6)

Authenticating a Server Certificate

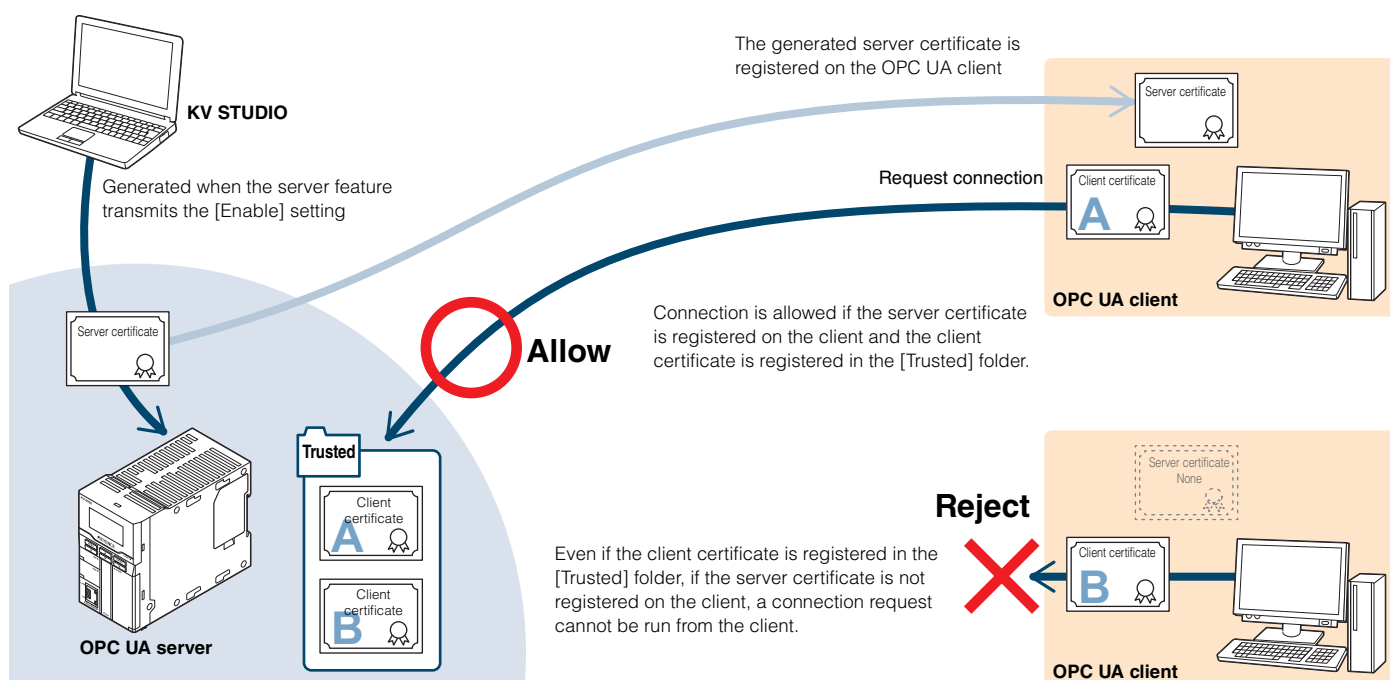
A server certificate is generated when [OPC UA server settings] that have [OPC UA server enabled] set to [Enable] with "KV STUDIO" are transmitted to the CPU unit (Page 3-5).

A generated server certificate must be registered on an OPC UA client to connect from an OPC UA client.

A connection can be established with a client once a server certificate is provided when a connection request is received from an OPC UA client and registered on the client.

Point For details about operating an OPC UA client, see the instruction manual for the applicable OPC UA client software.

- Reference**
- A server certificate can also be provided to the client by manually exporting it from "KV STUDIO".
 "Exporting a Server Certificate" (Page 3-5)
 - Information for a generated server certificate can be managed via [OPC UA server monitor].
 "Managing Server Certificate Information" (Page 3-6)



After a connection is established with an OPC UA, connection authentication is performed in accordance with the client certificate sent from the OPC UA client at the time of the connection request and the certificates registered in the [Trusted] folder.



For details about connection authentication using a client certificate, see "Authenticating Client Certificates" (Page 3-9).

Generating a Server Certificate


Server certificates are generated when a CPU unit for which the OPC UA server function is enabled and "KV STUDIO" connect.

A server certificate can be generated on the [OPC UA server certificate generation] dialog box that appears if there is no server certificate in the CPU unit when a project is sent to the CPU unit with [OPC UA server enabled] set to [Enable] for the OPC UA server settings.

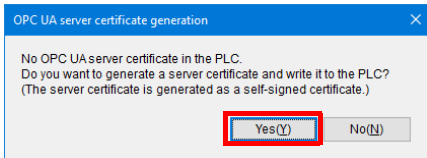
A generated server certificate is saved in the CPU unit according to [OPC UA server settings].

 Server certificates can also be generated via [OPC UA server monitor]. For details, see  "Regenerating a Server Certificate" (Page 3-7).

1 Transfer the settings to the CPU unit.

For details about transferring settings, see  "KV STUDIO User's Manual".

2 Click "Yes".



3 Configure the settings as necessary.

Item	Description
Organization name (N) ^{*1}	Enter the name of the organization that will manage the server (default setting: KEYENCE CORPORATION).
Organizational unit (U) ^{*1}	Enter the name of the organization department or division that will manage the server (default setting: Blank).
Locality (M) ^{*1}	Enter the name of the place where the organization that will manage the server is located (default setting: Osaka).
State or Province (P) ^{*1}	Enter the name of the state or province where the organization that will manage the server is located (default setting: Osaka).
Country (I) ^{*2}	Enter the name of the country where the organization that will manage the server is located (default setting: JP).
Valid period (year)(V)	Enter the period (year) that the server certificate is valid for. (default setting: 20).
Export certificate and private key (E)	Selecting this check box outputs a certificate and private key ^{*3} to the output folder when generating a server certificate (default setting: Blank).
Reference	Click this button to specify a destination to export a certificate and private key.
Output folder	Displays the specified export path.

^{*1} The characters that can be entered are as follows:
0 to 9, a to z, A to Z, half-width space [], hyphen [-], period [.] , underscore [_], comma [,], slash [/], parentheses [()].
The limit is 64 characters.

^{*2} Enter the country code (two half-width Latin characters).

^{*3} Registering a certificate in the OPC UA client enables the client to send a connection request to the server. A private key is created only when a server certificate is generated.

4 To apply the settings, click "OK".

A server certificate is generated with the configured settings and saved on the CPU unit.

 "Storage location for server certificates and private keys" (Page 3-5)

- Storage location for server certificates and private keys
Server certificates are stored in CPU memory or an SD card according to [OPC UA server settings].

For details about settings, see  "Certificate storage" (Page 2-1).

The destination is as follows.


Description	Path
Server certificate	cert\unit00\opcua\pki\own\server-cert.der
Private key	cert\unit00\opcua\pki\own\server-key.bin

Exporting a Server Certificate

Export a server certificate registered in the CPU unit when providing a server certificate to an OPC UA client before connecting or for some other reason.

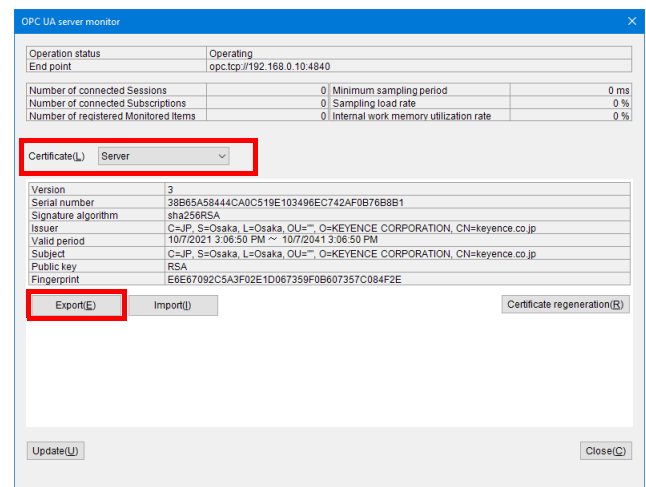
Export a certificate via [OPC UA server monitor].

1 Display [OPC UA server monitor].

 "Displaying [OPC UA server monitor]" (Page 3-6)

2 For [Certificate], select [Server].

3 Click "Export".



The [Save As] dialog box appears.

4 Specify the export destination, and then click "Save".

The server certificate file is saved in the specified location.

Private Keys

The server and client that exchanged the certificate confirm each other's identity. The sender signs data using electronic data called a private key and it is checked by the receiver using electronic data called a public key that is included with the certificate. If data is transmitted without checking it with a certificate and a different OPC UA server device uses the same endpoint URL, there is the risk that incorrect information may be exchanged with the OPC UA client. Deploying an issued server certificate together with the private key on the OPC UA server enables risks like the one stated above to be prevented. If the private key is deployed on the CPU memory in the "KV-8000(A)" and the memory is formatted, the private key will also be deleted. Therefore, communications will no longer be possible with OPC UA client devices, and a server certificate will have to be regenerated and re-registered on the clients' devices.

Backing up the private key on the CPU memory beforehand and then saving it again on the CPU memory in the "KV-8000(A)" after formatting will alleviate the need to regenerate and re-register a server certificate.

Managing Server Certificate Information

The OPC UA server functions can run the following functions on server certificates:

- Display server certificate information (📖 Page 3-6): Displays information related to server certificates.
- Update server certificate information (📖 Page 3-7): Refreshes displayed information related to server certificates with information in the CPU unit.
- Regenerate server certificates (📖 Page 3-7): Regenerates a server certificate when the IP address changes or for some other reason.
- Import server certificates into the CPU unit (📖 Page 3-8): Imports server certificates into the CPU unit when using CA-signed server certificates.

Displaying Server Certificate Information

Display server certificate information deployed on the CPU unit. Information for a server certificate can be displayed via [OPC UA server monitor].

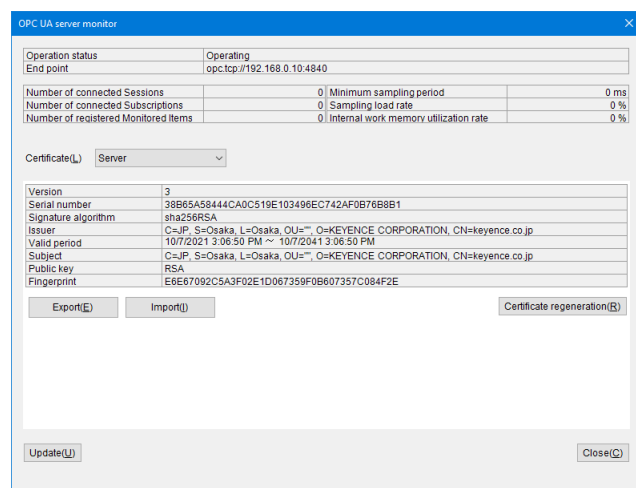
- Displaying [OPC UA server monitor]

1 Change "KV STUDIO" to monitoring mode or online edit mode.

Point [OPC UA server monitor] can only be displayed when "KV STUDIO" is in [Monitor], [Online edit] or [Replay] mode.
For details about [Monitor], [Online edit], and [Replay] modes, see 📖 "KV STUDIO User's Manual".

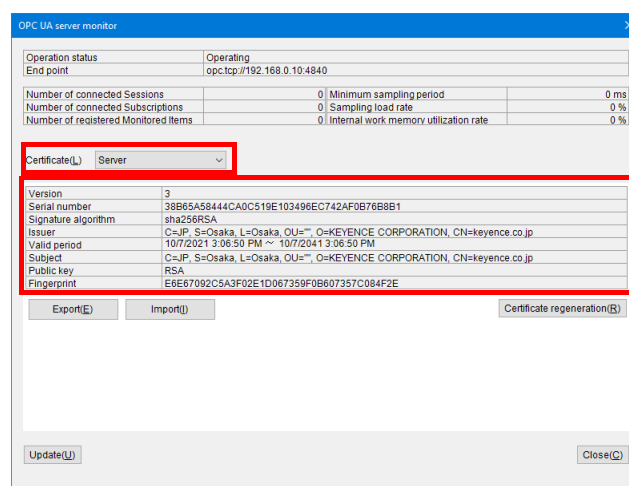
2 Right-click the CPU unit in [Unit configuration] on the workspace and on the menu that appears, click "OPC UA server monitor (E)".

