Operating Guide

iC7 Series OPC UA

OPC UA OS7UC

Explore our solutions
drives.danfoss.com

Contents

1 Introduction and Safety

1.1 Purpose of the Guide

This operating guide provides information about configuring the system, controlling the drive, accessing parameters, configuring, troubleshooting, and some typical application examples. The operating guide is intended for use by qualified personnel, who are familiar with the iC7 drives, OPC UA technology, and the PC or PLC that is used as a controller in the system.

Read the instructions before configuring OPC UA and follow the procedures in this guide.

The OPC UA client shown in the examples in this guide is UaExpert. Instructions for using the different simulation tools are not in the scope of this guide. Refer to the documentation of the client in use for the instructions.

1.2 Additional Resources

Additional resources are available to help understand the features, and safely install and operate the iC7 series products:

- Safety guides, which provide important safety information related to installing iC7 series drives and power converters.
- Installation guides, which cover the mechanical and electrical installation of drives, power converters, or functional extension options.
- Design guides, which provide technical information to understand the capabilities of the iC7 series drives or power converters for integration into motor control and monitoring systems.
- Operating guides, which include instructions for control options, and other components for the drive.
- Application guides, which provide instructions on setting up the drive or power converter for a specific end use. Application guides for application software packages also provide an overview of the parameters and value ranges for operating the drives or power converters, configuration examples with recommended parameter settings, and troubleshooting steps.
- *Facts Worth Knowing about AC Drives*, available for download on www.danfoss.com.
- Other supplemental publications, drawings, and guides are available at www.danfoss.com.

Latest versions of Danfoss product guides are available for download at https://www.danfoss.com/en/service-and-support/documentation/.

1.3 Safety Symbols

The following symbols are used in Danfoss documentation and products.

⚠ DANGER

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

⚠ WARNING

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

⚠ CAUTION

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

Indicates information considered important, but not hazard-related (for example, messages relating to property damage).

	ISO warning symbol for general warnings
	ISO warning symbol for hot surfaces and burn hazard
	ISO warning symbol for high voltage and electric shock
	Symbol for indicating the required discharge time of the capacitors in the product.
	ISO action symbol for referring to the instructions

1.4 Qualified Personnel

Correct and reliable transport, storage, installation, operation, and maintenance are required for the trouble-free and safe operation of the product. Only qualified personnel are allowed to install and operate this equipment.

Qualified personnel are defined as trained staff, who are authorized to install, commission, and maintain equipment, systems, and circuits in accordance with pertinent laws and regulations. Also, the qualified personnel must be familiar with the instructions and safety measures described in this guide.

1.5 Safety Precautions

⚠ DANGER

HIGH VOLTAGE

Drives and power converters contain high voltage when connected to AC mains input, DC supply, or load sharing. Failure to perform installation, startup, and maintenance by qualified personnel can result in death or serious injury.

- Only qualified personnel are allowed to perform installation, startup, and maintenance.

⚠ WARNING

UNINTENDED START

When the drive or power converter is connected to the AC mains or connected on the DC terminals, the motor may start at any time, causing risk of death, serious injury, and equipment or property damage.

- Stop the drive or power converter before configuring parameters.
- Make sure that the drive or power converter cannot be started by an external switch, a fieldbus command, an input reference signal from the control panel, or after a cleared fault condition.
- Disconnect the drive or power converter from the mains whenever safety considerations make it necessary to avoid an unintended motor start.
- Check that the drive or power converter and any driven equipment are in operational readiness.

⚠ WARNING

DISCHARGE TIME

The drive or power converter contains DC-link capacitors, which can remain charged even when the drive or power converter is not powered. High voltage can be present even when the warning indicator lights are off. Failure to wait the specified time after power has been removed before performing service or repair work can result in death or serious injury.

- Stop the motor.
- Disconnect all power sources, including permanent magnet type motors.
- Wait for capacitors to discharge fully. The discharge time is specified on the drive or power converter product label.
- Measure the voltage level to verify full discharge.

⚠ WARNING

LEAKAGE CURRENT HAZARD

Leakage currents exceed 3.5 mA. Failure to ground the drive or power converter properly can result in death or serious injury.

- Ensure that the minimum size of the ground conductor complies with the local safety regulations for high touch current equipment.

⚠ WARNING

EQUIPMENT HAZARD

Contact with rotating shafts and electrical equipment can result in death or serious injury.

- Ensure that only trained and qualified personnel perform installation, start-up, and maintenance.
- Ensure that electrical work conforms to national and local electrical regulations.
- Follow the procedures in this guide.

⚠ CAUTION

INTERNAL FAILURE HAZARD

An internal failure in the drive or power converter can result in serious injury when the drive or power converter is not properly closed.

- Ensure that all safety covers are in place and securely fastened before applying power.

1.6 Abbreviations

Table 1: Abbreviations

Term	Definition
AddressSpace	Collection of information that an OPC UA Server makes visible to its clients.
Attribute	Data element of a node which can be read and written by a client.
BrowseName	Attribute of a node: Nodes have a BrowseName attribute that is used as a non-localized human-readable name when browsing the AddressSpace to create paths out of BrowseNames.
Compute	The device using data from servers to aggregate information, for example a SCADA or cloud.
Endpoint	A physical address available on a network that allows clients to access 1 or more services provided by a server.

Table 1: Abbreviations - (continued)

Term	Definition
Discovery	Mechanism which allows OPC UA clients to find OPC UA servers on the network.
DiscoveryUrl	A URL for a network endpoint that provides the information required to connect to a server.
DisplayName	Attribute of a node: a human-readable name that is used to identify the node during browsing operations.
Information Model	Organizational framework that defines, characterizes, and relates information resources of a given system or set of systems.
Method	Callable software function that is a component of an object.
MyDrive® Insight	Commissioning tool
Namespace	A container for NodeIDs with commonalities. Typically used for companion specification content and other OPC specifications, for example, UA and/or DA.
Node	A fundamental component of an address space.
NodeId	A unique identifier assigned to every node (variables, methods, objects) in the address space. The NodeId is used by clients to access the node directly, for example, reading, writing and calling methods.
Object	Node that represents a physical or abstract element of a system.
ObjectType	Node that represents the type definition for an object.
OPC UA	OPC Unified Architecture (OPC UA) is a machine-to-machine communication protocol used for industrial automation and developed by the OPC Foundation.
Reference	Explicit relationship (a named pointer) from 1 node to another node.
SCADA	Supervisory Control And Data Acquisition, typically the machine-user interface.
Secure Channel	A logical connection between a single client and a single server.
Service	Client-callable operation in an OPC UA server.
Session	A long-term logical connection between a single client and a single server on OPC UA application level.
Variable	Node that contains a value.

1.7 Trademarks

OPC UA is a trademark of the OPC Foundation.

1.8 Version History

This guide is regularly reviewed and updated. All suggestions for improvement are welcome.

The original language of this guide is English.

Table 2: Version History

Version	Remarks
AQ513539982268, version 0201	User management information replaced with references to application guides with comprehensive information on user management.
AQ513539982268, version 0101	First release.

2 Product Overview

2.1 Overview

The iC7 drives and power converters support fieldbus protocols for horizontal communication to control devices and monitoring protocols for providing data vertically to SCADA and/or Cloud.

The OPC UA monitoring protocol can be ordered as an add-on to a fieldbus protocol when ordering a drive, or alternatively, it can be activated later by a proof-of-purchase token.

Table 3: OPC UA Model Codes

Model code	Description
+BBUC	OPC UA OS7UC

OPC UA is an Ethernet-based monitoring protocol and can be used together with fieldbus protocols based on standard Ethernet. Interface selection depends on the fieldbus protocol. Some fieldbus protocols change the Ethernet layer and as a result, OPC UA is only available for interface X0. For more information on the interface selection, see 3.3.1 Configuring OPC UA.

2.2 iC7 Series OPC UA OS7UC Features

2.2.1 OPC UA Server

iC7 series OPC UA OS7UC implements an OPC UA server providing the features listed in Table 4 and supports authentication methods listed in Table 5.

Table 4: Server Features

Category	Name	Description
Encoding	OPC UA Binary	Supports UA Binary Encoding. Values of these data types are encoded in compact binary formats, contiguously and without tagging, that is, the receiver is assumed to understand the structure it is decoding.
Transport	UA-TCP UA-SC UA Binary	This transport facet defines a combination of network protocol, security protocol, and message encoding that is optimized for low resource consumption and high performance. It combines the simple TCP-based network protocol UA-TCP 1.0 with the binary security protocol UA-SecureConversation 1.0 and the binary message encoding UA-Binary 1.0.
Security Policy	Basic256Sha256	This security facet defines a security policy used for configurations with high security needs. The security facet requires a PKI infrastructure.
	Aes256Sha256RsaPss	This security facet defines a security policy used for configurations with average security needs. The security facet requires a PKI infrastructure.
	Aes128Sha256RsaOeap	This security facet defines a security policy used for configurations with high security needs. The security facet requires a PKI infrastructure.
Message Security Mode	Sign	Provides authenticity and no confidentiality. Used when confidentiality is of no concern.
	Sign & Encrypt	Provides authenticity and confidentiality to the level provided by the selected security policy.

Table 5: Authentication Methods

Name	Description
Anonymous	A user that is not yet authenticated.
Username Password	Authentication of the users defined on the device using username and password.

For more information on user accounts and roles, see 3.2 User Management.

2.2.2 Supported Services

iC7 series OPC UA OS7UC supports services listed in Table 6.

Table 6: Supported Services

Category	Name	Description
Discovery	FindServers()	This service returns the servers known to a server or discovery server. The behavior of discovery servers is described in detail in OPC 10000-12.
	GetEndpoints()	This service returns the endpoints supported by a server and all of the configuration information required to establish a secure channel and a session.
Secure Channel	OpenSecureChannel()	This service is used to open or renew a secure channel that can be used to ensure confidentiality and integrity for message exchange during a session. This service requires the communication stack to apply the various security algorithms to the messages as they are sent and received. Specific implementations of this service for different communication stacks are described in OPC 10000-6.
	CloseSecureChannel()	This service is used to terminate a secure channel.
Session	CreateSession()	This service is used by an OPC UA client to create a session, and the server returns 2 values which uniquely identify the session.
	CloseSession()	This service is used to terminate a session.
	ActivateSession()	This service is used by the client to specify the identity of the user associated with the session.
View	Browse()	This service is used to discover the references of a specified node. The browse can be further limited by the use of a View. This Browse service also supports a primitive filtering capability.
	BrowseNext()	This service is used to request the next set of Browse or BrowseNext response information that is too large to be sent in a single response.
	TranslateBrowsePathsToNodeIds()	This service is used to request that the server translates 1 or more browse paths to NodeIds.
	RegisterNodes()	A server often has no direct access to the information that it manages. Variables or services might be in underlying systems where additional effort is required to establish a connection to these systems. The RegisterNodes service can be used by clients to register the nodes that they know they access repeatedly (for example, Write or Call). It allows servers to set up anything needed so that the access operations are more efficient.
	UnregisterNodes()	This service is used to unregister NodeIds that have been obtained via the RegisterNodes service.
Attribute	Read()	This service is used to read 1 or more attributes of 1 or more nodes.
	Write()	This service is used to write values to 1 or more attributes of 1 or more nodes.

