ibaPDA-OPC-UA-Server+

OPC UA Server for Measurement Data

Manual

Issue 1.2

Measurement Systems for Industry and Energy

www.iba-ag.com

Manufacturer

iba AG

Koenigswarterstr. 44

90762 Fuerth

Germany

Contacts

Main office	+49 911 97282-0
Fax	+49 911 97282-33
Support	+49 911 97282-14
Engineering	+49 911 97282-13
E-mail	iba@iba-ag.com
Web	www.iba-ag.com

The content of this publication has been checked for compliance with the described hardware and software. Nevertheless, discrepancies cannot be ruled out, and we do not provide guarantee for complete conformity. However, the information furnished in this publication is updated regularly. Required corrections are contained in the following regulations or can be downloaded on the Internet.

The current version is available for download on our web site www.iba-ag.com.

Version	Date	Revision - Chapter / Page	Author	Version SW
1.2	01-2022	Note on update cycle; writable tags; certificate store	RM	7.2.0

Content

1 About this manual

This documentation describes the function and application of the software

ibaPDA-OPC-UA-Server+.

1.1 Target group and previous knowledge

This documentation is aimed at qualified professionals who are familiar with handling electrical and electronic modules as well as communication and measurement technology. A person is deemed to be a professional if they are capable of assessing the assigned work and identifying possible risk areas on the basis of their specialist training, expertise and experience as well as knowledge of the applicable regulations.

In particular, this documentation is intended for personnel involved in the engineering, testing, commissioning or maintenance of the respective programmable logic controllers and communication systems. For the handling of *ibaPDA-OPC-UA-Server+* the following basic knowledge is required and/or useful:

- Windows operating system
- Basic knowledge of *ibaPDA*
- Experience of configuring an OPC UA server

1.2 Notations

In this manual, the following notations are used:

Action	Notation
Menu command	Menu *Logic diagram*
Calling the menu command	*Step 1 – Step 2 – Step 3 – Step x* Example: Select the menu *Logic diagram - Add - New function block*.
Keys	<Key name> Example: <Alt>; <F1>
Press the keys simultaneously	<Key name> + <Key name> Example: <Alt> + <Ctrl>
Buttons	<Key name> Example: <OK>; <Cancel>
File names, paths	"Filename", "Path" Example: "Test.doc"

1.3 Used symbols

If safety instructions or other notes are used in this manual, they mean:

Danger!

The non-observance of this safety information may result in an imminent risk of death or severe injury:

- Observe the specified measures.

Warning!

The non-observance of this safety information may result in a potential risk of death or severe injury!

- Observe the specified measures.

Caution!

The non-observance of this safety information may result in a potential risk of injury or material damage!

- Observe the specified measures

Note

A note specifies special requirements or actions to be observed.

Tip

Tip or example as a helpful note or insider tip to make the work a little bit easier.

Other documentation

Reference to additional documentation or further reading.

2 System requirements

The following system specifications are required for use of OPC UA Server+:

- *ibaPDA v7.0.0* or higher
- License for *ibaPDA-OPC-UA-Server+*
- Network connection to one or more OPC UA clients

Other documentation

Further requirements for the respective computer hardware and the supported operating systems can be found in *ibaPDA* documentation.

Note

It is advisable to run the OPC UA communications for data acquisition on a separate network to avoid interference from the Ethernet data traffic between *ibaPDA* and other network nodes (file servers, data file requirements, etc.), which may affect the OPC UA data telegrams.

License information

Order No.	Product designation	Description
30.670051	ibaPDA-OPC-UA-Server+	Extension license for an *ibaPDA* system which adds the function: OPC UA Server+

Table 1: Available OPC UA Server+ licenses

3 OPC UA Server and OPC UA Server+

3.1 General information

By default, *ibaPDA* provides the OPC UA server functionality in order to make data and information about its own status publicly available. This includes information such as

- Issue
- Active licenses
- Status of data acquisition and recording
- Connected OPC UA clients

The OPC UA server function is thus used as an alternative to the SNMP interface or the watchdog telegram in order to inform other systems about the status of *ibaPDA* .

With the *ibaPDA-OPC-UA-Server+* extension, you can also publish all recorded or calculated signals as well as text channels via OPC UA.

This allows other systems with OPC UA client functionality to access data collected by *ibaPDA* .

The signals that are published via OPC UA can be conveniently selected using the signal tree in the *ibaPDA* Manager.

The signal values are updated cyclically.