[OPC UA server monitor] appears.



- Displaying server certificate information

1 For [Certificate], select [Server].



The information below is displayed.

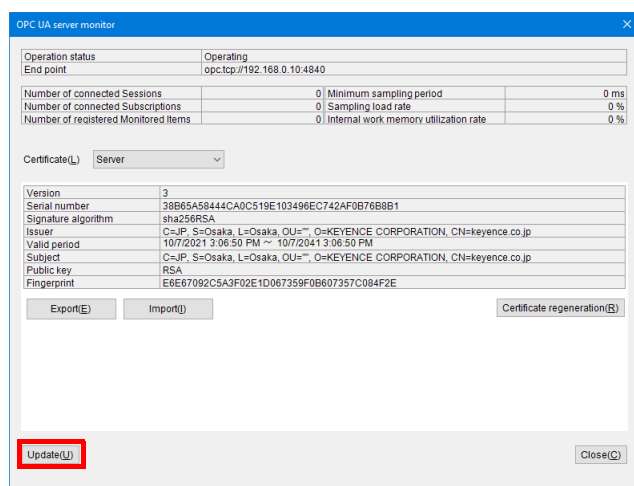
Item* ¹	Description of feature
Version	This is the certificate version information.
Serial number	This is the identification number for the certificate.
Signature algorithm	This is the signature algorithm assigned to the certificate.
Issuer	This is the name of the certificate authority that issued the certificate. E.g.) C=JP, S=Osaka, O=KEYENCE CORPORATION, CN=keyence.co.jp
Valid period	This is the period that the certificate is valid for. E.g.) 2021/11/23 11:19:43 to 2041/11/23 11:19:43
Subject	This is the owner of the public key. For a self-signed certificate, this is the same as [Issuer]. E.g.) C=JP, S=Osaka, O=KEYENCE CORPORATION, CN=keyence.co.jp
Public key	This is the applicant's public key and its type.
Fingerprint	This is a check code to prevent certificate tampering.

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

Updating Server Certificate Information

Update server certificate information via [OPC UA server monitor] with information in the CPU unit.

1 Click "Update".



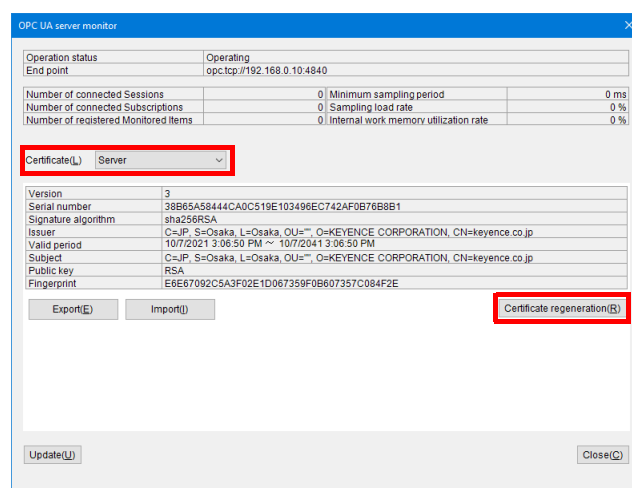
The details of the server certificate are refreshed with data in the CPU unit.

Regenerating a Server Certificate

If the OPC UA server IP address or other information on the server certificate is changed, the server certificate in the CPU unit can be manually regenerated. Regenerate a certificate via [OPC UA server monitor].

Important If the OPC UA server IP address is changed, the server certificate will have to be regenerated and re-registered on OPC UA clients. Changing the IP address will cause the server certificate IP address and CPU unit IP address to no longer match and connecting may no longer be possible from the OPC UA client. Follow the procedures below to regenerate a server certificate.

- 1 Display [OPC UA server monitor].
 "Displaying [OPC UA server monitor]" (Page 3-6)
- 2 For [Certificate], select [Server].
- 3 Click "Certificate regeneration".



The [OPC UA server certificate generation] dialog box appears.

4 Configure the settings as necessary.

Item	Description
Organization name (N) ^{*1}	Enter the name of the organization that will manage the server (default setting: KEYENCE CORPORATION).
Organizational unit (U) ^{*1}	Enter the name of the organization department or division that will manage the server (default setting: Blank).
Locality (M) ^{*1}	Enter the name of the place where the organization that will manage the server is located (default setting: Osaka).
State or Province (P) ^{*1}	Enter the name of the state or province where the organization that will manage the server is located (default setting: Osaka).
Country (I) ^{*2}	Enter the name of the country where the organization that will manage the server is located (default setting: JP).
Valid period (year) (V)	Enter the period (year) that the server certificate is valid for. (default setting: 20).
Export certificate and private key (E)	Selecting this check box outputs a certificate and private key ^{*3} to the output folder when generating a server certificate (default setting: Blank).

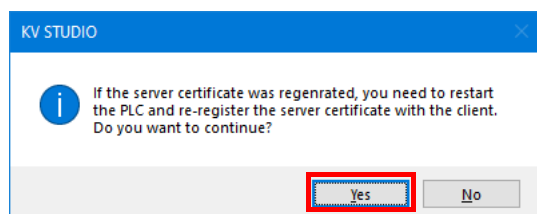
Item	Description
Reference	Click this button to specify a destination to export a certificate and private key.
Output folder	Displays the specified export path.

- *1 The characters that can be entered are as follows:
0 to 9, a to z, A to Z, half-width space [], hyphen [-], period [.], underscore [_], comma [,], slash [/], parentheses [()].
The limit is 64 characters.
- *2 Enter the country code (two half-width Latin characters).
- *3 Registering a certificate in the OPC UA client enables the client to send a connection request to the server.

5 To apply the settings, click "OK".

A confirmation dialog box appears.

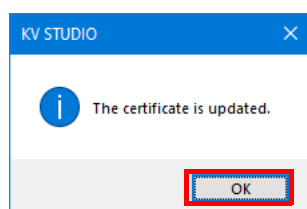
6 Click "Yes".



A server certificate is regenerated with the configured settings and saved on the CPU unit.

☞ "Storage location for server certificates and private keys" (Page 3-5)
Once processing is completed, a dialog box appears.

7 Click "OK".



- Point**
- The IP address recorded on the regenerated server certificate is the IP address set in the CPU unit at that time.
 - After regenerating a server certificate, make sure to export the server certificate and install it on the OPC UA client. If the server certificate is not installed after it is regenerated that will cause the server certificate IP address and CPU unit IP address to no longer match and communications may no longer be possible with the OPC UA client.
 - ☞ "Exporting a Server Certificate" (Page 3-5)
 - To use a regenerated certificate for authentication or overwrite a certificate using a storage transfer tool or the like, restart the device.

Importing a Server Certificate

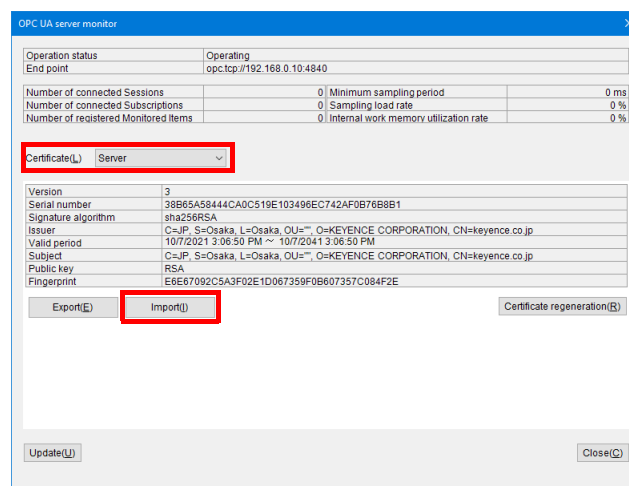
Import a server certificate into the CPU unit when using a CA-signed server certificate or a server certificate other than a self-signed one.
Import a certificate via [OPC UA server monitor].

1 Display [OPC UA server monitor].

☞ "Displaying [OPC UA server monitor]" (Page 3-6)

2 For [Certificate], select [Server].

3 Click "Import".

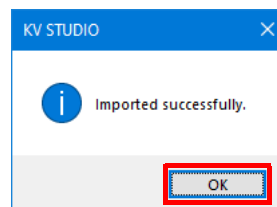


The [Browse For Folder] dialog box appears.

4 Select the folder where the certificate file is saved, and then click "OK".

The server certificate file is imported into the CPU unit.
Once processing is completed, a dialog box appears.

5 Click "OK".



- Point**
- A server certificate must be imported together with a private key.
 - To use a CA-signed server certificate, a CA-signed server certificate, CA certificate, and certificate revocation list must be provided and imported into the OPC UA client.
 - The CPU unit must be restarted to use the imported server certificate for authentication.

3-4 Client Certificates

A client certificate is a certificate that authenticates the identity of an OPC UA client.

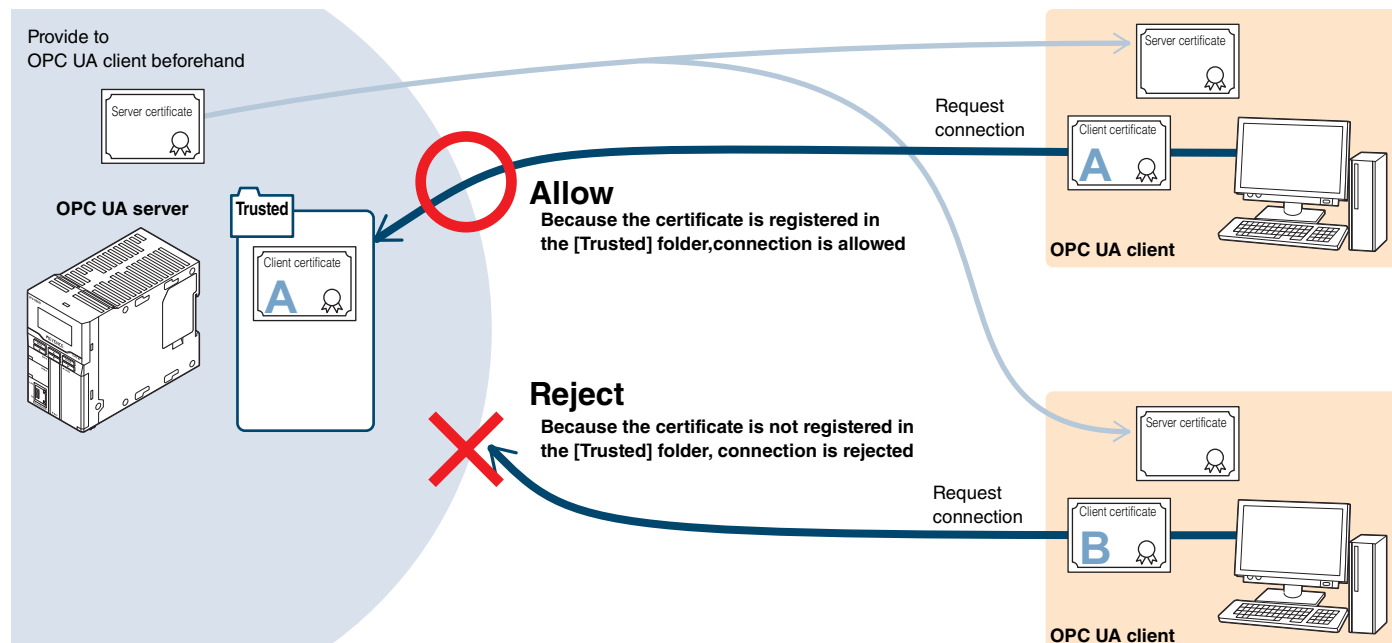
If the security functions are set, then connecting can be accomplished by registering the client certificate on the OPC UA server.

This section describes the authenticating of self-signed client certificates and the managing of client certificates.

To use CA-signed client certificates, see ["A-1 CA-signed Client Certificates"](#) (Page A-1).