Table 6: Supported Services - (continued)

Category	Name	Description
Method	Call()	This service is used to call (invoke) a list of methods.
MonitoredItems	CreateMonitoredItems()	This service is used to create and add 1 or more MonitoredItems to a subscription.
	DeleteMonitoredItems()	This service is used to remove 1 or more MonitoredItems of a subscription.
	ModifyMonitoredItems()	This service is used to modify MonitoredItems of a subscription. Changes to the MonitoredItem settings shall be applied immediately by the Server. They take effect when practical but not later than twice the new revisedSamplingInterval.
	SetMonitoringMode()	This service is used to set the monitoring mode for 1 or more MonitoredItems of a subscription.
	SetTriggering()	This service is used to create and delete triggering links for a triggering item.
Subscription	CreateSubscription()	This service is used to create a subscription. Subscriptions monitor a set of MonitoredItems for notifications and return them to the client in response to publish requests.
	ModifySubscription()	This service is used to modify a subscription.
	SetPublishingMode()	This service is used to enable sending of notifications on 1 or more subscriptions.
	Publish()	This service is used for 2 purposes: • To acknowledge the receipt of NotificationMessages for 1 or more subscriptions. • To request the server to return a NotificationMessage or a keep-alive message. Since publish requests are not directed to a specific subscription, they may be used by any subscription.
	Republish()	This service requests the subscription to republish a NotificationMessage from its retransmission queue. If the server does not have the requested message in its retransmission queue, it returns an error response.
	DeleteSubscriptions()	This service is invoked to delete 1 or more subscriptions that belong to the client's session.
	TransferSubscriptions()	This service is used to transfer a subscription and its MonitoredItems from 1 session to another. For example, a client may need to reopen a session and then transfer its subscriptions to that session. It may also be used by 1 client to take over a subscription from another client by transferring the subscription to its session.

2.2.3 Information Models

iC7 series OPC UA OS7UC supports namespaces listed in Table 7.

Table 7: Supported Information Models

Information model	Namespace	Specification
OPC UA	http://opcfoundation.org/UA/	–
Device integration	http://opcfoundation.org/UA/DI/	OPC 10000-100 Devices
Machinery	http://opcfoundation.org/UA/Machinery/	OPC 40001-1 Machinery Basic Building Blocks

2.3 OPC Standard

2.3.1 OPC Technologies

OPC ranges different technologies:

- OPC Classic
- OPC Unified Architecture
- OPC UA Field eXchange

The iC7 series OPC UA OS7UC supports the OPC UA protocol used to communicate from Device to Compute.

OPC UA is intended to be used for the following use cases:

- Controller-to-Controller
- Controller-to-Compute
- Device-to-Compute

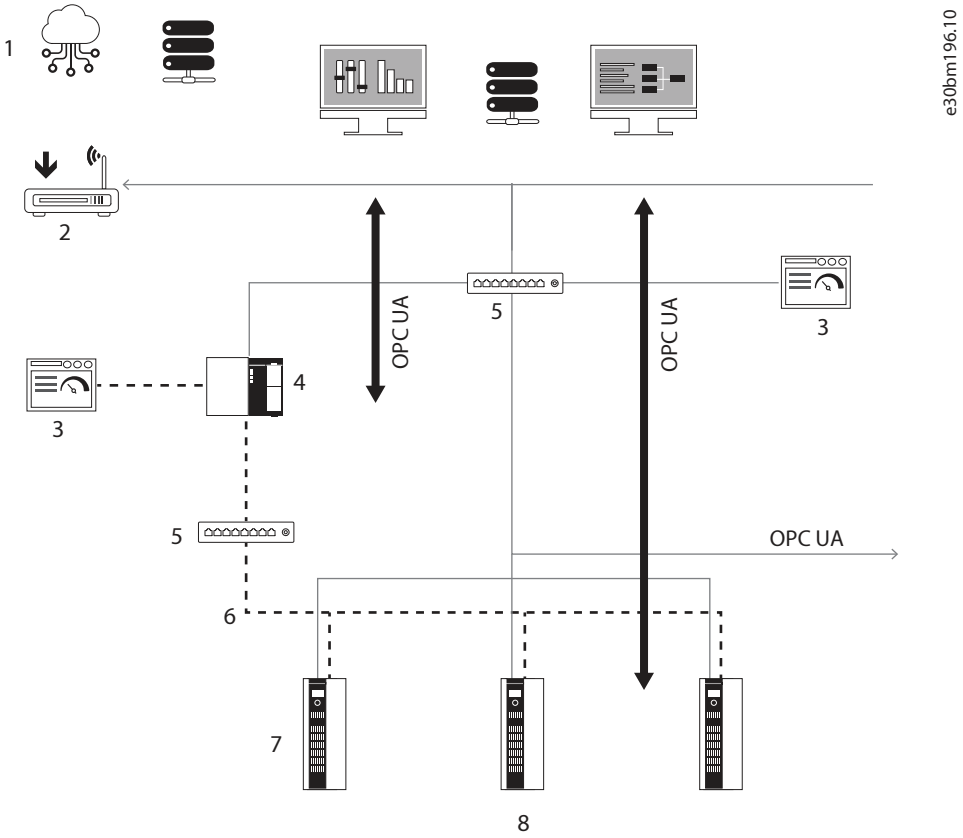


Figure 1: OPC UA Architecture in Applications with iC7 Drives

1	Cloud	2	OEM edge
3	HMI	4	PC
5	Switch	6	Configuring fieldbus
7	Sensors, I/Os, and other devices	8	iC7 drives

2.3.2 OPC UA Communication Model

Conformance units, also known as facets, in OPC UA server implementations define the specific features and functionalities supported by the server. The conformance units are defined by the OPC Foundation. For more information, see https://opcfoundation.org/.

OPC UA profiles, such as the Micro Embedded Device 2022 Server Profile, define a selection of conformance units for certain devices. See Figure 2 and Figure 3.

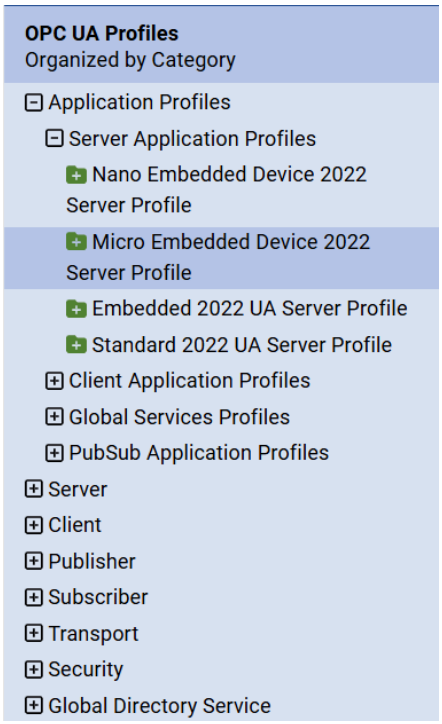


Figure 2: Example of OPC UA Profiles

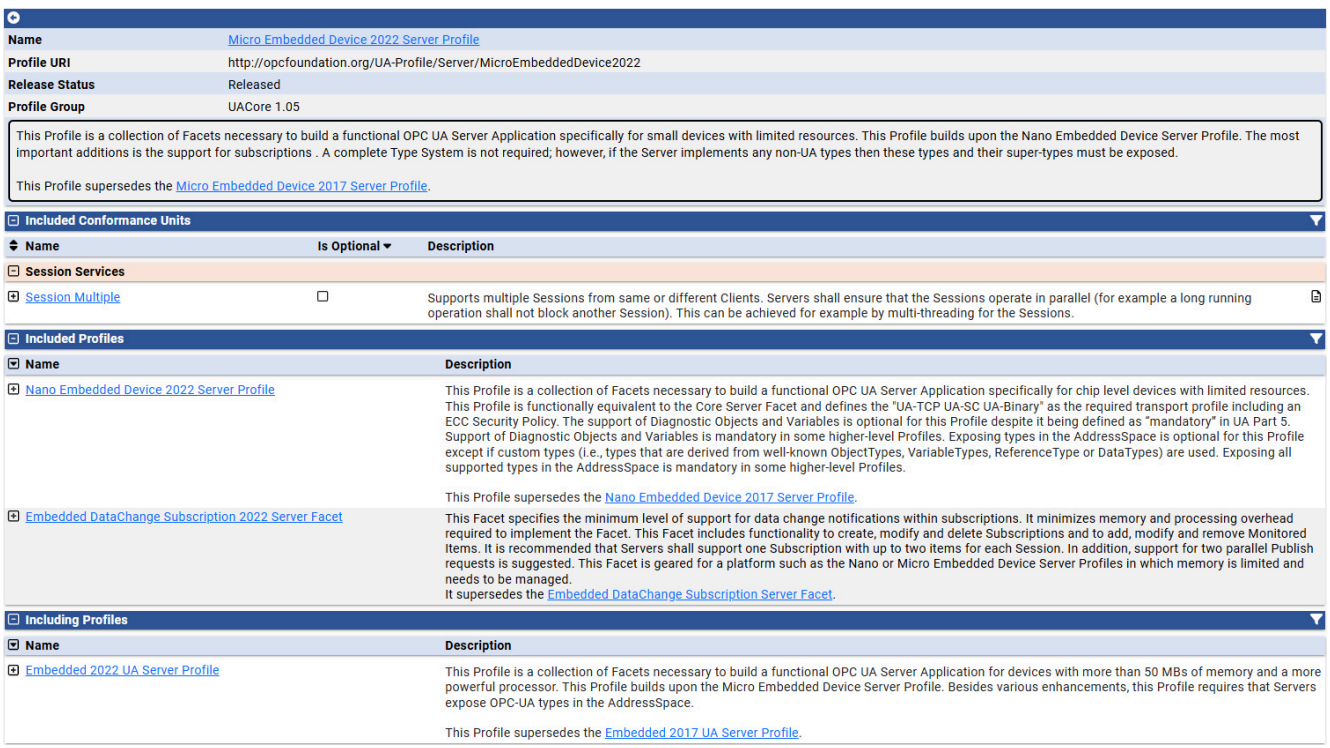


Figure 3: Example of Conformance Units in an OPC UA Profile

2.3.3 OPC UA Information Models

Each server supports data through information models. Information models are defined at different levels. Figure 4 shows how the different types of information models are combined into products.

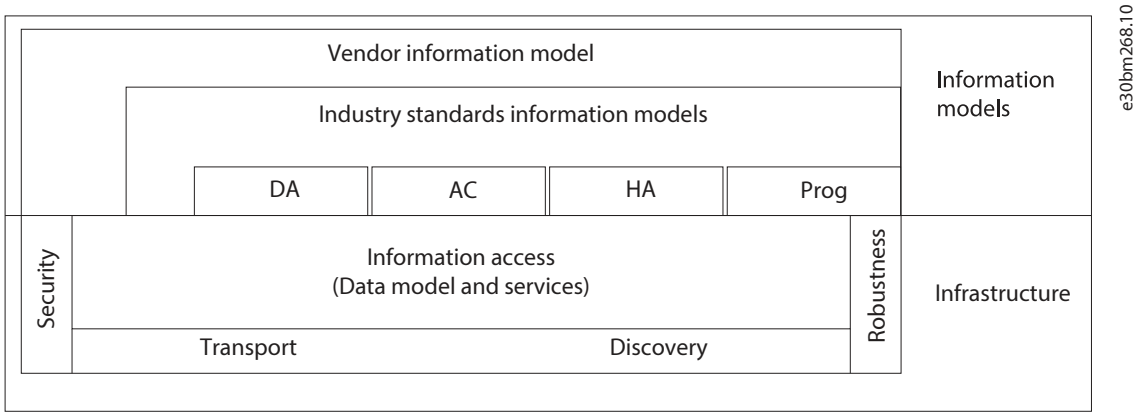


Figure 4: OPC UA Information Modeling

- Core information models define standard features of OPC UA, for example, device information (DI).
- Companion information models are typically defined by industries to standardize the data provided for machines.
- Vendor Specific Extensions define vendor-specific behavior that is not covered by core information models or companion information models.

3 Configuration

3.1 Prerequisites

Make sure that the following requirements are met:

- The system clock is set to a valid time. For more information, refer to the application guide of the application software installed on the drive.
- UaGDS Configuration Tool version 1.1.0 or newer is installed.
- The user account has the SecurityAdmin role. For details on user management, see section *User Management* in Industry Application for iC7-Automation or Motion Application for iC7-Automation.

3.2 User Management

iC7 drives support user management with role-based access control. Users can be assigned 1 or more roles that determine their permissions and the actions they can perform on the drive. User management is done in MyDrive® Insight.

For details on user management, see section *User Management* in Industry Application for iC7-Automation or Motion Application for iC7-Automation. For information on the cybersecurity features of iC7 drives, see Cybersecurity for iC7-Automation Frequency Converters and Cybersecurity for iC7 System Products.