Note

The tags in the OPC UA server are refreshed at the same rate as the *ibaPDA* outputs. Thus, the fastest update cycle derives from the least common multiple of all module time bases or is at least 50 ms respectively.

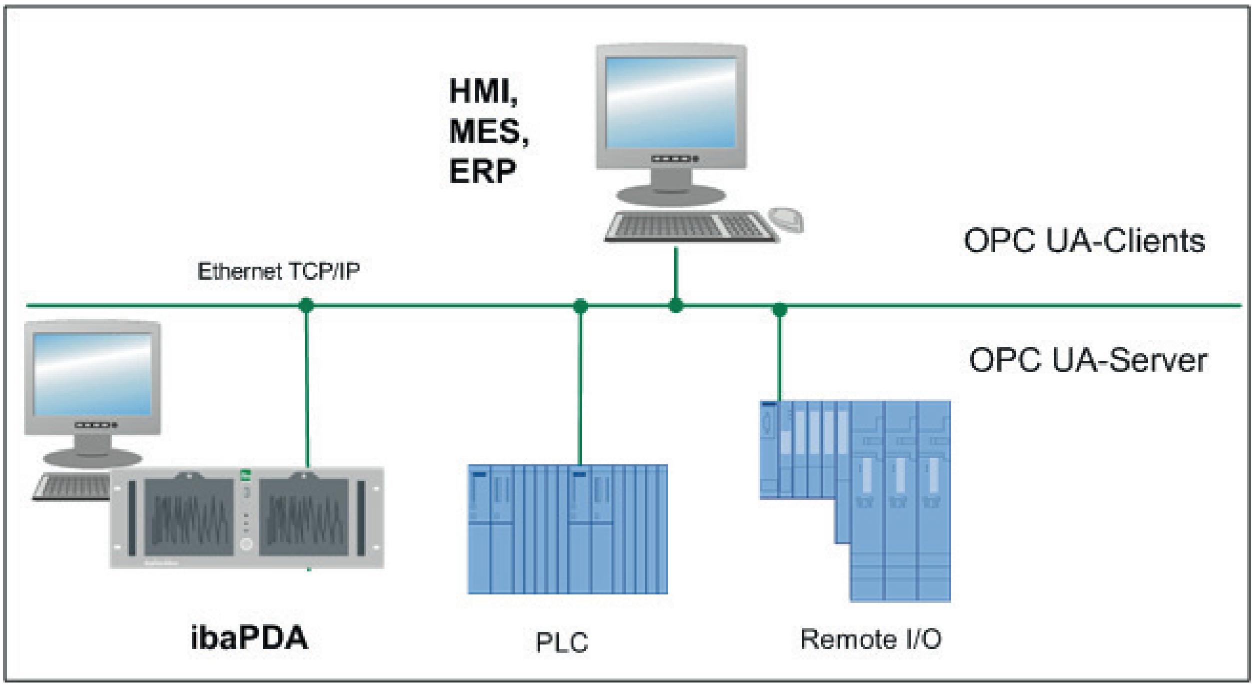
The OPC UA clients can only read (but not write) the tags provided by *ibaPDA* as the OPC UA server.

If required, you may add so called *Writable Tags* (analog and digital) to the OPC UA server data model. By means of an *OPC UA server module*, which can be added on the interface node *OPC UA*, it is possible that OPC UA clients can write values into the OPC UA server of *ibaPDA*. In order to use *Writable Tags* and the *OPC UA server module* you will also need the license *ibaPDA-OPC-UA-Server+*.

You can import or generate the certificates required for communication between the OPC UA server (*ibaPDA*) and an OPC UA client in *ibaPDA*.

3.2 System topologies

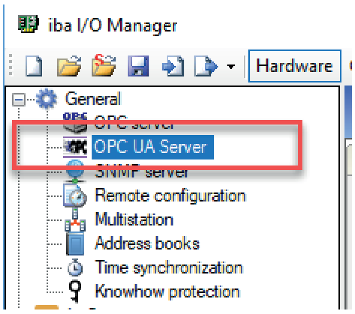
The following drawing gives an overview of a possible configuration.



4 Configuration and engineering ibaPDA

Open the I/O manager, e.g., from the toolbar .