Authenticating Client Certificates

The client certificate sent from the OPC UA client together with the connection start request is matched with the client certificate in the [Trusted] folder, then the connecting is permitted if it is registered in the [Trusted] folder.



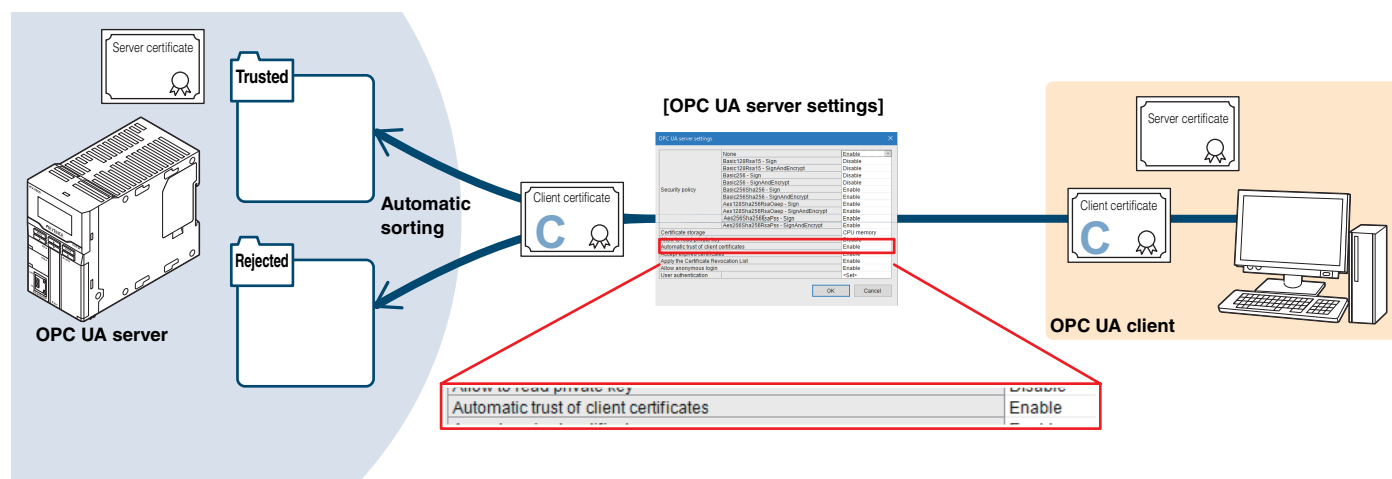
There are two ways to register a certificate in the [Trusted] folder: Automatically sort in accordance with the [Automatic trust of client certificates] setting in [OPC UA server settings] or manually register a certificate via [OPC UA server monitor].

- ["Automatic Sorting Using \[Automatic trust of client certificates\]"](#) (Page 3-9)
- ["Registering Additional Client Certificates"](#) (Page 3-10)

Reference Information for registered client certificates can be managed via [OPC UA server monitor].
["Managing Client Certificate Information"](#) (Page 3-11)

Automatic Sorting Using [Automatic trust of client certificates]

Client certificates not registered in the [Trusted] folder are sorted into the [Trusted] folder or [Rejected] folder when a client first connects in accordance with the [Automatic trust of client certificates] setting configured in [OPC UA server settings]. If a client certificate is sorted into the [Trusted] folder, connecting begins. Connecting is allowed for the second connection onwards because the client certificate is registered in the [Trusted] folder ([Page 3-1](#)). Client certificates registered in the [Rejected] folder can also be moved to the [Trusted] folder manually using "KV STUDIO" ([Page 3-12](#)).



- Connecting is allowed if a client certificate is in the [Trusted] folder.
 Even if a client certificate is in the [Rejected] folder, connecting is allowed as long as the same client certificate is in the [Trusted] folder.
- The [Automatic trust of client certificates] setting is enabled by default.

Registering Additional Client Certificates

Connecting can be allowed by adding the client certificate file (.der extension) provided by the OPC UA client to the [Trusted] folder in the CPU unit in advance. Add client certificates via [OPC UA server monitor].

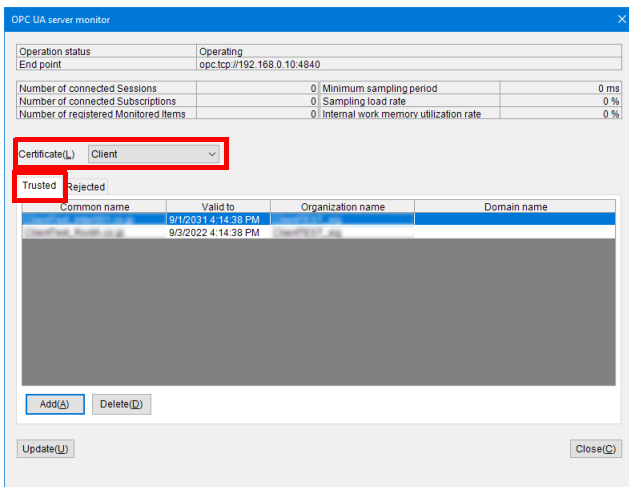
Point When registering certificates to the [Trusted] folder, double check that the client certificate being registered can be trusted. If a client certificate for which connecting should not be allowed is accidentally registered in the [Trusted] folder, that client is allowed to connect. As a result, confidential information on the server may be leaked and unauthorized operations may be performed.

1 Display [OPC UA server monitor].

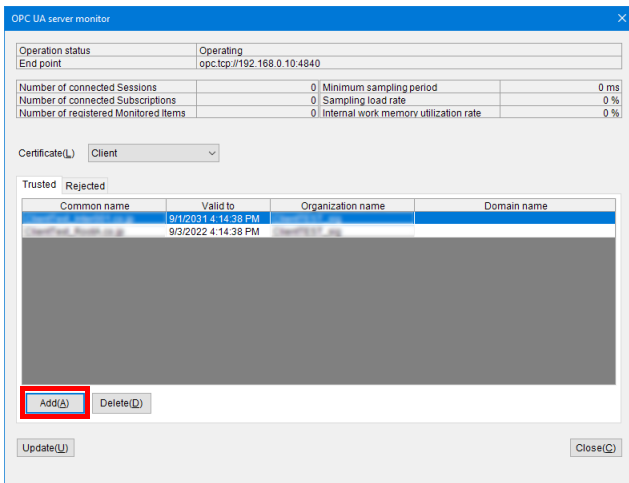
☞ "Displaying [OPC UA server monitor]" (Page 3-6)

2 For [Certificate], select [Client].

3 Select the [Trusted] tab.



4 Click "Add".

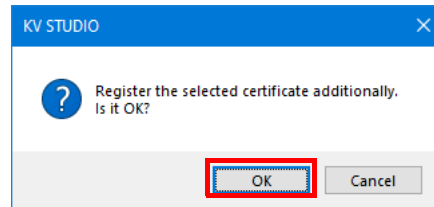


The [Open] dialog box appears.

5 Select the client certificate file (.der extension) to be added and click "Open".

A confirmation dialog box appears.

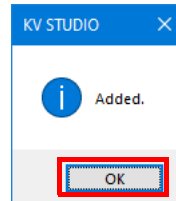
6 Click "OK".



The selected client certificate is added to the CPU unit and displayed on the [Trusted] tab.

Once processing is completed, a dialog box appears.

7 Click "OK".



Reference In addition to adding a client certificate in advance, a client certificate provided by the client at the time of connection can also be automatically added. In accordance with the [Automatic trust of client certificates] setting (☞ Page 2-2) in [OPC UA server settings], a client's client certificate that was not registered at the time of connection request can be automatically registered in the [Trusted] folder or [Rejected] folder.

- Enable: Registered in the [Trusted] folder.
- Disable: Registered in the [Rejected] folder.

If [Enable] is selected, all clients that make a connection request will be trusted, so there may be some clients who will be registered accidentally. Check the list on the [Trusted] tab and delete client certificates that should be rejected as necessary.

☞ "Deleting Client Certificates" (Page 3-12)

• Deploying client certificates

Client certificates are deployed to CPU memory or an SD card according to [OPC UA server settings].

For details about settings, see ☞ "Certificate storage" (Page 2-1).

The destination path is as follows.

Description	Path
[Trusted] folder	cert\unit00\opcua\pk\trusted
[Rejected] folder	cert\unit00\opcua\pk\rejected

- Reference**
- The maximum number of files that can be recognized in the [Trusted] and [Rejected] folders is 32 respectively. If the number of files deployed exceeds the maximum, the system may not function correctly.
 - If a new certificate is sent from a client when the [Automatic trust of client certificates] setting is set to [Enable] and 32 certificates are already registered, connecting will be allowed, but the certificate will not be registered in the [Trusted] folder.

Managing Client Certificate Information

The following functions can be performed on client certificates saved in the CPU unit:

- Display client certificate information (□ Page 3-12): Displays information such as the client certificate's common name and the end of the valid period.
- Display client certificate details (□ Page 3-12): Displays detailed information related to client certificates.
- Allow rejected client certificates (□ Page 3-12): Moves client certificates in the [Rejected] folder to the [Trusted] folder.
- Delete client certificates (□ Page 3-12): Deletes client certificates in the CPU unit.

Displaying Client Certificate Information

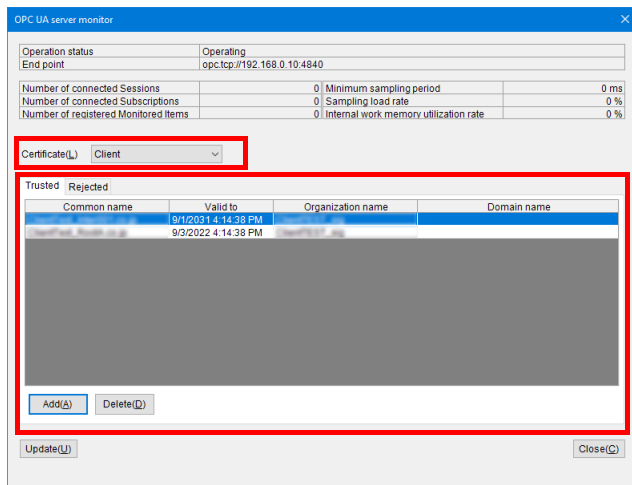
Display client certificate information registered in the [Trusted] folder or [Rejected] folder in the CPU unit.

Display client certificate information via [OPC UA server monitor].

1 Display [OPC UA server monitor].

□ "Displaying [OPC UA server monitor]" (Page 3-6)

2 For [Certificate], select [Client].



The information below is displayed.

Item	Description
[Trusted] tab	Displays client certificates registered in the [Trusted] folder on the CPU unit.
Common name	This is the name of the certificate.
Valid to	This is date and time that the valid period for the certificate ends.
Organization name	This is the name of the organization that issued the certificate.
Domain name	This is the certificate domain name.
[Rejected] tab	Displays client certificate information registered in the [Rejected] folder on the CPU unit.
Common name	Same as the [Trusted] tab.
Valid to	
Organization name	
Domain name	
Trust	Moves certificates registered in the [Rejected] tab to the [Trusted] tab.
Update	Recaptures information for client certificates registered on the CPU unit and refreshes the [Trusted] tab and [Rejected] tab content.

Reference □ Double-clicking a client certificate in the list enables detailed information for that client certificate to be displayed.

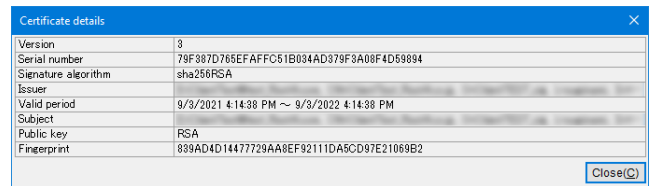
□ "Displaying the Details of Client Certificates" (Page 3-11)

Displaying the Details of Client Certificates

1 On the [Trusted] tab or [Rejected] tab, double-click the certificate on the displayed list.

The [Certificate details] dialog box appears.


Reference □ In some cases, such as if the list display has not been refreshed, the [Certificate details] dialog box may not appear. Click "Update" to refresh the list display and check whether the client certificate is registered on the CPU unit.