3.3 Configuring the OPC UA Connection

3.3.1 Configuring OPC UA

OPC UA parameters are in parameter group ***10 Connectivity*** > ***Protocols*** > ***OPC UA***.

1. In MyDrive® Insight or the control panel, navigate to ***10 Connectivity*** > ***Protocols*** > ***OPC UA*** > ***Configuration***.
2. In parameter ***10.3.6.2.1 Interface Selection***, select the interface for OPC UA.

Table 8: Parameter for OPC UA Interface Selection

Parameter index number	Parameter name	Parameter number	Selections	Description
10.3.6.2.1	***Interface Selection***	7086	• ***None*** • ***X0*** (default) • ***X1/X2***	Select the interface for OPC UA. The selection list depends on the available interfaces capable of running OPC UA. Use ***None*** to disable OPC UA.

3. In parameter ***10.3.6.2.2 Reverse Connect URL***, set the OPC UA reverse connection URL.

The parameter is used to define the client receiving reverse connections.

Table 9: Parameter for Reverse Connect URL

Parameter index number	Parameter name	Parameter number	Description
10.3.6.2.2	***Reverse Connect URL***	7085	Set OPC UA reverse connection URL. Clear to remove the reverse connection.

A valid URL contains the OPC scheme, a port number, and a path: [opc_scheme://]fqdn[:port_no][path]

Square brackets indicate optional segments in the URL.

Table 10: Reverse Connect URL Elements

Element	Description
opc_scheme	opc_scheme allows opc.tcp.
port_no	port_no allows values 1–65535.
path	path is any valid path starting with and constructed using slashes (/). Backslash (\) is not supported.

Examples of valid URLs:

- opc.tcp://somehost.example.com:1234/path/to
- opc.tcp://somehost:1234/path/to
- opc.tcp://somehost:1234
- opc.tcp://somehost
- somehost:1234/path/to
- somehost.example.com:1234
- somehost

3.3.2 Establishing an OPC UA Connection

Prerequisites:

For information on the location of the Ethernet connectors, refer to the product-specific design or installation guide. To use OPC UA, the drive must be ordered with OPC UA OS7UC (+BBUC).

OPC UA can be used on the selected Ethernet connectors. Depending on the Ethernet port usage of the drive, OPC UA use may be restricted to port X0. Establish the connection using a routable IP address (DHCP or static).

The OPC UA client shown in the examples in this guide is UaExpert. For more information on using UaExpert, see https://www.unified-automation.com/. Any other OPC UA client can also be used to operate OPC UA OS7UC.

1. In MyDrive® Insight, select the connection.

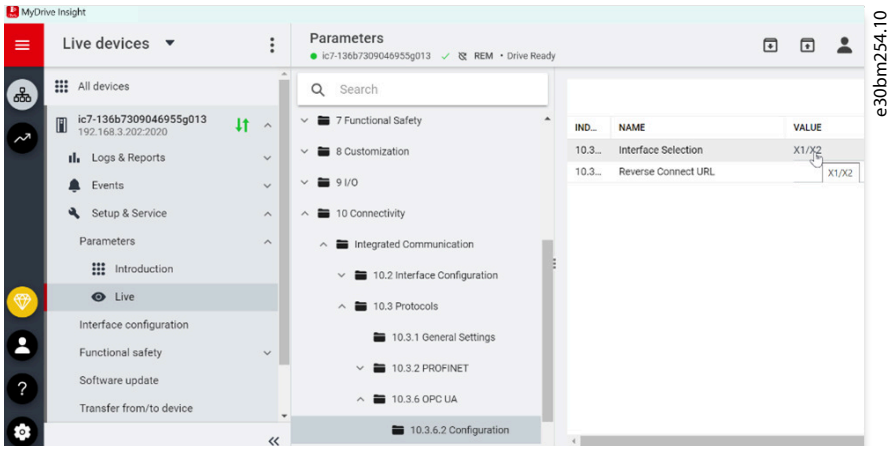
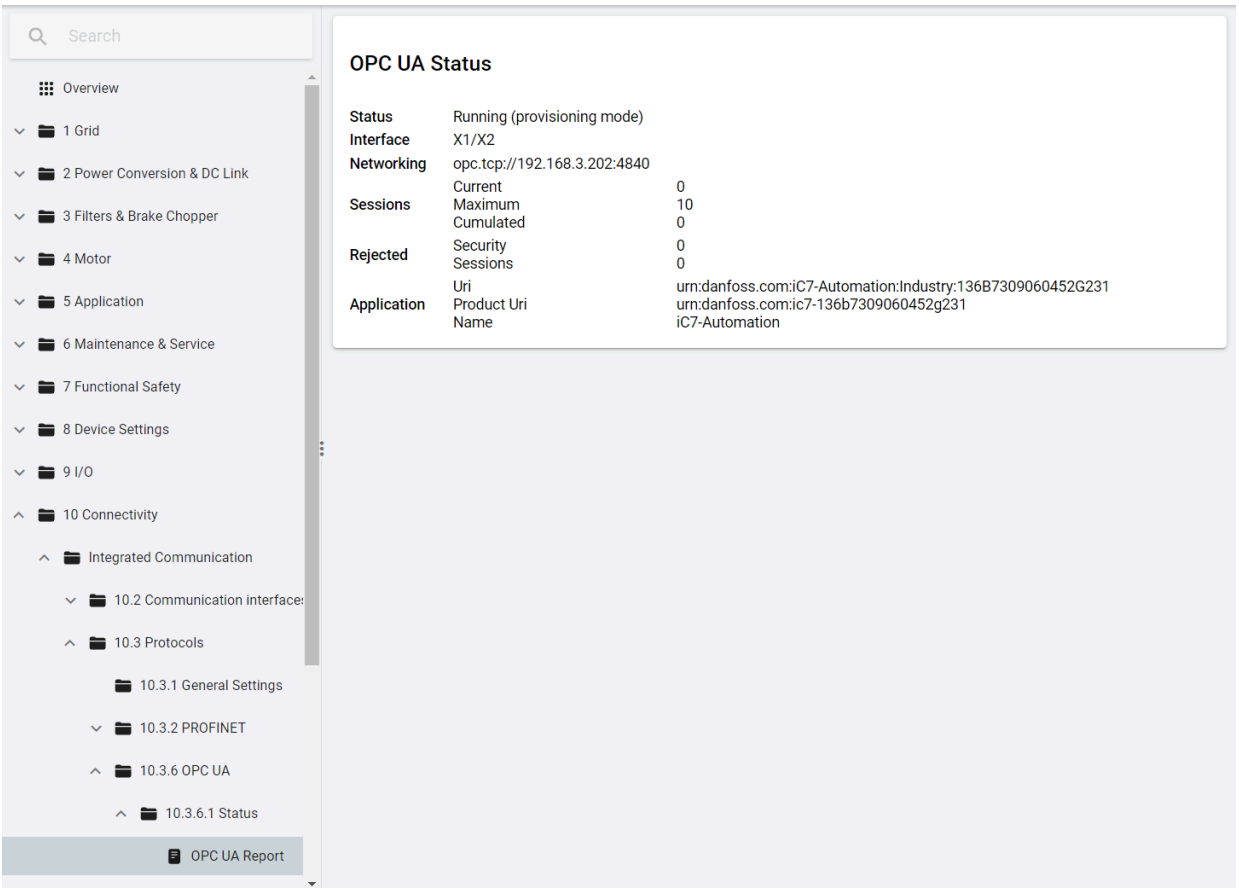


Figure 5: Selecting the Interface for OPC UA in MyDrive® Insight

2. Ensure that the server OPC UA status is showing as ***Running*** (provisioning mode).

See Figure 7 for information on OPC UA status transitions.