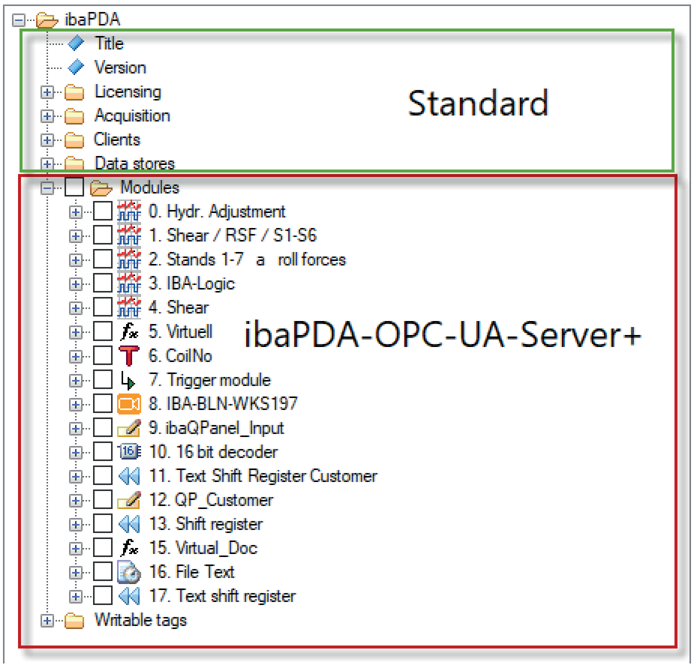
You will see the *OPC UA-Server* node in the signal tree under *General*.



Select the node and then select the *Tags* tab on the right.

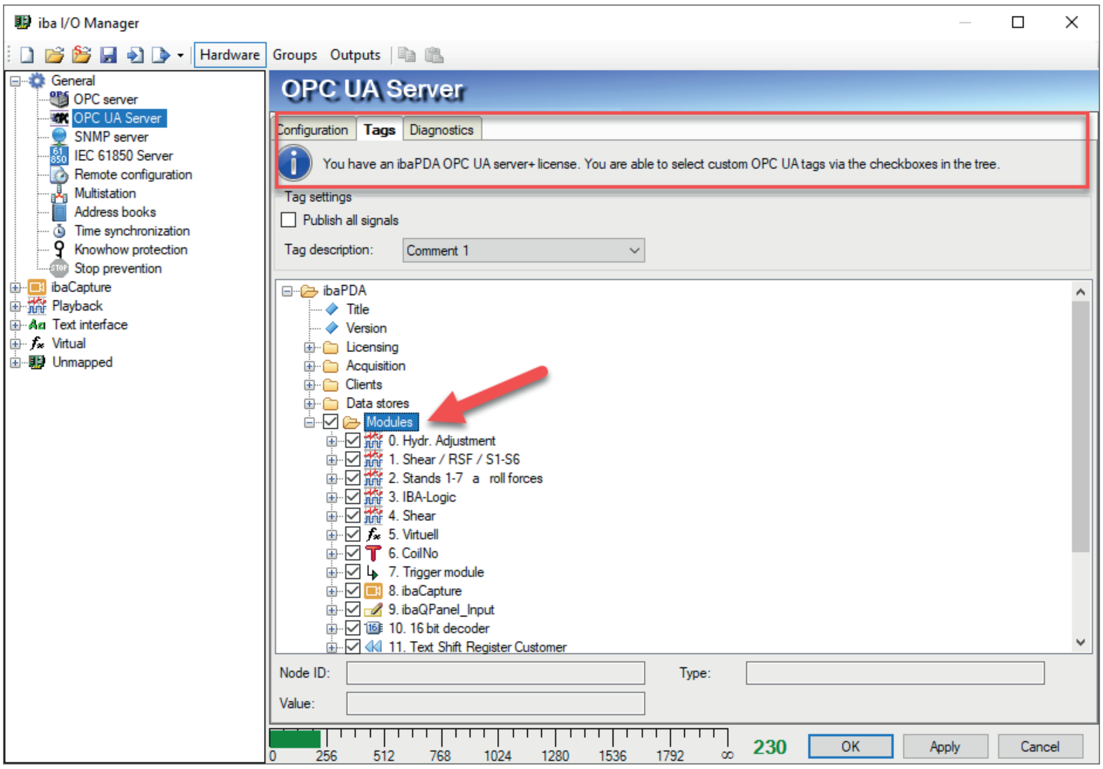
In the tab you will see a signal tree with the tags that *ibaPDA* makes available. The tags that are available in the standard version do not have check boxes.

The signals or tags under the *Modules* node have check boxes and can only be used with the *ibaPDA-OPC-UA-Server+* license.



If the OPC UA Server+ function is not enabled in your dongle, a note appears at the top of the tab.