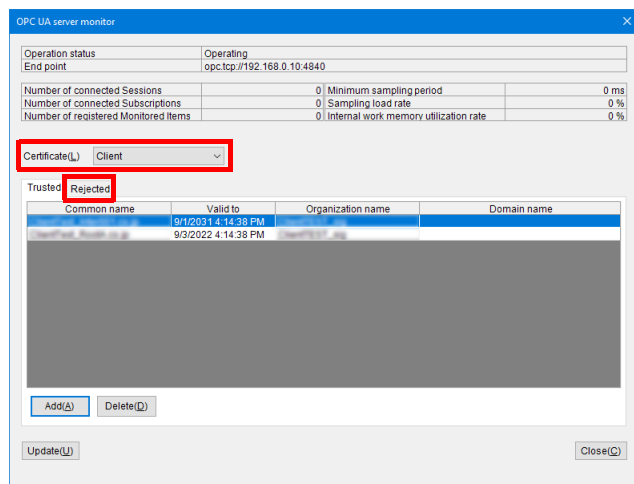


Item	Description
Version	This is the certificate version information.
Serial number	This is the identification number for the certificate.
Signature algorithm	This is the signature algorithm assigned to the certificate.
Issuer	This is the name of the certificate authority that issued the certificate. E.g.) C=JP, S=Osaka, O=KEYENCE CORPORATION, CN=keyence.co.jp
Valid period	This is the period that the certificate is valid for. E.g.) 2021/11/23 11:19:43 to 2041/11/23 11:19:43
Subject	This is the owner of the public key. For a self-signed certificate, this is the same as [Issuer]. E.g.) C=JP, S=Osaka, O=KEYENCE CORPORATION, CN=keyence.co.jp
Public key	This is the applicant's public key and its type.
Fingerprint	This is a check code to prevent certificate tampering.
Close	Closes the [Certificate details] dialog box.

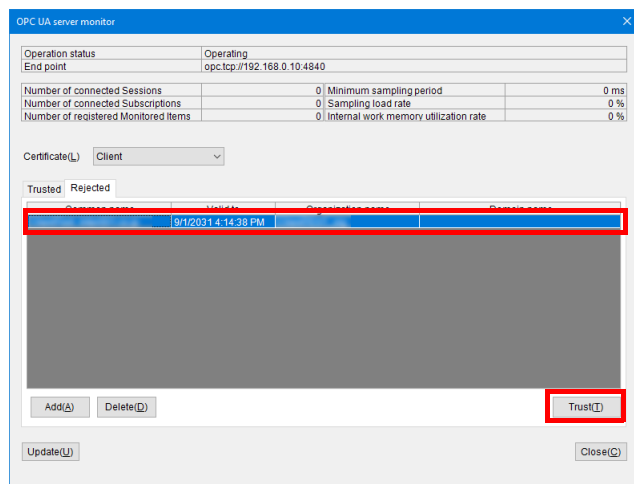
Allowing Rejected Client Certificates

If a client certificate was accidentally registered in the [Rejected] folder, it can be moved from the [Rejected] folder to the [Trusted] folder to allow connecting. Allow a rejected client certificate via [OPC UA server monitor].

- 1 Display [OPC UA server monitor].
 "Displaying [OPC UA server monitor]" (Page 3-6)
- 2 For [Certificate], select [Client].
- 3 Select the [Rejected] tab.



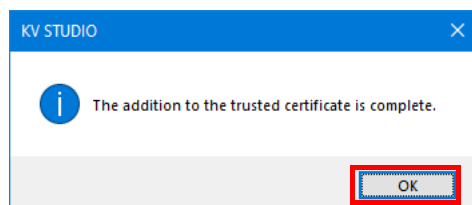
- 4 Select the client certificate to be moved and click "Trust".



The selected client certificate is moved to the [Trusted] folder the [Rejected] tab display is refreshed.

Once processing is completed, a dialog box appears.

- 5 Click "OK".




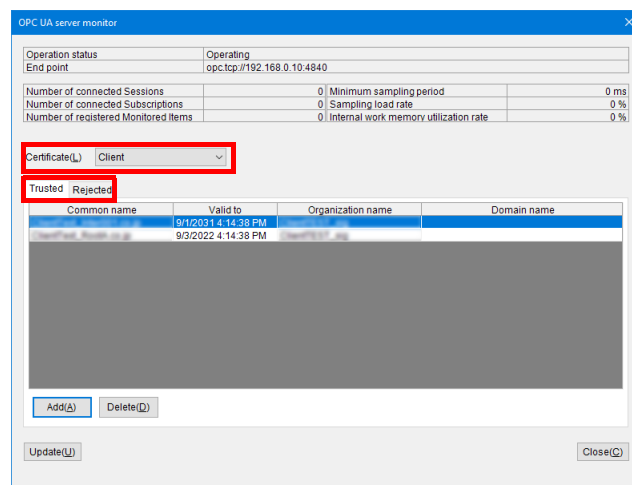
Deleting Client Certificates

Delete a client certificate registered in the [Trusted] folder or [Rejected] folder on the CPU unit.

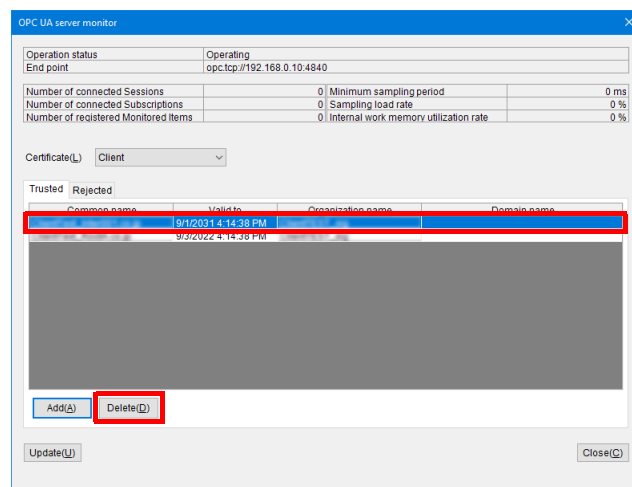
The procedure is the same for both the [Trusted] folder and [Rejected] folder.

Delete a client certificate via [OPC UA server monitor].

- 1 Display [OPC UA server monitor].
 "Displaying [OPC UA server monitor]" (Page 3-6)
- 2 For [Certificate], select [Client].
- 3 Depending on the client certificate to be deleted, select either the [Trusted] tab or [Rejected] tab.

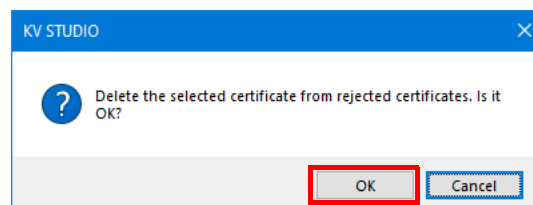


- 4 Select the client certificate to be deleted and click "Delete".



A confirmation dialog box appears.

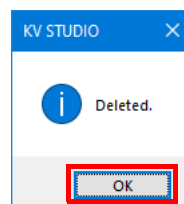
- 5 Click "OK".



The client certificate on the CPU unit is deleted.

Once processing is completed, a dialog box appears.

- 6 Click "OK".



3-5 User Authentication

The OPC UA server functions support user authentication through a user name and password ensuring security with two-factor user authentication in combination with application authentication.

To perform user authentication, perform the following operations:



- Display user information (📖 Page 3-13): Displays a list of users on who user authentication is performed.
- Add a user (📖 Page 3-13): Adds a user on who user authentication is performed.
- Change a user name/password (📖 Page 3-14): Changes the user name and password for the registered user.
- Delete a user (📖 Page 3-14): Deletes a registered user.

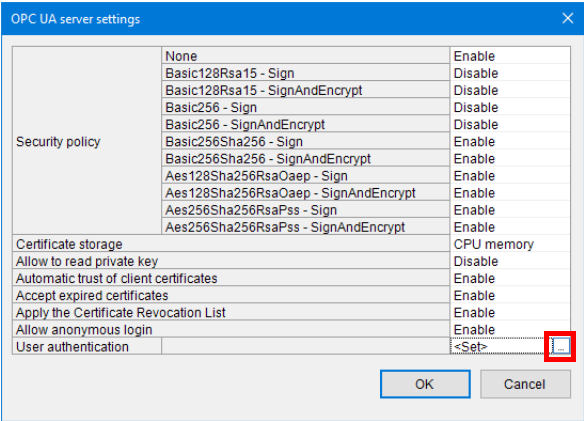
Reference

The OPC UA server functions also supports anonymous login (📖 Page 2-2).
If OPC UA communications cannot be performed successfully, also check whether the anonymous login settings for the CPU unit and OPC UA client match.

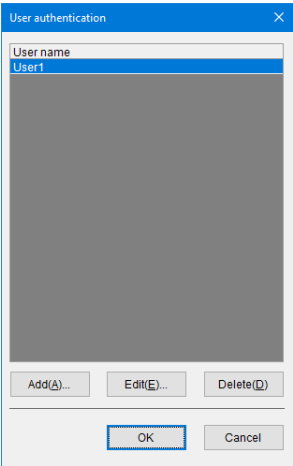
Displaying User Information

Display a list of users on who user authentication is performed.
User information is displayed on the [OPC UA server settings] dialog box.

- 1 In the unit editor, select [OPC UA server settings] - [OPC UA server settings] and then click  .
The [OPC UA server settings] dialog box will appear.
- 2 For [User authentication], click <Set> and then click  that appears.



The [User authentication] dialog box will appear and display a list of registered user names.

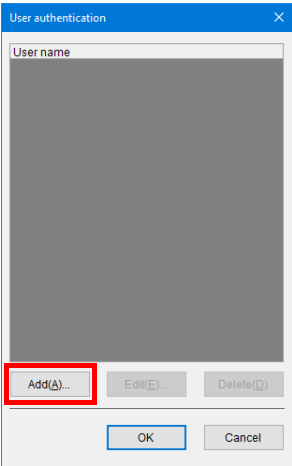


Item	Description
User name	Displays a list of names of users on who user authentication is performed.
Add	Click this button to add a user on who user authentication is performed. 📖 "Adding a User" (Page 3-13)
Edit	Click this button to change the user name and password of a registered user. 📖 "Changing a User Name/Password" (Page 3-14)
Delete	Click this button to delete a registered user. 📖 "Deleting a User" (Page 3-14)

Adding a User

Add a user on who user authentication is performed.

- 1 Display the [User authentication] dialog box.
📖 "Displaying User Information" (Page 3-13)
- 2 Click "Add".

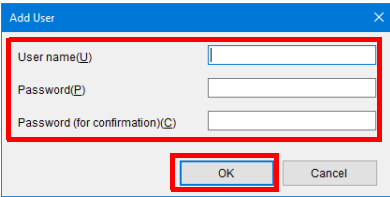


The [Add User] dialog box appears.

- 3 Enter a user name into [User name (U)] and the same password into [Password (P)] and [Password (for confirmation) (C)], and then click "OK".

Point

A user name and password can only be used in ASCII code.




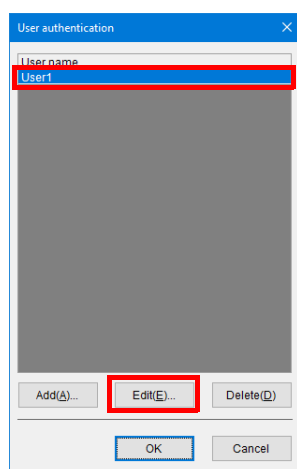
A user name will appear in [User name] on the [User authentication] dialog box.

- 4 Click "OK".
The user is added.
Clicking "Cancel" discards any changes to the settings and closes the [User authentication] dialog box.

Changing a User Name/Password

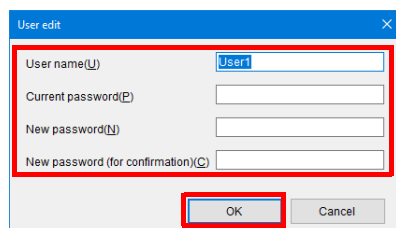
Change the user name and password of a registered user.

- 1 Display the [User authentication] dialog box.
 "Displaying User Information" (Page 3-13)
- 2 Select the user name to change the user name and/or password, and click "Edit".