e30bm628.10

Figure 6: OPC UA Status: Running

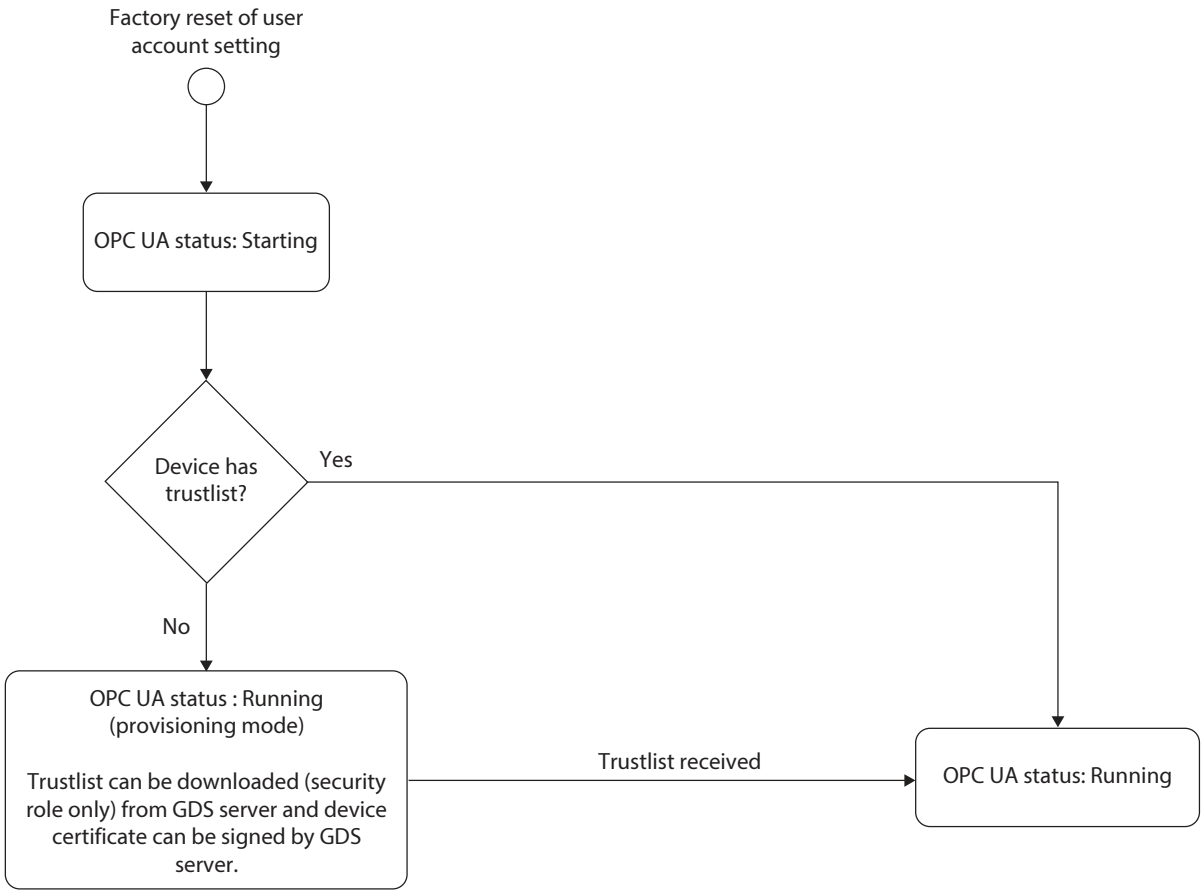


Figure 7: OPC UA Status Transitions

3. In UaExpert, select *Add Server*.

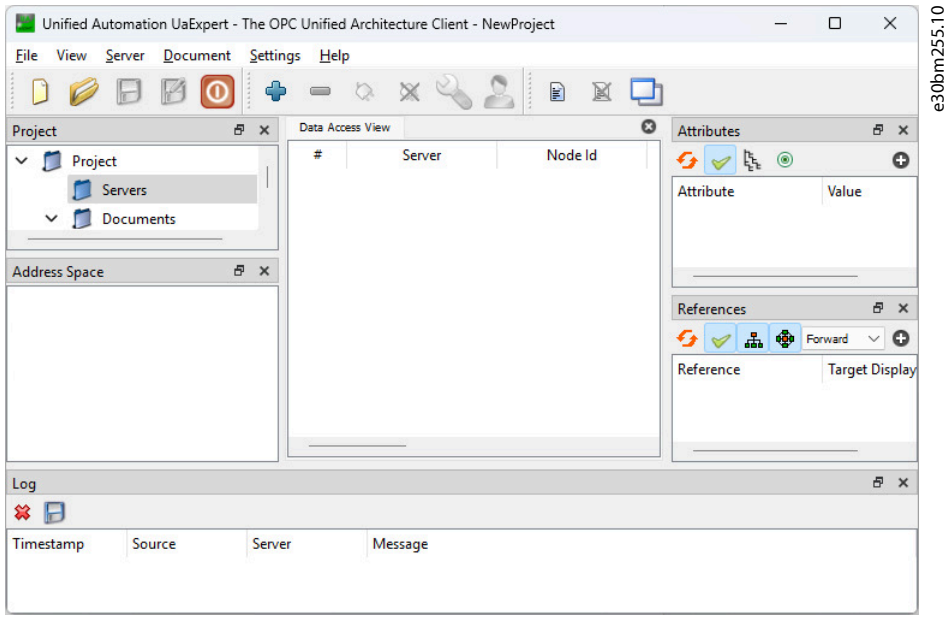


Figure 8: Adding a Server in UaExpert

4. Select *Custom Discovery*.

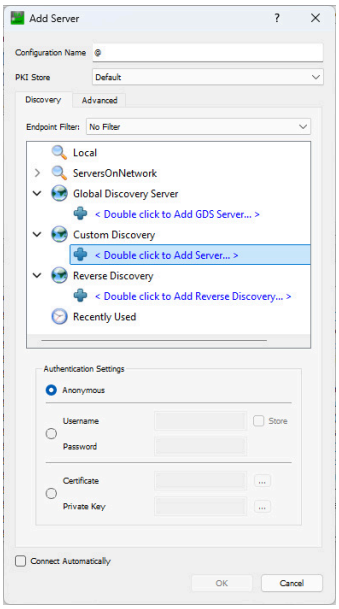


Figure 9: Using Custom Discovery in UaExpert

5. Enter the protocol, the IP address, and the port of the device (4840) and click *OK*.

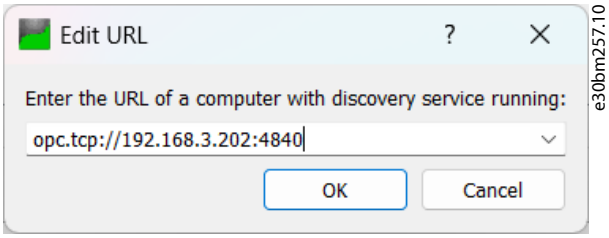


Figure 10: Entering Connection Information in UaExpert

The server is added in UaExpert.

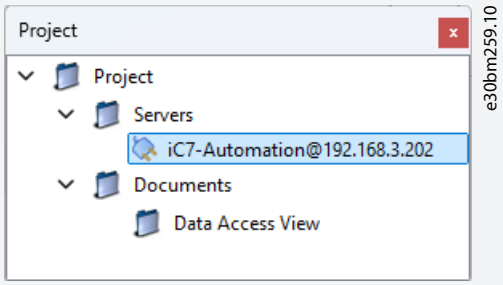
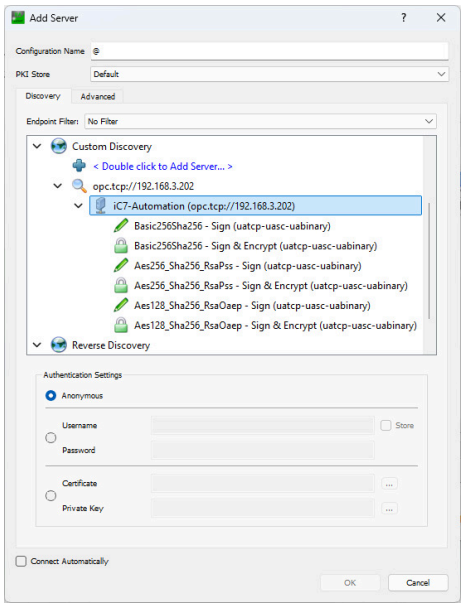


Figure 11: New Server in UaExpert

6. Expand the server and select the security profile to use.



e30bm258.10

Figure 12: Selecting the Security Profile in UaExpert

3.3.3 Establishing Secure Connection using GDS Push

Prerequisites:

- Make sure that the system clock is set to a valid time. For more information, refer to the application guide of the application software installed on the drive.
- Install UaGDS Configuration Tool version 1.1.0 or newer.
- Make sure that the server OPC UA status is showing as Running (provisioning mode) in MyDrive® Insight as shown in Figure 13.

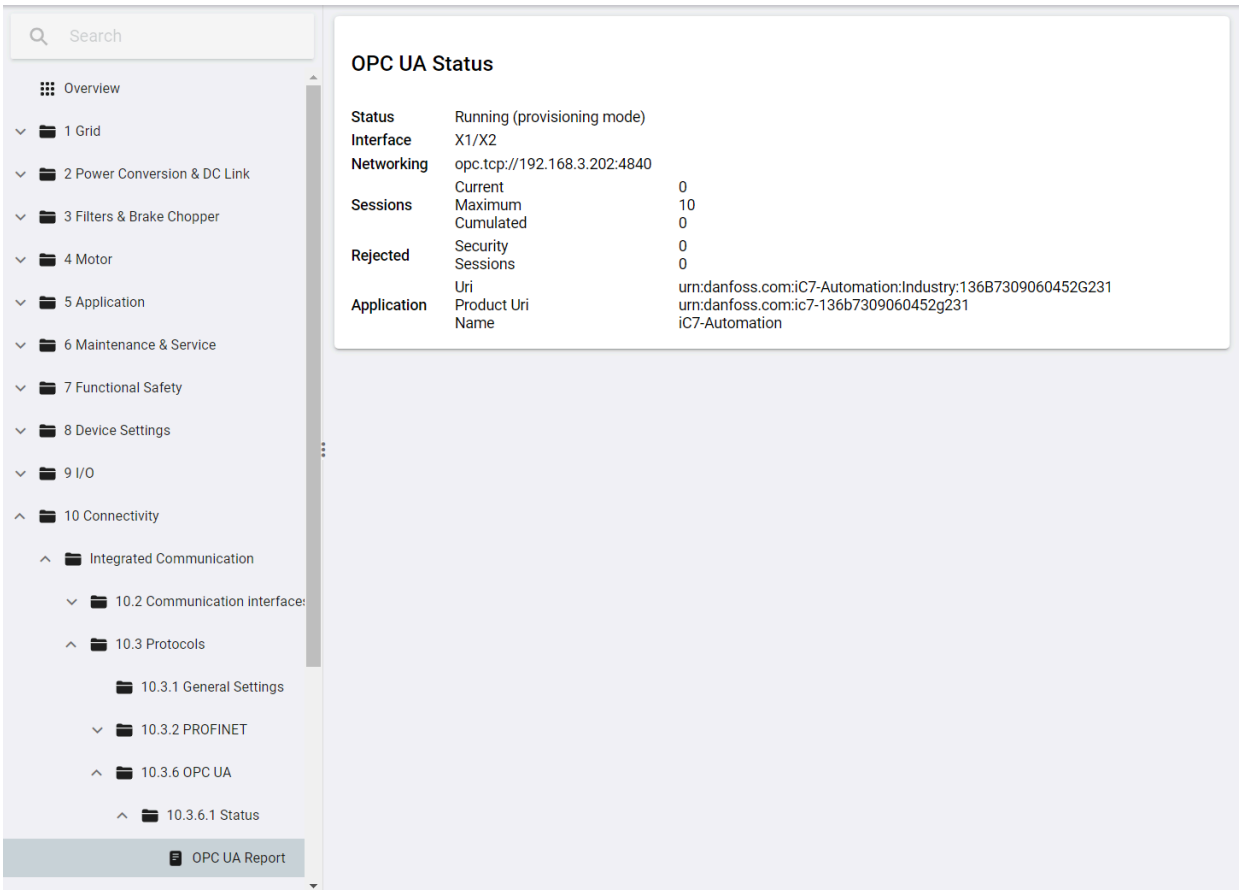
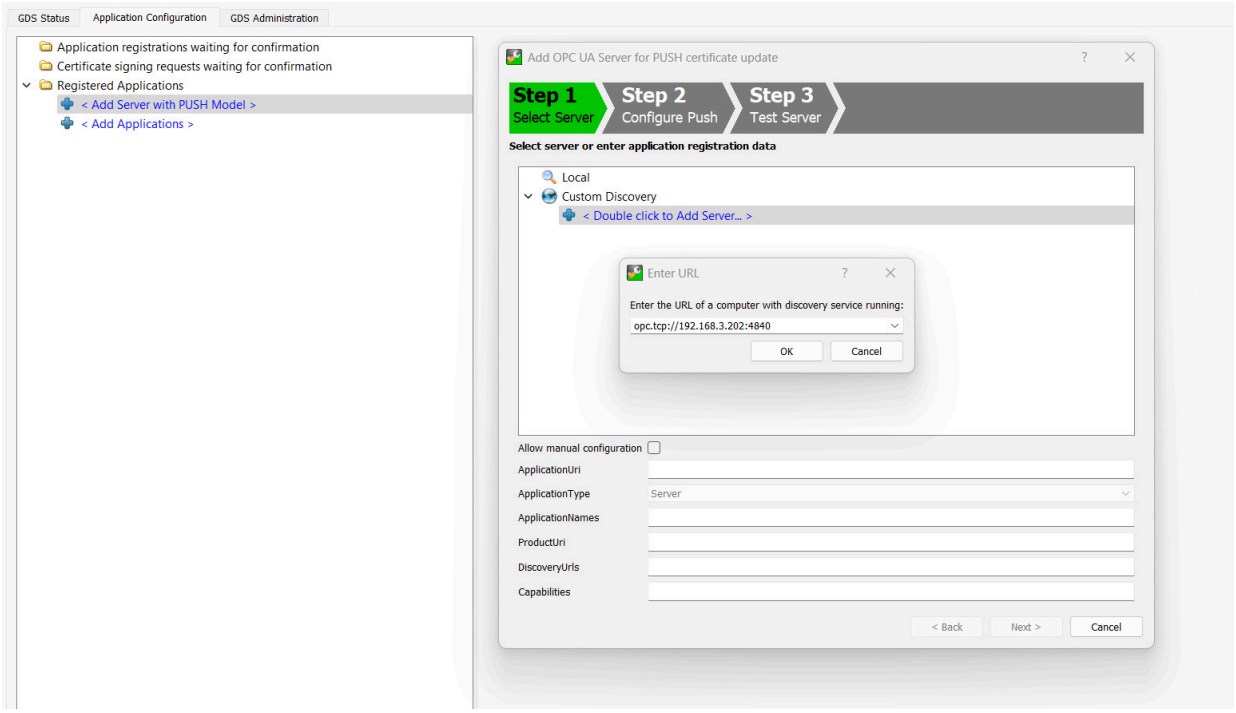


Figure 13: Checking OPC UA Status

- Make sure that the user account has the SecurityAdmin role.