If the OPC UA Server+ function is enabled in your dongle, you will find a corresponding note in the tab and you can check the boxes to select signals.



You have an ibaPDA OPC UA server+ license. You are able to select custom OPC UA tags via the checkboxes in the tree.

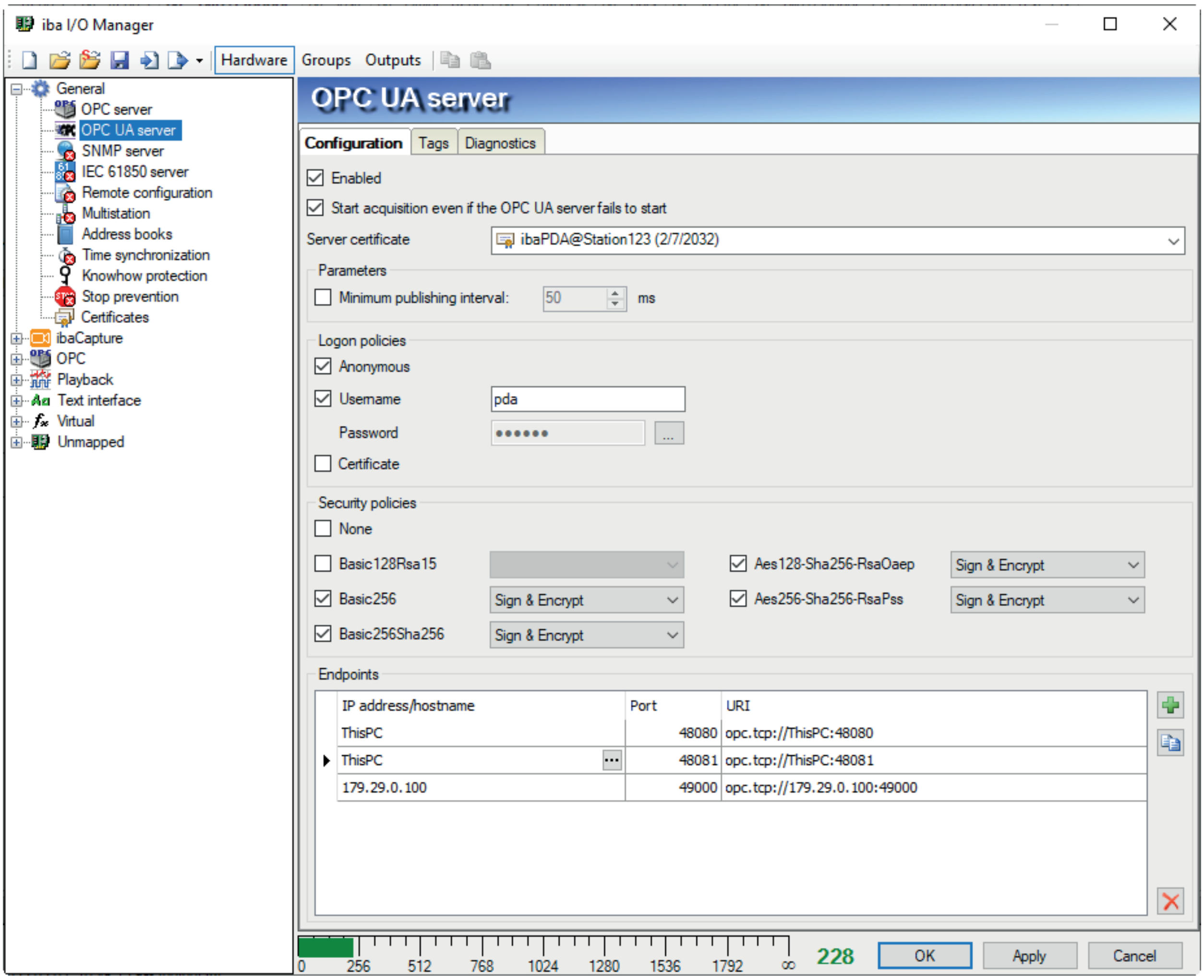
Tag settings

□ Publish all signals

Tag description: Comment 1

4.1 OPC UA Server – Configuration

To configure further settings, you first need to enable the OPC UA server in the *Configuration* tab.