The [User edit] dialog box appears.

- 3 To change a user name, enter a user name in [User name (U)], and passwords in [Current password (P)], [New password (N)], and [New password (for confirmation) (C)], and then click "OK".



The display returns to the [User authentication] dialog box.


- 4 Click "OK".

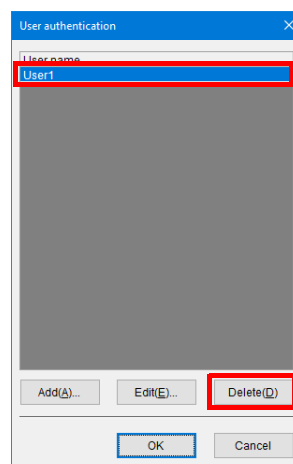
The changes are now set.

Clicking "Cancel" discards any changes and closes the [User authentication] dialog box.

Deleting a User

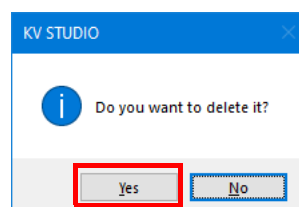
Delete a registered user.

- 1 Display the [User authentication] dialog box.
 "Displaying User Information" (Page 3-13)
- 2 Select the user to be deleted and click "Delete".



A confirmation dialog box appears.

- 3 Click "Yes".



The display returns to the [User authentication] dialog box.

- 4 Click "OK".

The user is now deleted.

Clicking "Cancel" discards the deletion and closes the [User authentication] dialog box.

Chapter 4 Settings for OPC UA Communications

Create variables and set as targets to read and write from the OPC UA client using OPC UA communications. Variables set as the target of communications are published based on the OPC UA address space and are readable and writable from the OPC UA client.

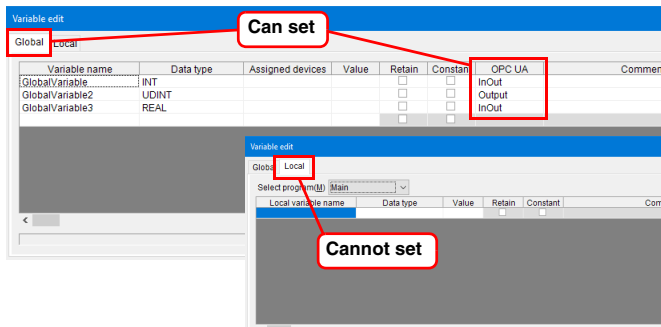
This section describes the requirements of variables that can be created and how to set them.

4-1 Variables

This section describes variables that can be set as variables that can be read and written from the OPC UA client as targets of OPC UA communications.

Types of variables

Only global variables can be set as targets of OPC UA communications. Local variables cannot be set as targets of OPC UA communications.



Data types

Data types that can and cannot be set are as follows.

O: Can set x: Cannot set

Data type	Setting	Description
BOOL	O	Bit
UINT	O	One-word unsigned integer
INT	O	One-word signed integer
UDINT	O	Two-word unsigned integer
DINT	O	Two-word signed integer
REAL	O	Single-precision floating-point format
LREAL	O	Double-precision floating-point format
STRING ^{*1}	O	Strings
TIMER	x	Timer
COUNTER	x	Counter
ARRAY	O	Array
Structure	O	A structure that has an above data type that can be set as a member.

^{*1} Character codes handled by the STRING data type conform with languages set with the project language settings. For details about project language settings, see "KV STUDIO User's Manual."



When specifying variables on the OPC UA client, specify them in accordance with the OPC UA address space.

☞ "6-2 Reading and Writing Variables from an OPC UA Client" (Page 6-2)

Number of variables that can be set

There is a limit to the number of variables that can be set as targets of OPC UA communications.

Item	Limit
Number of variables	Max. 200,000 ^{*1}

^{*1} Includes the number of structural members and array elements.

4-2 Setting Variables

This section describes the procedure to create and set variables that are targets of OPC UA communications.

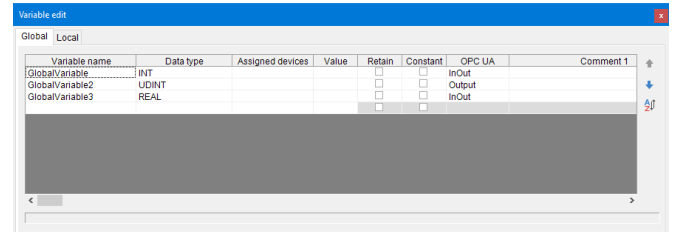
Configure the settings on the [Variable edit] window in "KV STUDIO".



Variable settings can be edited with [Editor] or [Online edit]. Editing cannot be performed in [Monitor] mode.

- On the menu, select "View (V)" - "Variable edit window (L)".
- Create a variable and set it as a target for OPC UA communications.

For details about how to create a variable, see "KV STUDIO User's Manual".



Item	Description
Global	Select [Global] as a type of variable to be defined. [Local] cannot be set as a target of OPC UA communications.
Variable name	Enter a name for the variable. Up to 128 alphanumeric characters can be entered irrespective of whether they are full- or half-width characters.
Data type	Set the variable data type. BOOL/UINT/INT/UDINT/DINT/REAL/LREAL/STRING/ARRAY/Structure
Assigned device	Set this option when manually allocating variables to the CPU unit device. Allocation is not required.
Value	<ul style="list-style-type: none"> Selecting the [Constant] check box: Specify the default values for the variable. If the [Constant] check box is selected, the values are fixed and cannot be changed. Clearing the [Constant] check box: Set the default values for the variable. The values can be changed to something other than the default values with the unit program or web dashboard.
Retain	The values are retained even if the CPU unit power is turned off.
Constant	Variables for which this check box is selected are handled as constants.
OPC UA	Sets the publish range for reading and writing of the OPC UA communications.. <ul style="list-style-type: none"> Private (default setting): The variable is not set as a target of OPC UA communications and cannot be read or written from the OPC UA client. InOut: The variable is set as a target of OPC UA communications and can be read and written from the OPC UA client. Output: The variable is set as a target of OPC UA communications and can only be read from the OPC UA client. The variable cannot be written to.
Comment 1 to Comment 8	Enter a comment for the variable. Up to 128 alphanumeric characters can be entered irrespective of whether they are full- or half-width characters.

Chapter 5 Monitoring Features

This chapter uses the "KV STUDIO" monitoring features to describe how to check the OPC UA server status and the variable read/write history from an OPC UA client.

- OPC UA server status (□□ Page 5-1): Can be checked with [OPC UA server monitor].

The registration status of certificates used for authentication and operation of certificates can also be checked via [OPC UA server monitor].

For details about certificate information, see the following sections:

□□ "3-3 Server Certificates" (Page 3-4)

□□ "3-4 Client Certificates" (Page 3-9)

□□ "A-1 CA-signed Client Certificates" (Page A-1)


- Variable read/write history from the OPC UA client (□□ Page 5-2): As this is recorded as device value changes, it can be checked on [Event/error monitor].

For details about how to operate [Event/error monitor], see □□ "KV STUDIO User's Manual".

5-1 Checking the Server Status

This section describes the procedures to check the OPC UA server status and what items can be checked via [OPC UA server monitor].

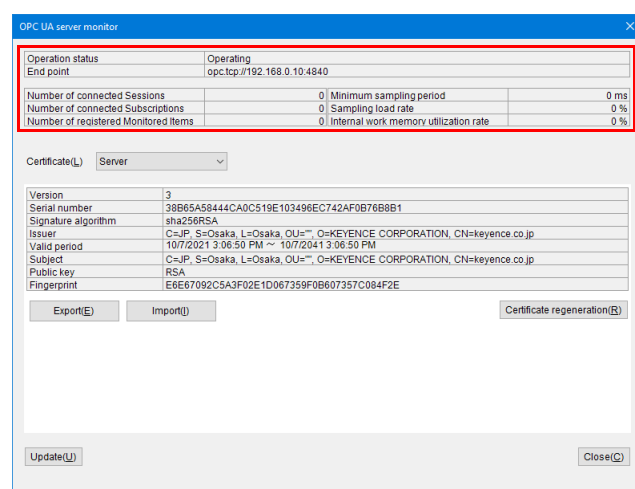
- 1 Change "KV STUDIO" to monitoring mode, online edit mode, or replay mode.

 **Point** [OPC UA server monitor] can only be displayed when "KV STUDIO" is in [Monitor], [Online edit] or [Replay] mode.
For details about [Monitor], [Online edit], and [Replay] modes, see □□ "KV STUDIO User's Manual".


- 2 Right-click the CPU unit in [Unit configuration] on the workspace and on the menu that appears, click "OPC UA server monitor (E)".

[OPC UA server monitor] appears.

- 3 Check the server status.




Item	Description
Number of registered monitored items	Displays the number of monitored items registered to the connected OPC UA client.
Minimum sampling period	Displays the minimum sampling cycle requested by the connected OPC UA client.
Sampling load rate	Displays the value for the sampling processing time/sampling cycle. If it exceeds 100%, it means that the sampling process cannot be completed within the sampling time. Sampling processing is executed within the END processing time of the CPU unit. If the sampling load factor is high, the processing of other communication functions executed within the END processing time may also be delayed. You may be able to reduce the delay by reducing the variables registered in the monitor item by grouping them as a structure, or by extending the END processing time setting of the CPU system settings.
Internal work memory utilization rate	Displays the use ratio of the work memory in the KV-8000(A). If the connection with the OPC UA client is unstable, check the value for the internal work memory utilization rate. If this value has exceeded 80%, it may mean that the load is too great. Reduce the load by reducing the number of registered monitored items and/or reducing the number of connected clients.
Update	Clicking this button refreshes the server status with the current details of the CPU unit.
Close	Clicking this button closes [OPC UA server monitor].

 **Reference** Changing the type of certificate for [Certificate] enables the registered details of certificates to be checked and operated. For details, see the following sections:

□□ "3-3 Server Certificates" (Page 3-4)

□□ "3-4 Client Certificates" (Page 3-9)

□□ "A-1 CA-signed Client Certificates" (Page A-1)

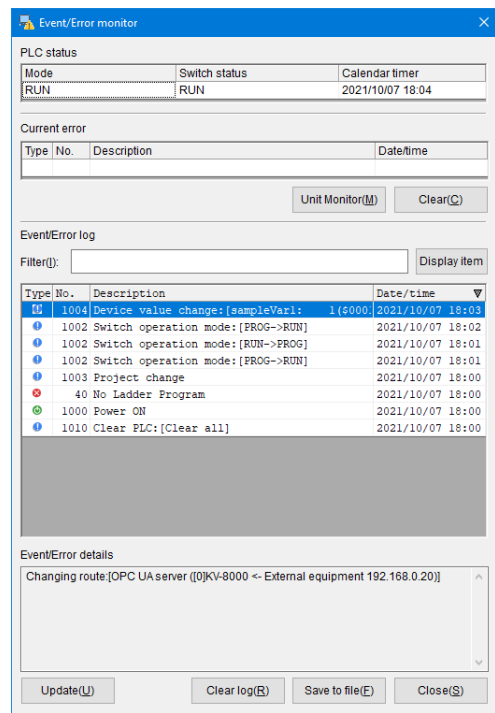
Item	Description
Operation status	The operation status (operating/stopped) for the OPC UA server appears.  Point The OPC UA server function will stop in the following cases: <ul style="list-style-type: none"> • [OPC UA server enabled] is set to [Disable] • The CPU unit is running • A project is being forwarded • A project is loading • The PLC is being cleared
End point	The endpoint URL for the OPC UA server is displayed. The endpoint URL can be set with the unit editor. □□ "2-2 CPU Unit Settings" (Page 2-3)
Number of connected sessions	The number of connected OPC UA clients (sessions) is displayed.
Number of connected subscriptions	The number of connected subscriptions is displayed.

5-2 Checking the History of Device Value Changes for Variables

This section describes the procedures for checking the history of device value changes for variables and what items can be checked from an OPC UA client on [Event/Error monitor].

1 On the menu, click "Debug (D)" - "Event/Error monitor (E)".

[Event/Error monitor] appears.