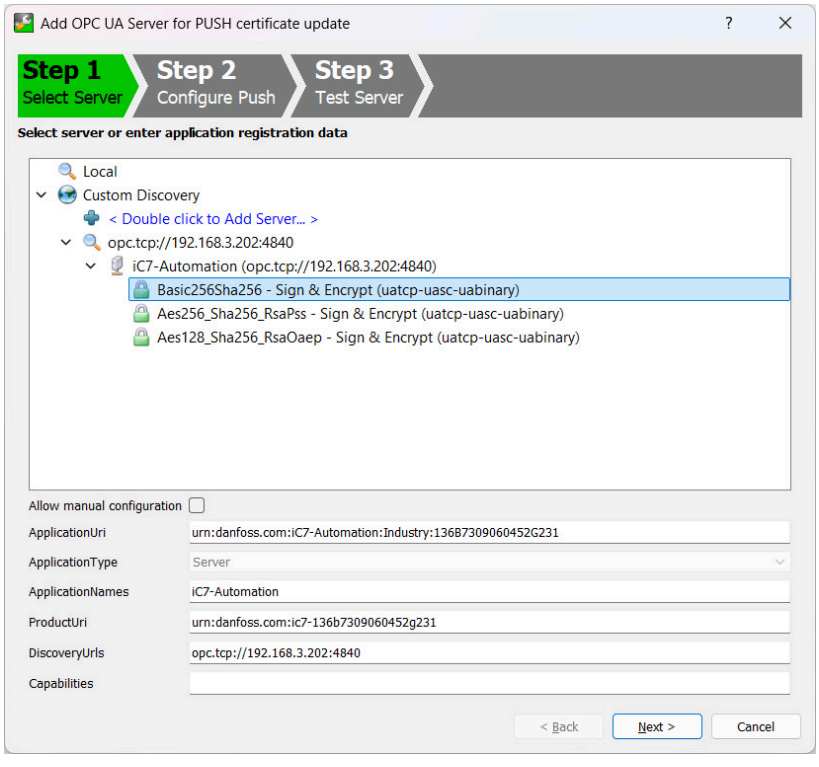
  1. Open UaGDS Configuration Tool and register the server by providing the IP address and port number. The IP address should match the OPC UA interface selected in MyDrive® Insight.



e30bm630.10

Figure 14: Registering the Server

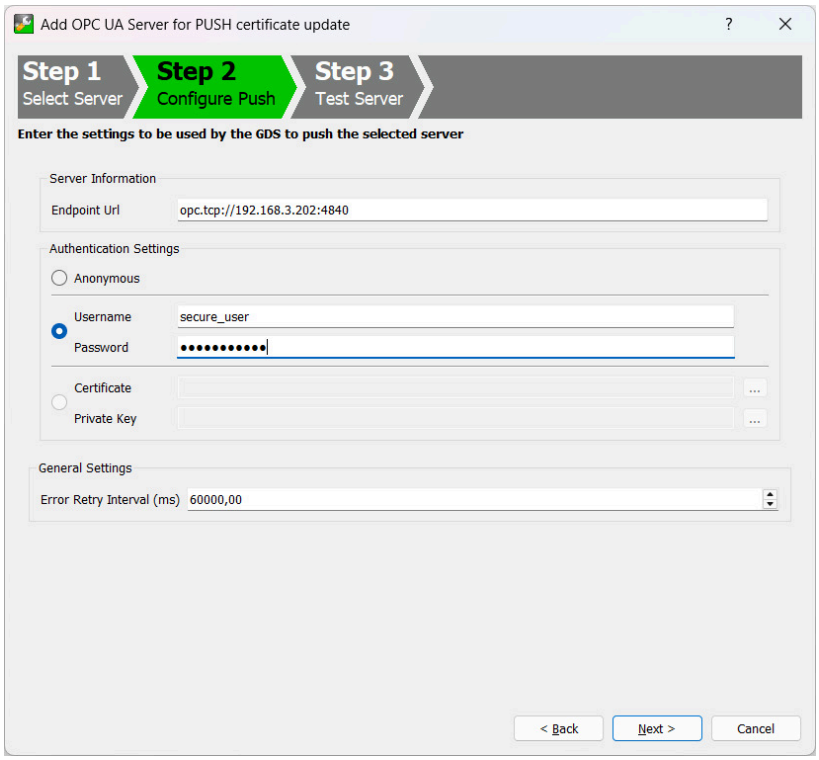
2. Select 1 of the available secure connections and click *Next*.



e30bm631.10

Figure 15: Selecting a Connection

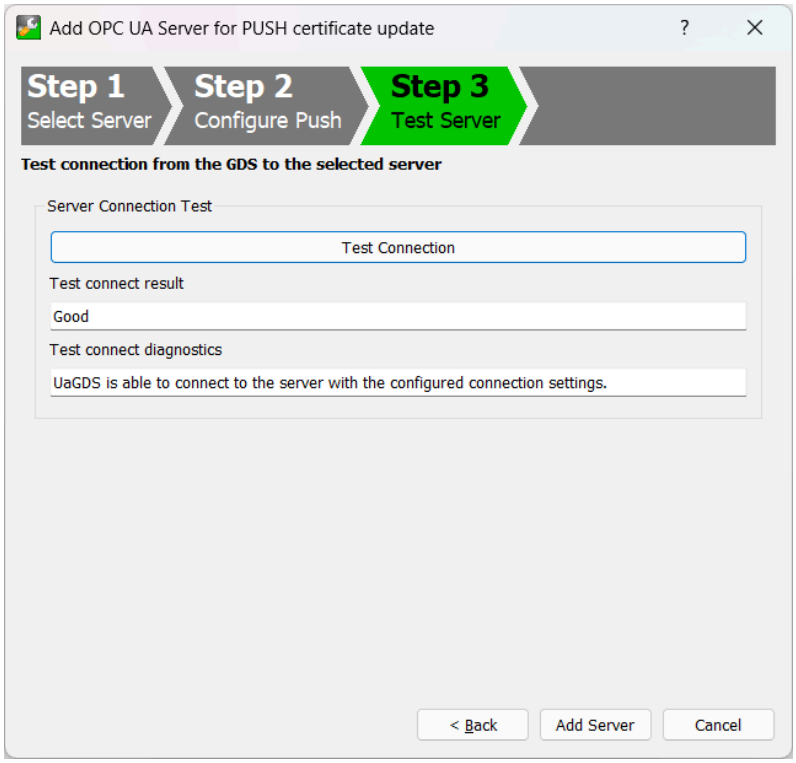
3. Enter the username of a user with the SecurityAdmin role and the password of the server, and click *Next*.



e30bm632.10

Figure 16: Entering User Information

4. Click *Test Connection*, check that the *Test connect result* is *Good*, and click *Add Server*.



e30bm633.10

Figure 17: Testing the Connection

Ensure that the status for the register with UaGDS Configuration Tool is *Succeeded*.

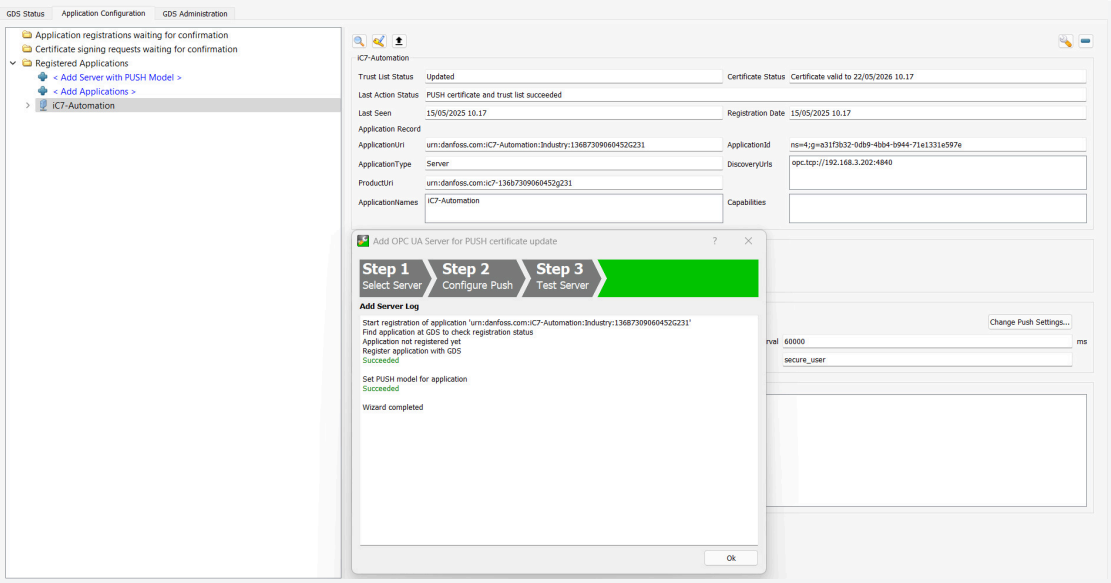


Figure 18: Successful Connection to UaGDS

5. Using UaExpert as the client, connect to the server with a trusted device using Global Discovery Server.

The client must be part of the same PKI handled by the UaGDS Configuration Tool. Connecting to the server can be done as an authenticated user. No specific role is required.

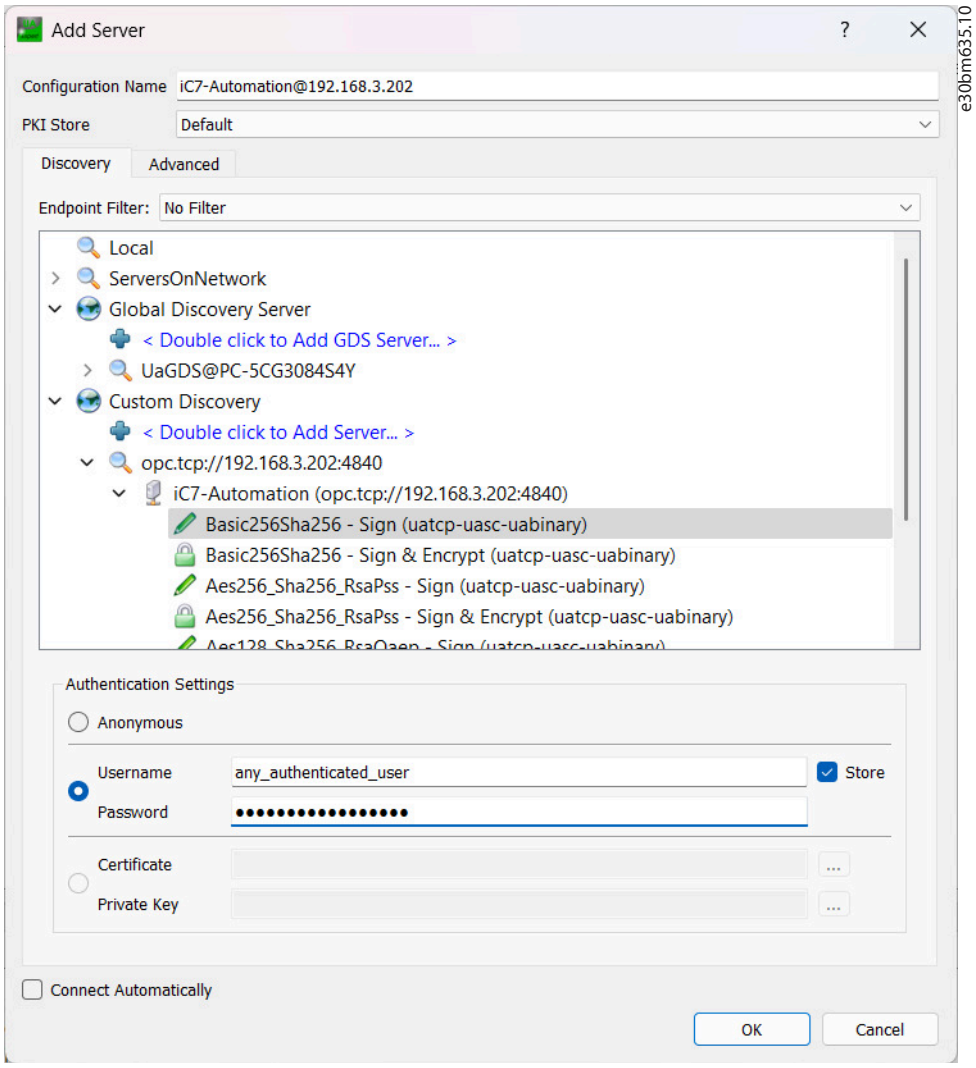


Figure 19: Connecting to the Server

3.4 Asset Management

iC7 Series OPC UA OS7UC implements asset management according to the following specifications:

- OPC 10000-100 Devices
- OPC 40001-1 Machinery Basic Building Blocks

For details, refer to the OPC Foundation website at https://opcfoundation.org. The Machinery Basic Building Blocks specification defines a IMachineTagNameplateType which is based on the ITagNameplateType defined in OPC 10000-100.