☑ Enabled

☑ Start acquisition even if the OPC UA server fails to start

Server certificate: ibaPDA@Station123 (2/7/2032)

Parameters

☐ Minimum publishing interval: 50 ms

Logon policies

☑ Anonymous

☑ Username: pda

Password: ••••••

☐ Certificate

Security policies

☐ None

☐ Basic128Rsa15		☑ Aes128-Sha256-RsaOaep	Sign & Encrypt
☑ Basic256	Sign & Encrypt	☑ Aes256-Sha256-RsaPss	Sign & Encrypt
☑ Basic256Sha256	Sign & Encrypt		

Endpoints

IP address/hostname	Port	URI
ThisPC	48080	opc.tcp://ThisPC:48080
ThisPC	48081	opc.tcp://ThisPC:48081
179.29.0.100	49000	opc.tcp://179.29.0.100:49000

Enabled
Check this box to enable the OPC UA server function.

Start acquisition even if the OPC UA server fails to start
If this option is enabled, the acquisition will start even if the OPC UA server cannot be started. In case of an error, a warning is indicated in the validation dialog. If the system has been started without an OPC UA server, *ibaPDA* will periodically try to start the OPC UA server. If the OPC UA server has not been started, no OPC UA variables will be published and *ibaPDA* will not be visible as an OPC UA server in the network.

Server certificate
Select the certificate that the OPC UA server should use from the drop-down list.

If you have not yet generated or imported a certificate, you can do so by selecting *Create new certificate* or *Manage certificates* from the list.

You will then be redirected to the central certificate store, which you can also find in the interface tree under *General - Certificates*.

The handling of certificates is described in chapter ↗ *Certificates*, page 15.

Parameters

If required, you can adjust the publishing interval of the OPC UA server here.

If you do not enable this option (default), the publishing interval is based on the smallest common multiple of all module time bases – as is the case with all other output interfaces – and is a minimum of 50 ms.

If you enable this option, you can set the publishing interval to a higher value, e.g., 500 ms. This ensures that the OPC UA server does not publish its tags faster than every 500 ms, even if a higher publishing rate is required by the clients.

This option can be used, for example, to counteract an overload of the communication bandwidth if many OPC UA clients are requesting large volumes of data from the server.

Login policies

At least one of the following login rules should be applied:

Anonymous
If this option is enabled, clients can log in to the OPC UA server without login credentials (user/password).

User name/password
If this option is enabled, clients can only log in if they can authenticate themselves by user name and password as configured in this dialog.

By clicking the 👁 button, the password will be temporarily displayed in a readable format.

Certificate
If this option is enabled, clients can log in if they can authenticate themselves by using a trusted certificate.

Security policies

At least one of the options must be enabled.

If you enable the option *None*, then connections without encryption are also supported.

For each of the other options or encryption types, you can select a security rule with signature and/or encryption:

- Sign
- Sign & Encrypt
- Sign + Sign & Encrypt

Note

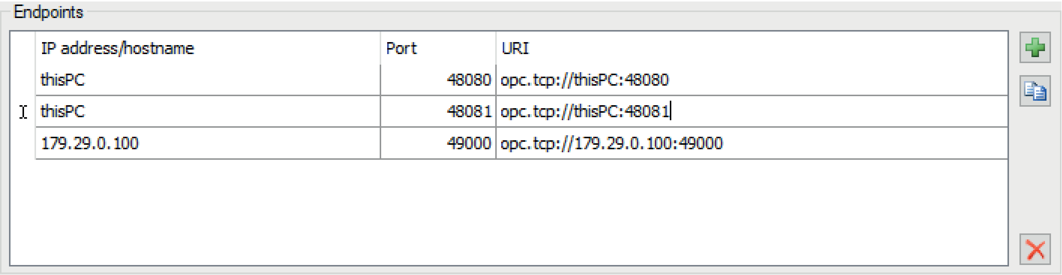
Basic128Rsa15 and Basic256 encryption are now obsolete.

For security reasons, the use of Basic256Sha256, Aes128-Sha256-RsaOaep or Aes256-Sha256-RsaPss encryption is preferred.

Endpoints

This area of the dialog lets you configure the local endpoints that the server will provide.

An endpoint is a combination of an IP address and a port number. Instead of entering a specific IP address, it is also possible to enter the computer name of the OPC UA server. This applies to all IP addresses of all network interfaces in the system. The URI (Uniform Resource Identifier) is formed from the IP address or computer name and the port number.



Endpoints

IP address/hostname	Port	URI
thisPC	48080	opc.tcp://thisPC:48080
thisPC	48081	opc.tcp://thisPC:48081
179.29.0.100	49000	opc.tcp://179.29.0.100:49000

In the example above, OPC UA clients can connect to the OPC UA server from any network using port 48400 or 48401. In addition, clients can also connect to IP address 172.29.0.100 via port 49000.