2 Check the history of device value changes for variables on [Event/Error log].


• Items that can be checked

Writing to a variable from an OPC UA client is recorded as a device value change.

For details about other displayed items via [Event/Error monitor], see [KV STUDIO User's Manual](#).

Chapter 6 Connecting from the OPC UA Client and Reading and Writing Variables

This section describes how to connect to the OPC UA server from an OPC UA client and information required when reading and writing variables from the OPC UA client.

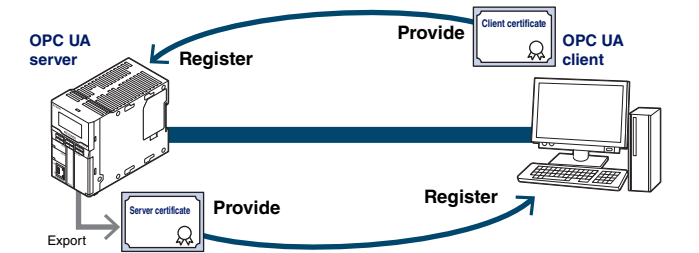
 Point

For details about operating an OPC UA client, see the instruction manual for the applicable OPC UA client software.

6-1 Connecting to the OPC UA Server


Preparing Certificates

To setup security, server and client certificates must be prepared before connecting.



- Registering a server certificate
A server certificate must be accepted from the OPC UA server and registered as a trusted destination in advance.
□ "Exporting a Server Certificate" (Page 3-5)
- Providing a client certificate
To connect to the OPC UA server, the OPC UA client must be recognized as a legitimate user by the OPC UA server.
Therefore, a client certificate for the OPC UA client that will connect to the OPC UA server must be created, provided to the OPC UA server, and registered as a trusted destination.
□ "Managing Client Certificate Information" (Page 3-11)

The OPC UA server function also supports a CA-signed client certificate. In that case, a CA-signed client certificate, CA certificate, and certificate revocation list are required.
□ "Managing CA-signed Client Certificates, CA Certificates, and Certificate Revocation Lists" (Page A-4)

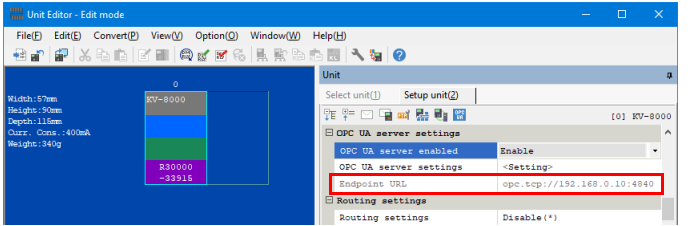
 Point

As the security policy is set to [None] by default, setting the client to [None] also enables communications without using a client certificate.

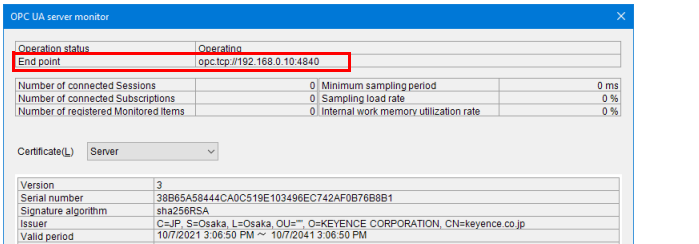
Destination URL

Specify the OPC UA server endpoint URL as the OPC UA client destination.
Format: `opc.tcp:// [IP address] : [Port No.]`

The endpoint URL can be checked with the unit editor or via [OPC UA server monitor].



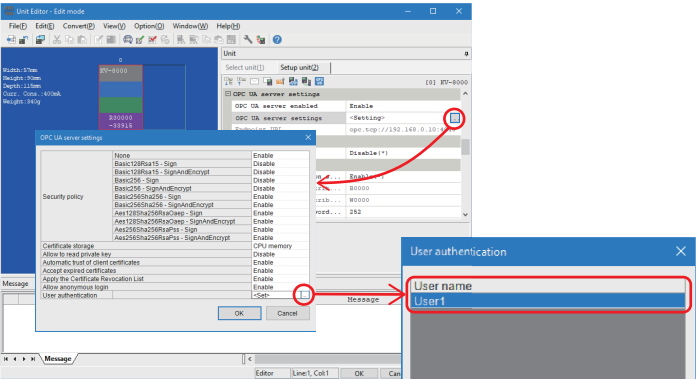
□ "2-2 CPU Unit Settings" (Page 2-3)



□ "5-1 Checking the Server Status" (Page 5-1)

User Name and Password

To perform user authentication when connecting to the OPC UA server, set the user name and password set in [User authentication] for [OPC UA server settings].



□ "User Authentication" (Page 3-13)

6-2 Reading and Writing Variables from an OPC UA Client

Reading and writing of variables from an OPC UA client is performed in accordance with the OPC UA address space.

This section describes variables set as targets of OPC UA communications and support for the OPC UA address space in "KV STUDIO".

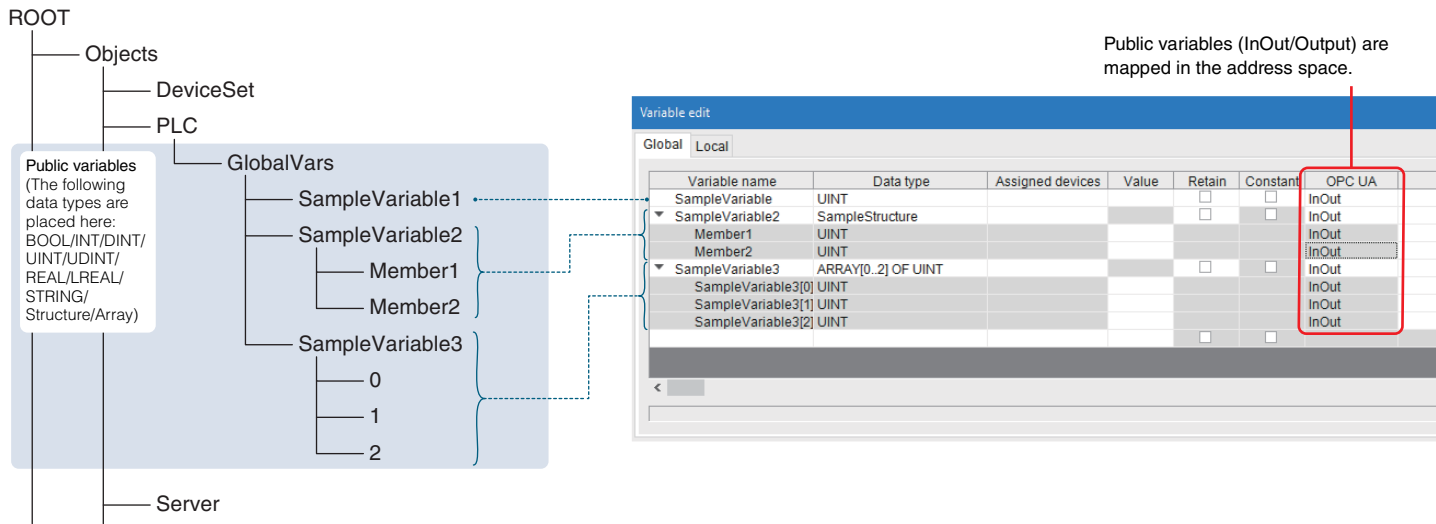
For details about creating and setting variables as communications targets, see ["Chapter 4 Settings for OPC UA Communications"](#) (Page 4-1).

Support for the OPC UA Address Space and Variables

The OPC UA address space and target variables set with "KV STUDIO" are supported as follows:

- Data types are BOOL/INT/DINT/UINT/UDINT/REAL/LREAL/STRING/Structure/Array variables.
Published as variables and placed under GlobalVars.
- Structure variable members and array elements are deployed as child node variables.

Specify variables from the OPC UA client on the OPC UA address space.



Mapping of Variables and Attributes

Variable names, data types, values, and other settings are mapped to the data type of nodes in the address space.

This section describes the mapping of the main "KV STUDIO" and OPC UA data types.

Point Only variables with a publish range of [InOut] or [Output] are mapped to the address space. [Private] variables are not mapped.

Reference For detailed node data types and their values, see the OPC UA address space standards.

KV STUDIO settings	Address space attributes	Description																		
Variable name	BrowseName or DisplayName	Variable names are not case sensitive.																		
Data type	DataType	<div>Data types supported by KV STUDIO and OPC UA are as follows.<table><tr><th>KV STUDIO</th><th>OPC UA</th></tr><tr><td>BOOL</td><td>Boolean</td></tr><tr><td>INT</td><td>Int16</td></tr><tr><td>DINT</td><td>Int32</td></tr><tr><td>UINT</td><td>UInt16</td></tr><tr><td>UDINT</td><td>UInt32</td></tr><tr><td>REAL</td><td>Float</td></tr><tr><td>LREAL</td><td>Double</td></tr><tr><td>STRING</td><td>String</td></tr></table><div>For the structure type, the structure name is noted in DataType. For the array type, the array data type is noted in DataType.</div></div>	KV STUDIO	OPC UA	BOOL	Boolean	INT	Int16	DINT	Int32	UINT	UInt16	UDINT	UInt32	REAL	Float	LREAL	Double	STRING	String
KV STUDIO	OPC UA																			
BOOL	Boolean																			
INT	Int16																			
DINT	Int32																			
UINT	UInt16																			
UDINT	UInt32																			
REAL	Float																			
LREAL	Double																			
STRING	String																			
Value	Value	A value is set in accordance with the data type.																		

Reading and Writing Variables

Device values can be read and written in accordance with the disclosure range (["Page 4-1"](#)).

As device value changes are recorded as CPU unit events, the revision history can be checked on [Event/Error monitor].

["5-2 Checking the History of Device Value Changes for Variables"](#) (Page 5-2)

Appendix

A-1 CA-signed Client Certificates

The OPC UA server functions support self-signed client certificates as well as CA-signed client certificates.

Client trustworthiness can be ensured by using a client certificate to prove a third party's identity when connecting to the OPC UA server via a global network.

This section describes the OPC UA server functions related to authentication when using CA-signed client certificates.

Authentication Using CA-signed Client Certificates

If using CA-signed client certificates for application authentication, communications are possible by just registering the CA certificate, which is to approve the CA signature on the OPC UA server, in the [Trusted] folder as long as the CA-signed client certificate is retained on the OPC UA client, even if client certificates issued by each client are not used (the [Revocation] folder that contains the certificate revocation list must also be created. It's alright if no items are registered in the certificate revocation list).

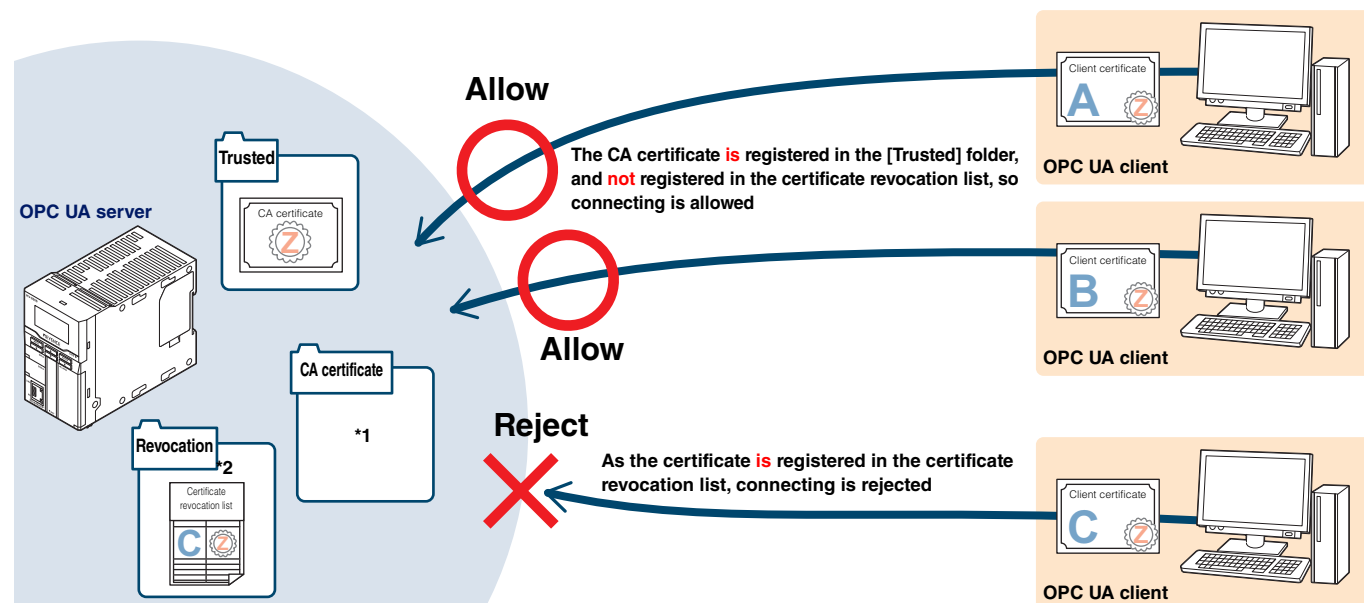
The "Certificate revocation list" is a list of client certificates that were revoked before they expired due to the fact that the certificate information was changed (organization name, IP address, and so on), the certificate leaked, or some other reason for client certificates issued by a CA. Connections by client certificates in this list are rejected.