The structure implements the following nodes:

- Hardware Revision
- Location
- Manufacturer
- ManufacturerUrl
- Model
- ProductCode
- ProductInstanceUri
- SerialNumber

- SoftwareRevision

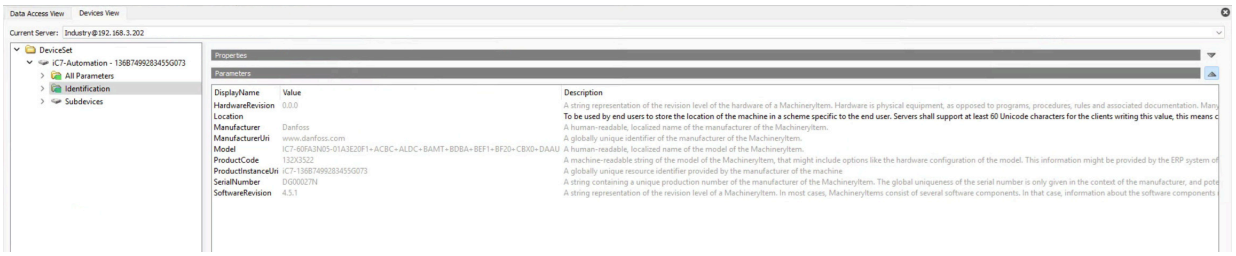


Figure 20: Example of Asset Information in UaExpert

The location node can be set when logged in. All other nodes are read-only.

3.5 Device Modeling

The iC7 drive is built as a modular, configurable drive, which can be complemented with 1 or more functional extension options. The number of functional extension option slots depends on the drive type and frame. For details on available option slots, refer to the product-specific guides.

In OPC UA, the main device is represented under the DeviceSet as shown in Figure 21.

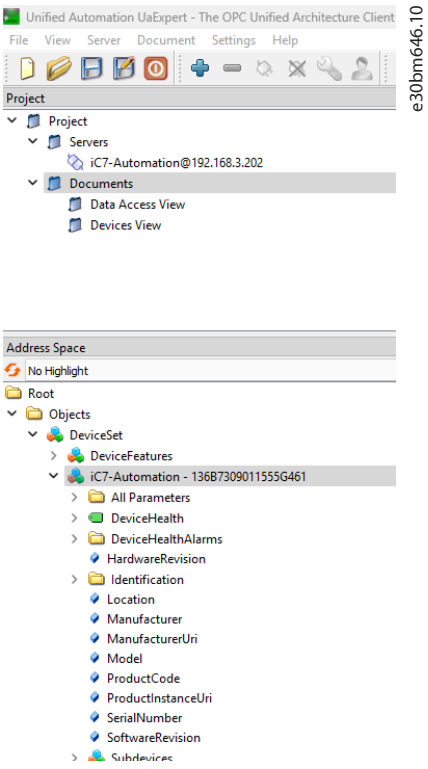


Figure 21: Example of DeviceSet

The DeviceSet contains all the information regarding the main components, such as the control unit and power unit, of the device.

When functional extension options, for example, the Basic I/O or General Purpose I/O option, are added to the device, they are listed under *Subdevices* as shown in Figure 22.

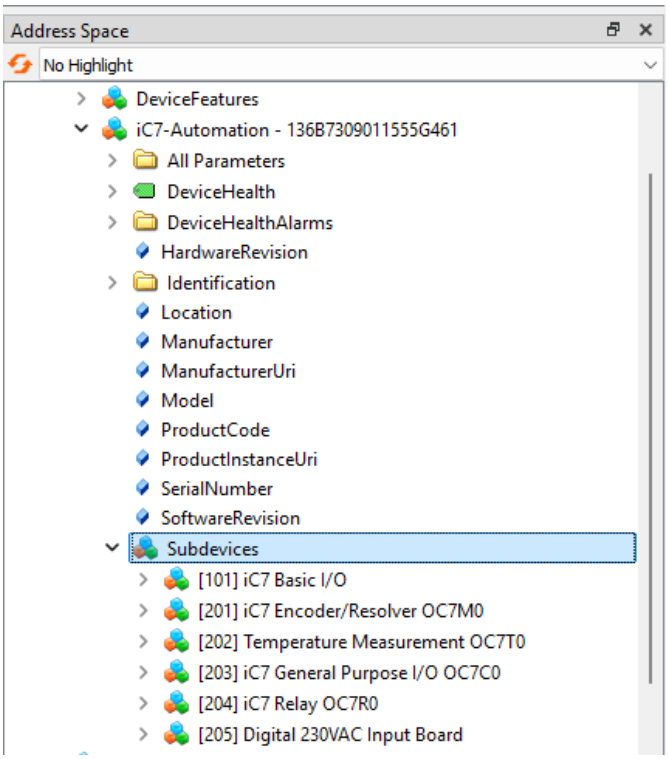


Figure 22: Subdevices View

Each functional extension in the device is listed under the *Subdevices* (see Figure 23). The number in the square brackets indicates the option slot number. Figure 23 shows an iC7-Automation drive with 6 functional extension options installed.

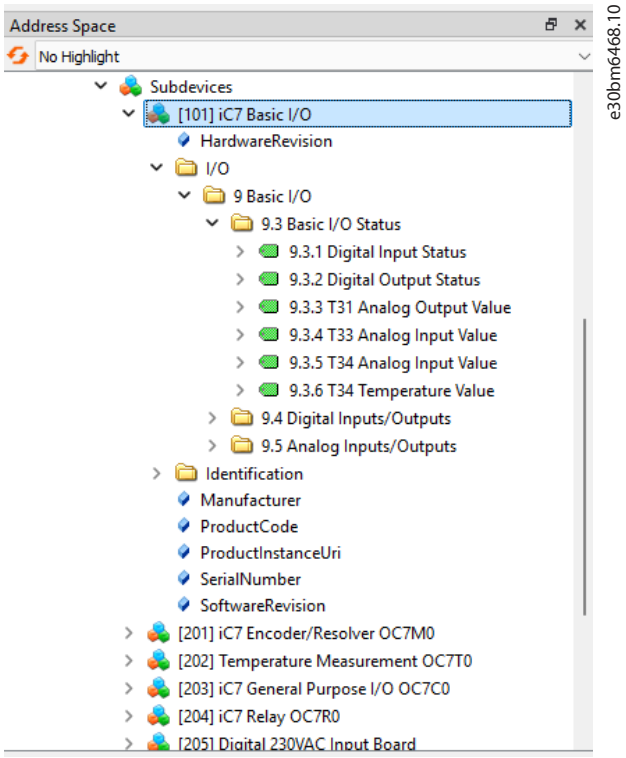


Figure 23: Example of Functional Extension Options in Subdevices

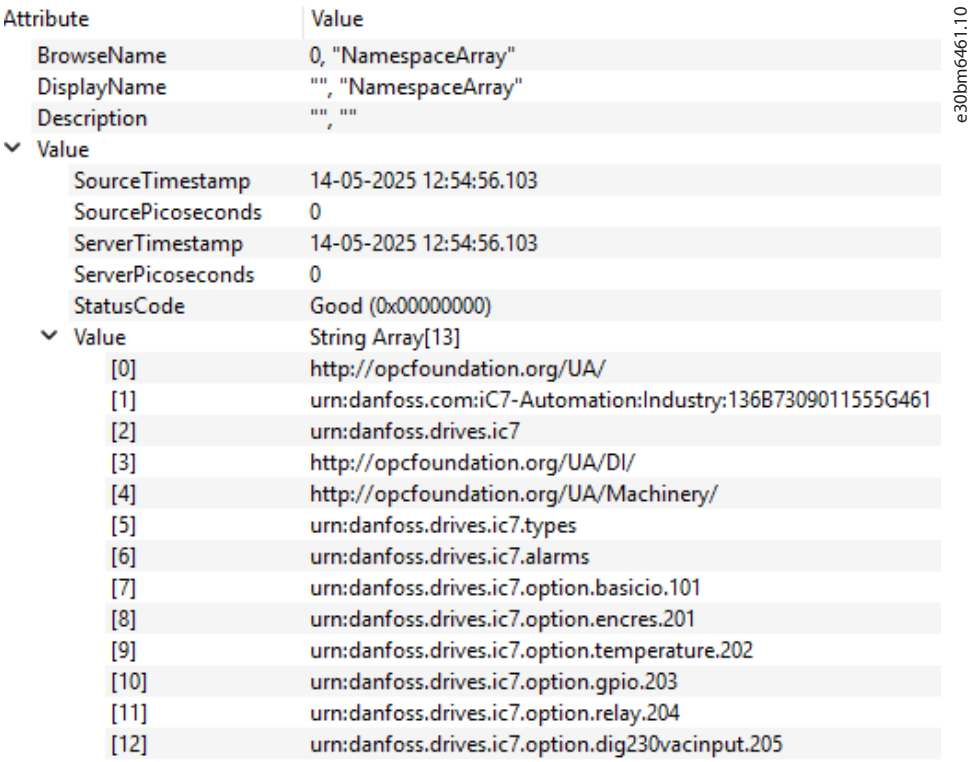
Information regarding the option can be found under the option itself. The information available for an option is structured in the same way as in the control panel or MyDrive® Insight.

3.6 Namespace

The namespace is a URI that identifies the naming authority responsible for assigning the identifier element of the NodeId. Naming authorities include the local Server, the underlying system, standards bodies, and consortia.

The iC7 drives consist of many namespaces. Some are based on standards from the OPC UA foundation, and some are vendor-specific for the specific device. See Figure 24 for an example of the NamespaceArray in iC7-Automation.

Figure 24: Namespace Array in iC7-Automation



The following namespace indexes refer to standards coming from the OPC UA foundation:

- Index 0: http://opcfoundation.org/UA/
- Index 3: http://opcfoundation.org/DI/
- Index4: http://opcfoundation.org/UA/Machinery/

The following namespace indexes refer to vendor-pecific implementation:

- Index 1: urn:danfoss.com:iC7-Automation:Industry:136B7309011555G461
- Index 2: urn:danfoss.drives.ic7
- Index 5: urn:danfoss.drives.ic7.types:
- Index 6: urn:danfoss.drives.ic7.alarms
- Index 7: urn:danfoss.drives.ic7.option.basicio.101

The indexes depend on the actual configuration of the device, for example, which slots functional extension options are mounted in.

3.7 Accessing Parameters

Prerequisites:

- When accessing parameters using OPC UA, it is recommended to allow access only for authorized users. For details on user management, see section *User Management* in Industry Application for iC7-Automation or Motion Application for iC7-Automation.
- It is recommended that access is removed for anonymous users when using OPC UA.

- Ensure that a user with adequate user access exists in the system.

Logging in as a user with the ***ConfigureAdmin*** role is required to modify parameter settings.

Parameters are shown in UaExpert in a similar tree-view as in MyDrive® Insight. Nodes in the *All Parameters* view in UaExpert use the parameter number as node ID. To access a node via the OPC UA parameter view, use the parameter number that is shown in the MyDrive Insight parameter view.

The instructions in this section describe logging in as a specific user.