- Authenticating all clients authenticated by a specific CA

Registering CA certificates authenticated by the applicable CA in the [Trusted] folder enables connecting to be allowed from devices that have the client certificate signed by the registered CA without having to register client certificates individually.

Client certificates sent together with a request to start connecting from the OPC UA client are allowed to connect if they satisfy the following conditions:

- The CA certificate is registered in the [Trusted] folder.
- The certificate is not on the certificate revocation list in the [Revocation] folder.
- A [Revocation] folder that contains a certificate revocation list exists.



*1 To use an intermediate CA certificate other than a root CA, such as a CA proved by the root CA (which is called an intermediate CA) as a root CA, as CA certificates up to the root CA other than CA certificates registered in the [Trusted] folder must be registered in the [CA certificate] folder.

*2 In the case of intermediate CA certificates, all certificate revocation lists up to the root CA must be registered in the [Revocation] folder in order to connect. CA certificates which are on the certificate revocation list will no longer be able to connect to the target and other intermediate CAs which are certified by that CA. Devices with a client certificate which are registered in the certificate revocation list cannot be connected to.

- The method to register a CA-signed client certificate and a CA certificate in the [Trusted] folder is the same as the procedure to register a self-signed client certificate.
 - ☐ "Registering Additional Client Certificates" (Page 3-10)
- Manually register CA certificates beforehand in the [CA certificate] and [Revocation] folders for the certificate revocation list via [OPC UA server monitor].
 - ☐ Adding a CA certificate : ☐ "Registering a CA Certificate" (Page A-2)
 - ☐ Adding a certificate revocation list : ☐ "Registering a Certificate Revocation List" (Page A-3)

- Reference**
- Whether to apply the certificate revocation list or not can be changed in the [Apply the Certificate Revocation List] settings in [OPC UA server settings].
 - ☐ "Apply the Certificate Revocation List" (Page 2-2)
 - Information for registered CA-signed client certificates, CA certificates, and certificate revocation lists can be managed via [OPC UA server monitor].
 - ☐ "Managing CA-signed Client Certificates, CA Certificates, and Certificate Revocation Lists" (Page A-4)

Registering a CA Certificate

Register a CA certificate file (.der extension) in the CPU unit.
Register a CA certificate on [OPC UA server monitor].

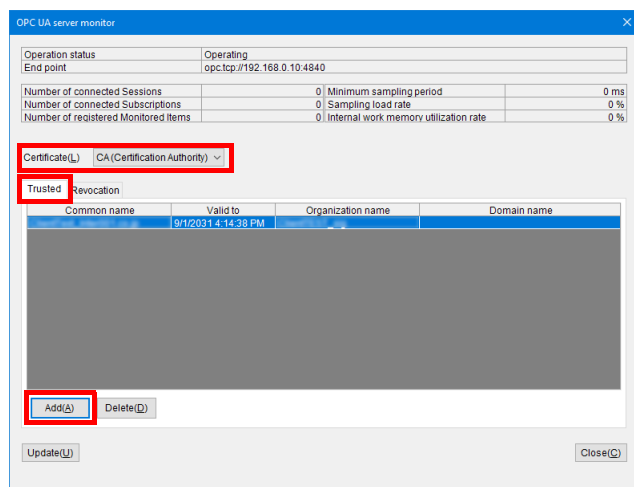
- Point**
- Double check that the CA certificate being registered can be trusted.
If a CA certificate issued by a CA for which connection should not be allowed is accidentally registered in the [Trusted] folder for [Client], all clients using certificates signed by that CA are allowed to connect. As a result, confidential information on the server may be leaked and unauthorized operations may be performed.
 - If a signed CA is an intermediate CA, register all CA certificates up to the root CA.

1 Display [OPC UA server monitor].

☞ "Displaying [OPC UA server monitor]" (Page 3-6)

2 For [Certificate], select [CA (Certification Authority)].

3 Display the [Trusted] tab and click "Add".

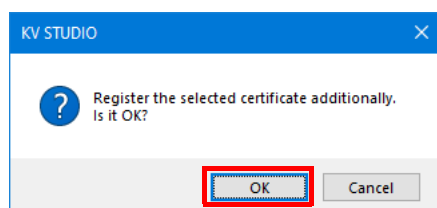


The [Open] dialog box appears.

4 Select the CA certificate file (.der extension) to be added and click "Open".

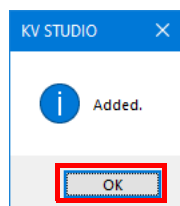
A confirmation dialog box appears.

5 Click "OK".



The selected certificate is added to the CPU unit and displayed on the [Trusted] tab.
Once processing is completed, a dialog box appears.

6 Click "OK".



CA Certificate Destination

CA certificates are deployed to CPU memory or an SD card according to [OPC UA server settings].

For details about settings, see ☞ "Certificate storage" (Page 2-1).

The destination is as follows.

Description	Path
[CA certificate] folder	cert\unit00\opcua\pk\issuer ^{*1}

^{*1} For details about the destination path for client certificates registered in [Trusted] for [Client], see ☞ "Deploying client certificates" (Page 3-10).

Reference The maximum number of files that can be recognized in the [CA certificate] folder is 32. If the number of files deployed exceeds the maximum, the system may not function correctly.

Registering a Certificate Revocation List

Register a certificate revocation list (.crl extension) in the CPU unit.
Add lists via [OPC UA server monitor].

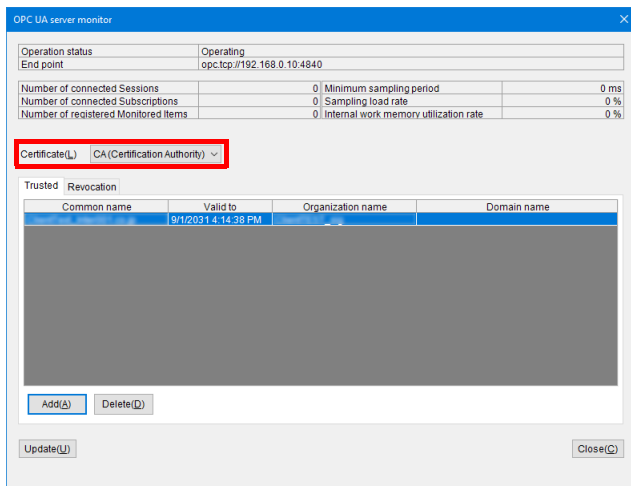


- CA certificates which are on the certificate revocation list will no longer be able to connect to the target and other intermediate CAs which are certified by that CA.
- Devices with a client certificate which are registered in the certificate revocation list cannot be connected to.
- Certificate revocation lists must be registered in the [Revocation] folder in order to connect.
- In the case of intermediate CA certificates, all certificate revocation lists up to the root CA must be registered in the [Revocation] folder in order to connect.

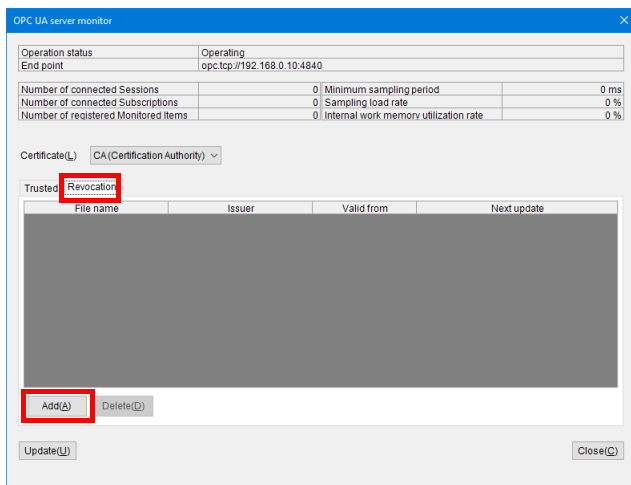
1 Display [OPC UA server monitor].

☞ "Displaying [OPC UA server monitor]" (Page 3-6)

2 For [Certificate], select [CA (Certification Authority)].



3 Display the [Revocation] tab and click "Add".

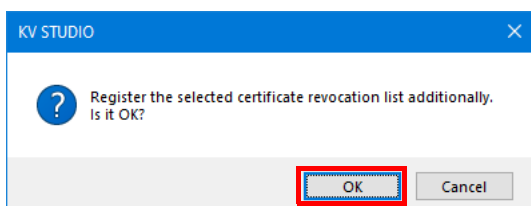


The [Open] dialog box appears.

4 Select the certificate revocation list to be added (.crl extension) and click "Open".

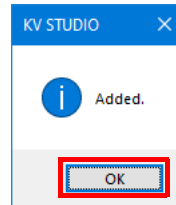
A confirmation dialog box appears.

5 Click "OK".



The selected certificate revocation list is registered in the CPU unit.
Once processing is completed, a dialog box appears.

6 Click "OK".



• Certificate revocation list destination

The certificate revocation list is deployed to CPU memory or an SD card according to [OPC UA server settings].

For details about settings, see ☞ "Certificate storage" (Page 2-1).

The destination is as follows.

Description	Path
[Revocation] folder	cert\unit00\opcua\pki\crl



The maximum number of files that can be recognized in the [Revocation] folder is 32. If the number of files deployed exceeds the maximum, the system may not function correctly.

Managing CA-signed Client Certificates, CA Certificates, and Certificate Revocation Lists

The OPC UA server functions can run the following features for CA-signed client certificates and certificate revocation lists:

- Display and delete CA-signed client certificate information: This is the same procedure as for self-signed client certificates. See the procedure for self-signed client certificates:
 - "Displaying Client Certificate Information" (Page 3-11)
 - "Displaying the Details of Client Certificates" (Page 3-11)
 - "Deleting Client Certificates" (Page 3-12)
- Display CA certificate and certificate revocation list information (□ Page A-4): Displays CA certificate and certificate revocation list information registered on the CPU unit.
- Display detailed CA certificate information (□ Page A-4): Displays detailed information about CA certificates registered on the CPU unit.
- Display certificate revocation list details (□ Page A-4): Displays details about certificate revocation lists registered on the CPU unit.
- Delete CA certificates and certificate revocation lists (□ Page A-5): Deletes CA certificates and certificate revocation lists registered on the CPU unit.

Displaying CA Certificates and Certificate Revocation Lists

This section describes the displaying of CA certificates and certificate revocation lists deployed on the CPU unit.

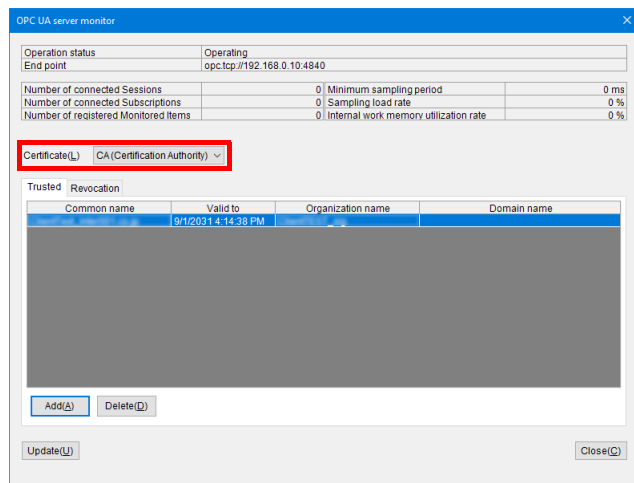
The method to display client certificate information is the same as for displaying a self-signed client certificate. See □ "Managing Client Certificate Information" (Page 3-11).