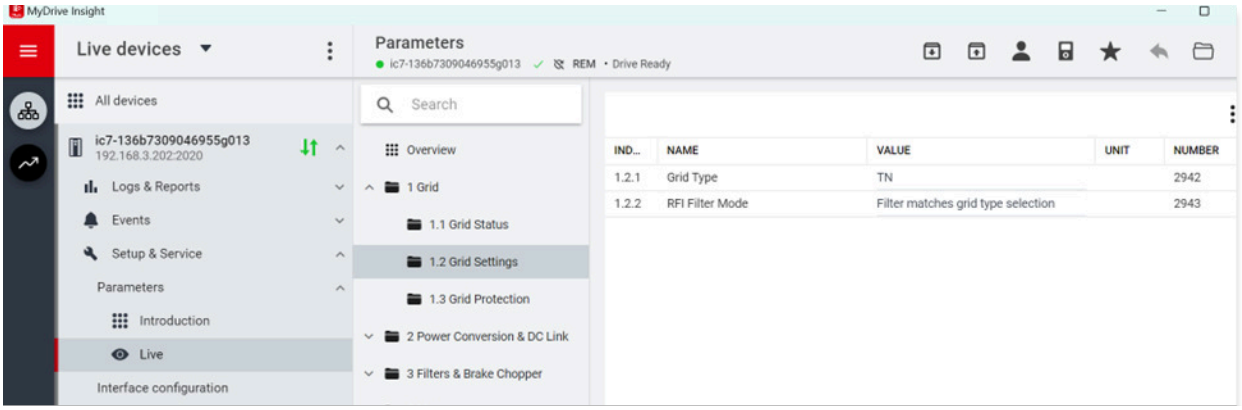


Figure 25: Parameter View in MyDrive Insight

1. In UaExpert, select *Change User*.

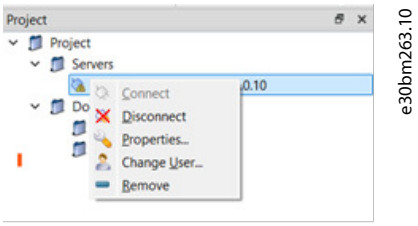


Figure 26: Logging into UaExpert

2. Use the authentication setting configured in MyDrive Insight and enter the password.

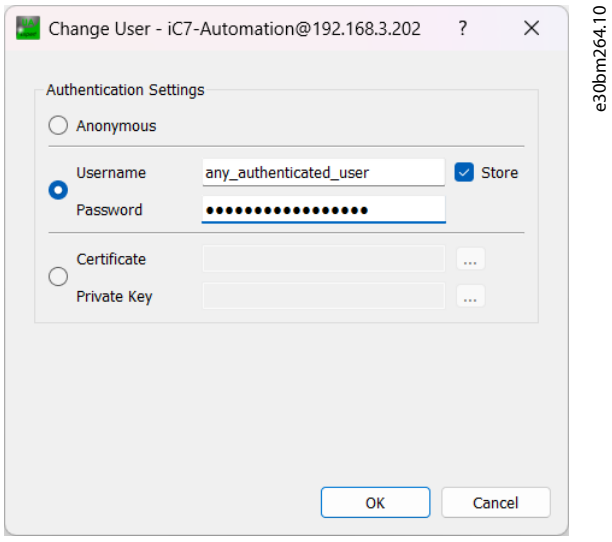
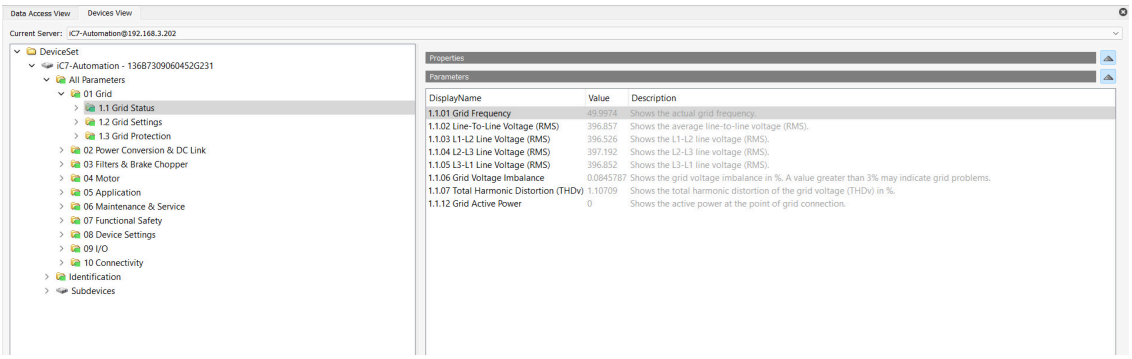


Figure 27: Changing the User in UaExpert

3. To locate a parameter in UaExpert, navigate to the parameter in the tree-view under *All Parameters*.



e30bm266.10

Figure 28: Parameter View in UaExpert

4. To view parameter information, click the parameter name.

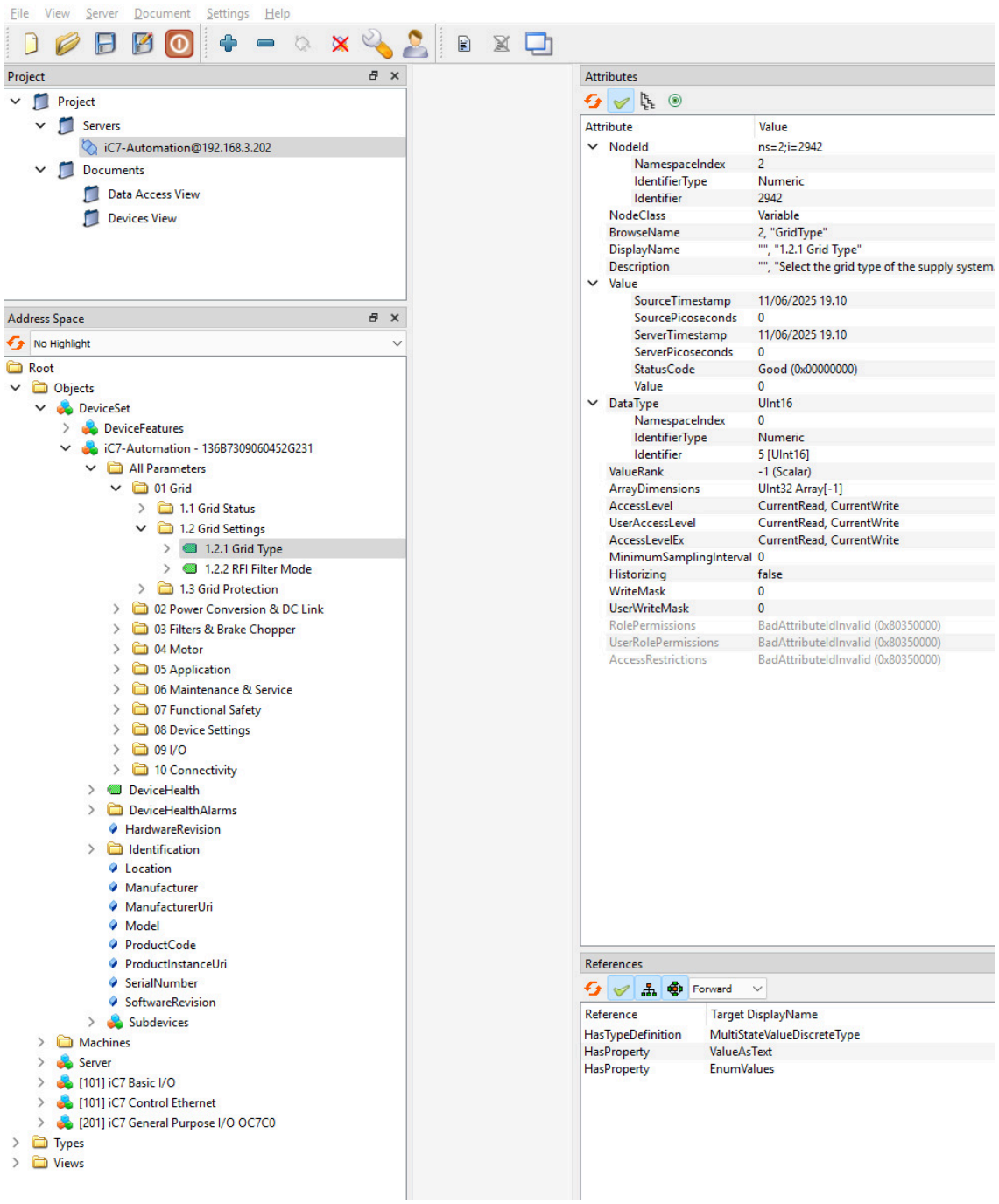


Figure 29: Using the Parameter View in UaExpert

3.8 Browse using NodeId, BrowseName, or DisplayName

In OPC UA, there are multiple ways to address a node, known as browsing. Browsing is supported through the following mechanisms:

- Browse by NodeId: The NodeId is identical to the Parameter Number given to the Parameters of the device. Parameter numbers do not change, but their location in the menus may vary based on software version. It is recommended to use the NodeId for permanent clients reading specific device data.
- Browse by BrowseName: BrowseName is a constructed name of the parameter when it was added to OPC UA and remains the same even if DisplayName is updated. The name is constructed so that it conforms to the limitations given by OPC UA BrowseName, for example, no spaces or special characters are allowed. If clients need to show the menu structure as given by the device, and reading or writing data is required, it is recommended to browse using BrowseName and show using DisplayName

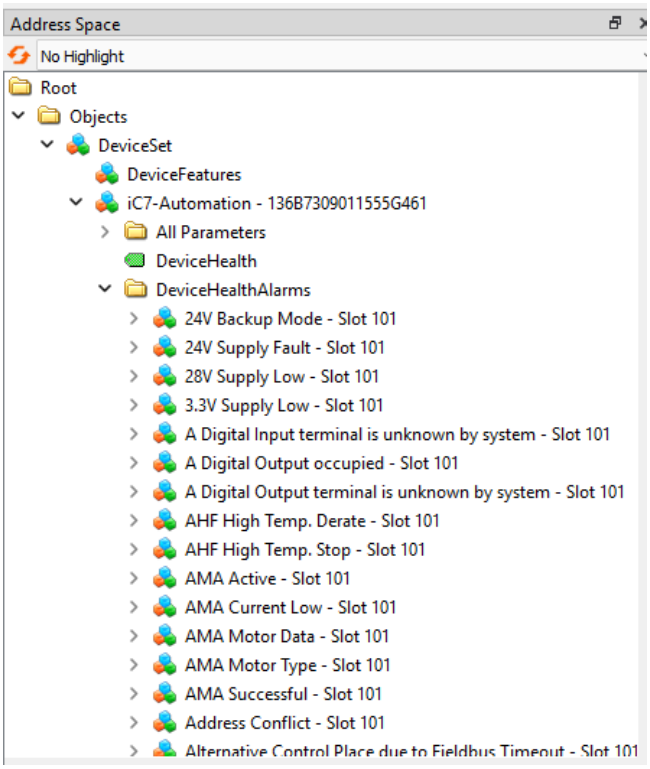
- Browse by DisplayName: The DisplayName is linked to the menu index and the current name of the index. The naming of menus can change.

Each mechanism has distinct advantages. When developing a client to access device data, consider compatibility with future product versions.

> **IMPORTANT: Avoid hardcoding namespace IDs.**
>
> Namespaces IDs are semi-dynamic within the device due to the support of 0 to many options of the same or different type. When options are added or removed, the namespace IDs change. It is recommended to always look up the namespace IDs. The product provides unique names for each namespace. It is recommended to list the Namespaces currently available and to look up the Namespace ID to be used based on the name.

3.9 Alarms and Conditions

The status of the devices can be monitored using the alarms and conditions feature in OPC UA. The general health status of a device can be read using the DeviceHealth interface. All alarms defined by the device, including options, are located in the folder DeviceHealthAlarms. It is also possible to subscribe to events.



e30bm644.10

Figure 30: Example of DeviceHealthAlarms

Table 11: Device Health Statuses

Name	Value	Description
NORMAL	0	No fault or warning occurrences active
FAILURE	1	Fault active
CHECK_FUNCTION	2	Not implemented
OFF_SPEC	3	Not implemented
MAINTENANCE_REQUIRED	4	Warning active (and no faults)

Alarms have a severity and attributes. The higher the number, the more severe the alarm is. The attribute ActiveState can be used to monitor if the alarm is active or not.

Table 12: Alarm Severity

Level	Type	Severity	Urgency
Info	Any	50	LOW
Warning	Any	450	MEDIUM
Warning	Requires a reset	500	MEDIUM
Fault	Requires a reset	800	HIGH
Fault	Protected	1000	HIGH

When alarms are reset on the drive, they are no longer active on OPC UA. The condition name contains the event number from the event log in MyDrive® Insight and the option slot number where the event originates from.

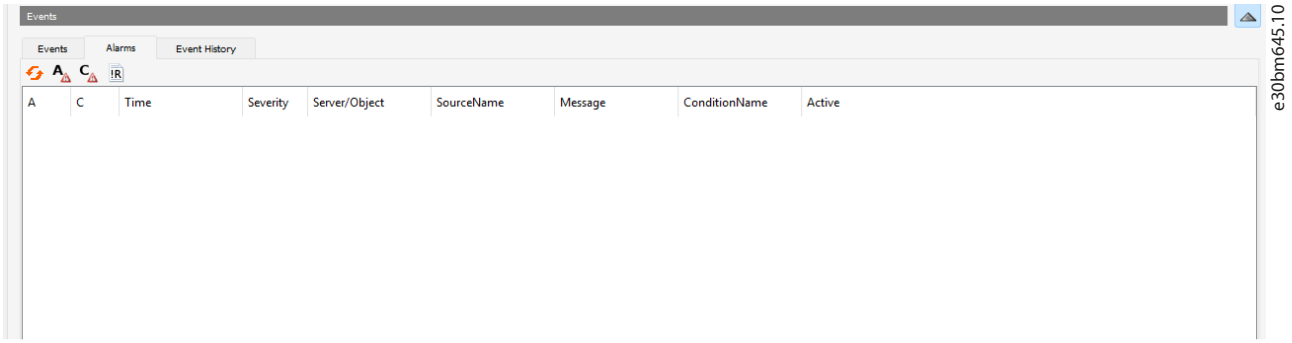


Figure 31: Example of Alarms in UaExpert

3.10 Subscribing to Events

1. Add the event view to *Documents* in UaExpert.

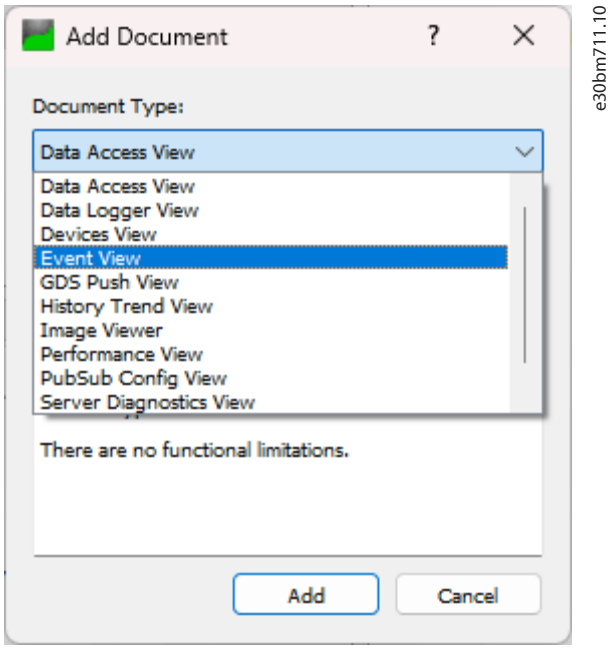


Figure 32: Adding the Event View

2. Drag the server into the *Configuration* view.

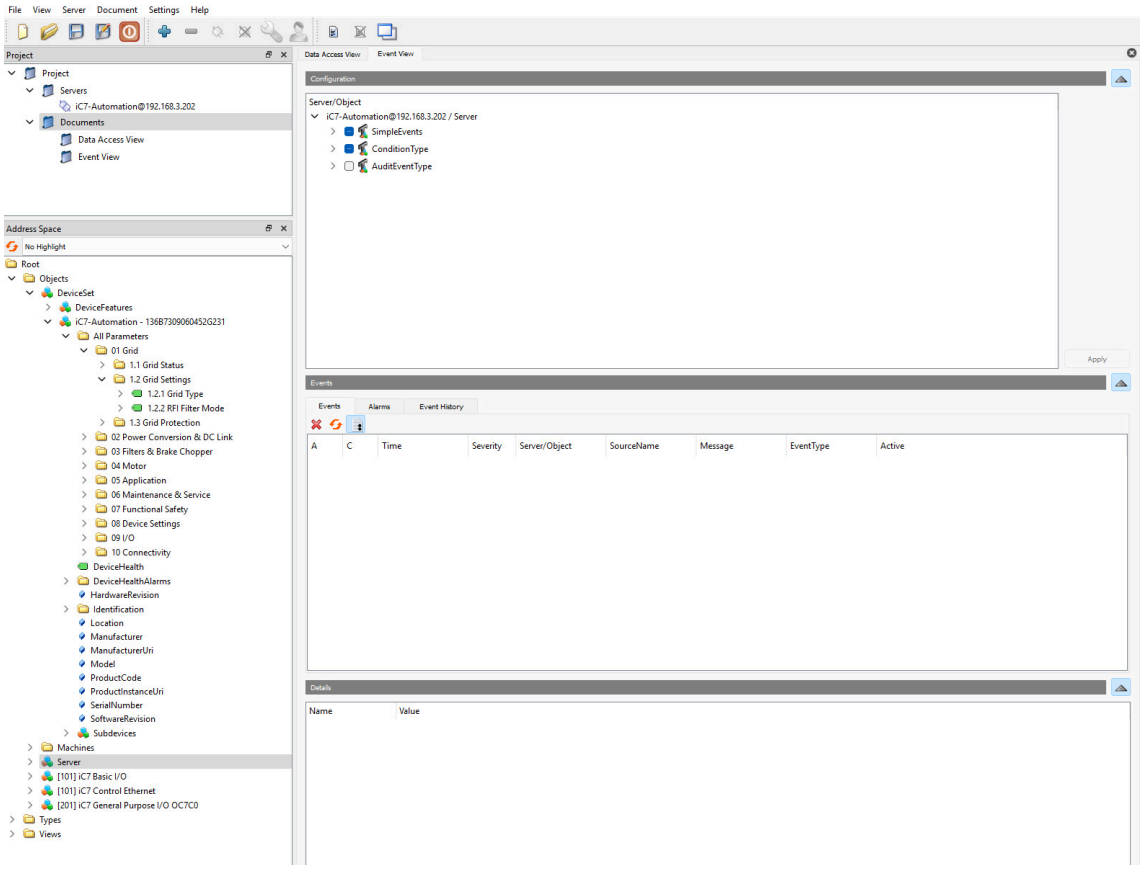


Figure 33: Adding the Server

When alarms are triggered in the server, information about the alarm is shown in the *Alarms* tab. The condition name contains the event number from the event log in MyDrive® Insight and the option slot number where the event originates from.

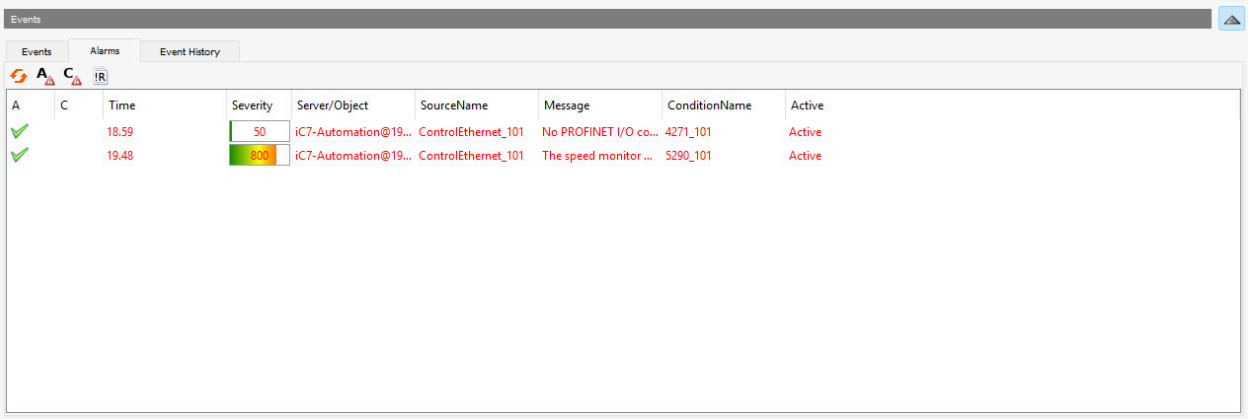


Figure 34: Viewing Alarms in UaExpert

When alarms are reset on the drive, they are no longer active on OPC UA.

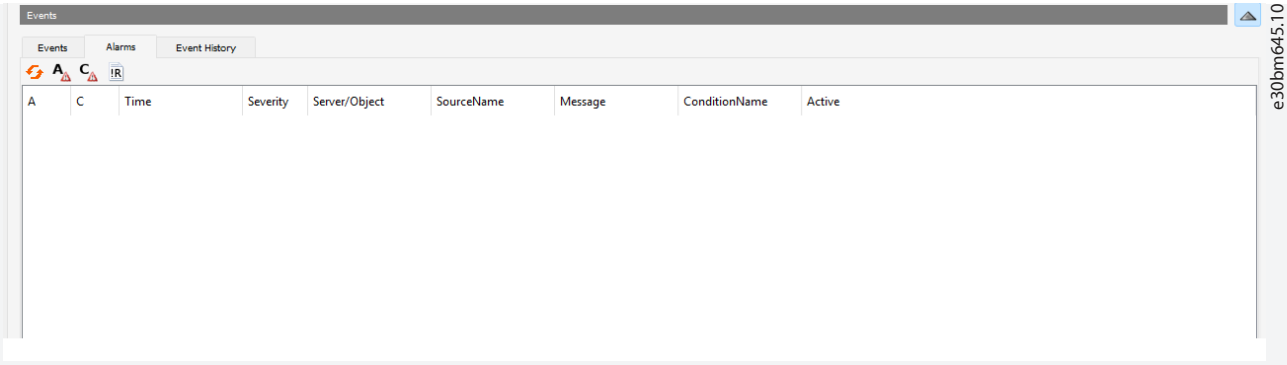


Figure 35: Cleared Alarms in UaExpert

4 Troubleshooting

Table 13: Troubleshooting OPC UA

Problem	Solution
Locked out of the device	If a previously created certificate prevents OPC UA communication from being established, use MyDrive® Insight to restore security settings to factory default settings.
	For forgotten account passwords, use an administrative account with the SecurityAdmin role to modify the settings for the account. When no administrative accounts are accessible, use the control panel to restore factory default settings. See the application guide for instructions.
Unable to push certificates to the device	Make sure that OPC UA is running and in provisioning mode on the device. Use the OPC UA status report to see the status of OPC UA of the device.
	Make sure that certificates are pushed to the device using an account that has the SecurityAdmin role.
Unable to log in from OPC UA	Check that the user account exists on the device. Log in to MyDrive® Insight using an account with the SecurityAdmin role to see the full list of user accounts.
	Make sure that the correct password is used for the user account. Check that the same user name and password can be used to log into MyDrive® Insight.
	Some OPC UA clients do not allow using empty passwords. Make sure that a password has been configured for the user account.
Unable to establish secure communication with the device from client	Make sure that the device has received a valid device certificate.
	Verify that the certificate of the device is valid for the device. For example, if the IP address or name of the device is changed, a new certificate needs to be created for the device.
	Make sure that the system clock is set to the correct time.
	Make sure that the certificate of the device has not expired.
	Check whether the certificate has been revoked.
	Check that the certificate is trusted by the client.
	Make sure that the client has access to the full certificate chain to validate the signature of the device certificate.
The client is unable to connect to the drive.	Make sure that the device supports OPC UA. Drives that support OPC UA have the OPC UA parameters shown in parameter group *10.3.6 OPC UA*. If no manifest is available, the drive or application does not support OPC UA.
	Check that the device can be reached through ping. If no reply is received: • Check the IP address configured for the device and client. • Check the cables and link.
	Check that OPC UA is enabled for the interface connected to the client. For information on changing the active OPC UA interface, see 3.3.1 Configuring OPC UA.
The client is unable to modify the data of nodes	Only authorized users are allowed to modify the data of the device. Make sure that the user account used to log in is an authorized user.
	Not all data is modifiable through OPC UA. Make sure that the data is writable.
	Some clients require an additional apply to write the data configured. Make sure that the client sends the write request as expected.
X1/X2 interface is not available in the selection list for the parameter	The X1/X2 interface is not available on the drive. Use X0 instead.
	The fieldbus configured for the X1/X2 interface does not support IP traffic. Use the X0 interface for OPC UA communication.

Danfoss A/S
Ulsnaes 1
DK-6300 Graasten
drives.danfoss.com

M00468
AQ513539982268en-010201
Danfoss A/S © 2026.05

136R0391