CA certificates and certificate revocation lists are displayed via [OPC UA server monitor].

1 Display [OPC UA server monitor].

□ "Displaying [OPC UA server monitor]" (Page 3-6)

2 For [Certificate], select [CA (Certification Authority)].



The information below is displayed.

Item	Description of feature
[Trusted] tab	Displays CA certificates deployed on the CPU unit.
Common name	This is the name of the certificate.
Valid to	This is the date and time that the valid period for the certificate ends.
Organization name	This is the name of the organization that issued the certificate.
Domain name	This is the certificate domain name.
[Revocation] tab	Displays the certificate revocation lists deployed on the CPU unit.
File name	This is the file name of the certificate revocation list.
Issuer	This is the name of the certificate authority that issued the certificate revocation list.
Valid from	This is the start date and time of the valid period for the certificate revocation list.
Next update	This is the date and time of the next update for the certificate revocation list.

Reference □ Double-clicking a CA certificate or certificate revocation list in the list displays detailed information for that CA certificate or certificate revocation list.

□ "Displaying Details of CA Certificates" (Page A-4)

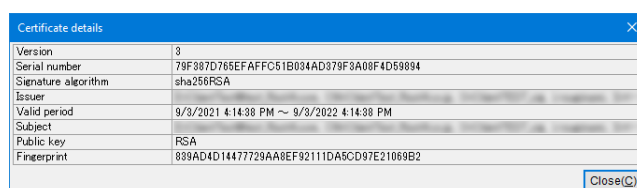
□ "Displaying the Details of a Certificate Revocation List" (Page A-5)

Displaying Details of CA Certificates

1 On the [Trusted] tab, double-click the certificate on the displayed list.

The [Certificate details] dialog box appears.

Reference □ In some cases, such as if the list display has not been refreshed, the [Certificate details] dialog box may not appear. Click [Update] to refresh the list display and check whether the CA certificate is registered on the CPU unit.



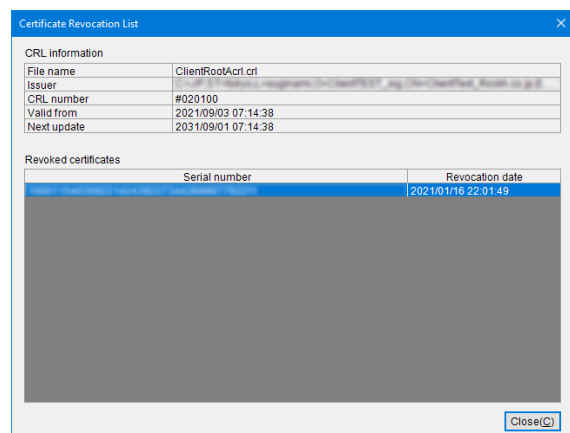
Item	Description
Version	This is the certificate version information.
Serial number	This is the identification number for the certificate.
Signature algorithm	This is the signature algorithm assigned to the certificate.
Issuer	This is the name of the certificate authority that issued the certificate. E.g.) C=JP, S=Osaka, O=KEYENCE CORPORATION, CN=keyence.co.jp
Valid period	This is the period that the certificate is valid for. E.g.) 2021/11/23 11:19:43 to 2041/11/23 11:19:43
Subject	This is the owner of the public key. For a self-signed certificate, this is the same as [Issuer]. E.g.) C=JP, S=Osaka, O=KEYENCE CORPORATION, CN=keyence.co.jp
Public key	This is the applicant's public key and its type.
Fingerprint	This is a check code to prevent certificate tampering.
Close	Closes the [Certificate details] dialog box.

Displaying the Details of a Certificate Revocation List

- 1 On the [Revocation] tab, double-click the certificate revocation list on the displayed list.

The [Certificate Revocation list] dialog box appears.

Reference In some cases, such as if the list display has not been refreshed, the [Certificate Revocation list] dialog box may not appear. Click "Update" to refresh the list display and check whether the certificate revocation list is registered on the CPU unit.



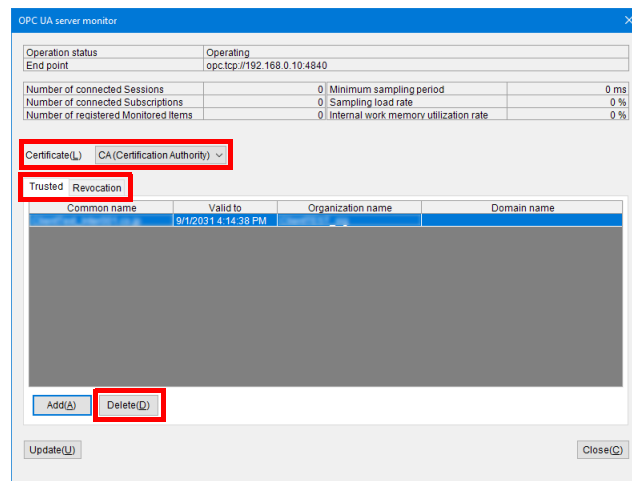
Item	Description of feature
File name	This is the file name of the certificate revocation list.
Issuer	This is the name of the certificate authority that issued the certificate revocation list. E.g.) C=JP,S=Osaka,O=KEYENCE CORPORATION, CN=keyence.co.jp
CRL number	This is the number to indicate the issue order of the certificate revocation lists.
Valid from	This is the start date and time of the valid period for the certificate revocation list.
Next update	This is the date and time of the next update for the certificate revocation list.
Serial number	This is the serial number of the revoked certificate.
Revocation date	This is the date and time that the certificate was revoked.

Deleting a CA Certificate or Certificate Revocation List

Delete a CA certificate or certificate revocation list on the CPU unit.

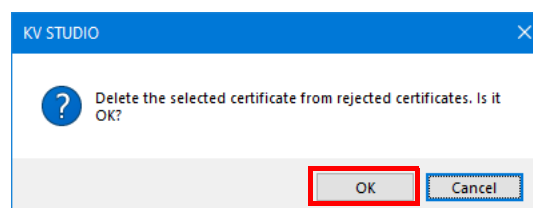
Delete a CA certificate or certificate revocation list via [OPC UA server monitor].

- 1 Display [OPC UA server monitor].
"Displaying [OPC UA server monitor]" (Page 3-6)
- 2 For [Certificate], select [CA (Certification Authority)].
- 3 Depending on whether a CA certificate or a certificate revocation list is being deleted, select either the [Trusted] tab or [Revocation] tab.
- 4 Select the CA certificate or certificate revocation list to be deleted and click "Delete".



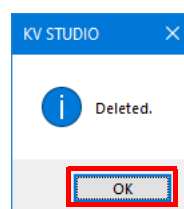
The confirmation dialog box appears.

- 5 Click "OK".



The selected CA certificate or certificate revocation list is deleted. Once processing is completed, a dialog box appears.

- 6 Click "OK".



Revision History

[illegible]

WARRANTIES AND DISCLAIMERS

- (1) KEYENCE warrants the Products to be free of defects in materials and workmanship for a period of one (1) year from the date of shipment. If any models or samples were shown to Buyer, such models or samples were used merely to illustrate the general type and quality of the Products and not to represent that the Products would necessarily conform to said models or samples. Any Products found to be defective must be shipped to KEYENCE with all shipping costs paid by Buyer or offered to KEYENCE for inspection and examination. Upon examination by KEYENCE, KEYENCE, at its sole option, will refund the purchase price of, or repair or replace at no charge any Products found to be defective. This warranty does not apply to any defects resulting from any action of Buyer, including but not limited to improper installation, improper interfacing, improper repair, unauthorized modification, misapplication and mishandling, such as exposure to excessive current, heat, coldness, moisture, vibration or outdoors air. Components which wear are not warranted.
- (2) KEYENCE is pleased to offer suggestions on the use of its various Products. They are only suggestions, and it is Buyer's responsibility to ascertain the fitness of the Products for Buyer's intended use. KEYENCE will not be responsible for any damages that may result from the use of the Products.
- (3) The Products and any samples ("Products/Samples") supplied to Buyer are not to be used internally in humans, for human transportation, as safety devices or fail-safe systems, unless their written specifications state otherwise. Should any Products/Samples be used in such a manner or misused in any way, KEYENCE assumes no responsibility, and additionally Buyer will indemnify KEYENCE and hold KEYENCE harmless from any liability or damage whatsoever arising out of any misuse of the Products/Samples.
- (4) **OTHER THAN AS STATED HEREIN, THE PRODUCTS/SAMPLES ARE PROVIDED WITH NO OTHER WARRANTIES WHATSOEVER. ALL EXPRESS, IMPLIED, AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF PROPRIETARY RIGHTS, ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL KEYENCE AND ITS AFFILIATED ENTITIES BE LIABLE TO ANY PERSON OR ENTITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, ANY DAMAGES RESULTING FROM LOSS OF USE, BUSINESS INTERRUPTION, LOSS OF INFORMATION, LOSS OR INACCURACY OF DATA, LOSS OF PROFITS, LOSS OF SAVINGS, THE COST OF PROCUREMENT OF SUBSTITUTED GOODS, SERVICES OR TECHNOLOGIES, OR FOR ANY MATTER ARISING OUT OF OR IN CONNECTION WITH THE USE OR INABILITY TO USE THE PRODUCTS, EVEN IF KEYENCE OR ONE OF ITS AFFILIATED ENTITIES WAS ADVISED OF A POSSIBLE THIRD PARTY'S CLAIM FOR DAMAGES OR ANY OTHER CLAIM AGAINST BUYER.** In some jurisdictions, some of the foregoing warranty disclaimers or damage limitations may not apply.

BUYER'S TRANSFER OBLIGATIONS:

If the Products/Samples purchased by Buyer are to be resold or delivered to a third party, Buyer must provide such third party with a copy of this document, all specifications, manuals, catalogs, leaflets and written information provided to Buyer pertaining to the Products/Samples.

Specifications are subject to change without notice.

KEYENCE CORPORATION

1-3-14, Higashi-Nakajima, Higashi-Yodogawa-ku, Osaka, 533-8555, Japan PHONE: +81-6-6379-2211

www.keyence.com/glb

AUSTRIA

Phone: +43 (0)2236 378266 0

BELGIUM

Phone: +32 (0)15 281 222

BRAZIL

Phone: +55-11-3045-4011

CANADA

Phone: +1-905-366-7655

CHINA

Phone: +86-21-3357-1001

CZECH REPUBLIC

Phone: +420 220 184 700

FRANCE

Phone: +33 1 56 37 78 00

GERMANY

Phone: +49-6102-3689-0

HONG KONG

Phone: +852-3104-1010

HUNGARY

Phone: +36 1 802 7360

INDIA

Phone: +91-44-4963-0900

INDONESIA

Phone: +62-21-2966-0120

ITALY

Phone: +39-02-6688220

KOREA

Phone: +82-31-789-4300

MALAYSIA

Phone: +60-3-7883-2211

MEXICO

Phone: +52-55-8850-0100

NETHERLANDS

Phone: +31 (0)40 206 6100

PHILIPPINES

Phone: +63-(0)2-8981-5000

POLAND

Phone: +48 71 368 61 60

ROMANIA

Phone: +40 (0)269 232 808

SINGAPORE

Phone: +65-6392-1011

SLOVAKIA

Phone: +421 (0)2 5939 6461

SLOVENIA

Phone: +386 (0)1 4701 666

SWITZERLAND

Phone: +41 (0)43 455 77 30

TAIWAN

Phone: +886-2-2721-1080

THAILAND

Phone: +66-2-078-1090

UK & IRELAND

Phone: +44 (0)1908-696-900

USA

Phone: +1-201-930-0100

VIETNAM

Phone: +84-24-3772-5555