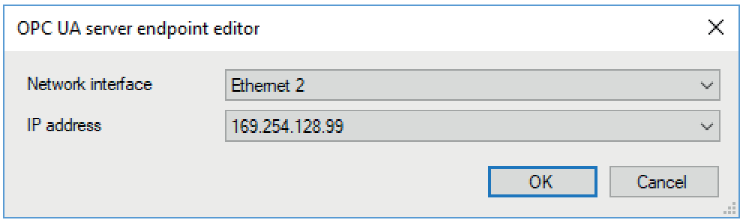
The list of endpoints includes some controls:

Button	Function
✚	Use this button to add a new endpoint. Initially, the new endpoint always has the same data as the local computer, which then needs to be edited.
⧉	This button lets you duplicate the selected endpoint, which you can then edit.
✕	Use this button to delete the selected endpoint from the list.

Table 2: Control elements for the endpoint list

By default, the name of the local computer is already entered in the list.

If you click on an endpoint in the list, the button … will appear. Click on this button to edit the endpoint.


OPC UA server endpoint editor

Network interface: Ethernet 2

IP address: 169.254.128.99

Select the desired network interface via which the OPC UA clients should communicate. The drop-down list shows all of the computer's available network interfaces with all IP addresses.

Click <OK> and the selected IP address will be displayed in the list.

Note

Currently only IPv4 addresses are supported.

4.2 Certificates

Communication with the OPC UA server is secured by means of certificates. The certificates are managed in the central certificate store in *ibaPDA*. This store also contains other certificates, e.g., for interfaces and data stores, in addition to the certificates for OPC UA communication.

4.2.1 Introduction

For secure and encrypted TLS/SSL communication between a client and a server, so-called certificates are used because they enable secure authentication.

Before a client can connect to a server, an application certificate must first be configured. Certificates can be provided from both the server and client side. Communication can only take place if each partner trusts the partner certificate.

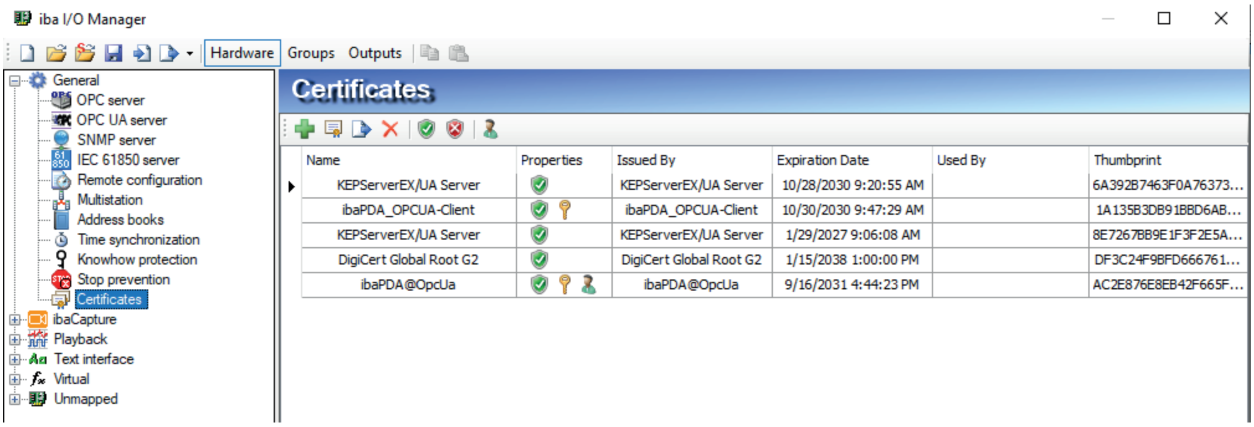
Certificates can either be exchanged spontaneously when a connection is established or registered as trusted in advance. If a previously unknown certificate is offered when a connection is established, the user must manually accept or reject the certificate. Accepted certificates are automatically entered into the table in the *certificate store* and marked as trusted. If the certificate is rejected, then no communication will take place.

You can also register certificates and then mark them as "not trusted". Communication with partners with such certificates is then always denied. Once certificates have been registered, i.e., entered in the table in the certificate store, the user will no longer be notified or prompted when communication is established – regardless of whether the certificates are marked as "trusted" or "not trusted".

Some interfaces in *ibaPDA*, such as the e-mail output, use Windows certificates. Other features, such as OPC UA server or MQTT data stores use certificates from the central certificate store of *ibaPDA*.

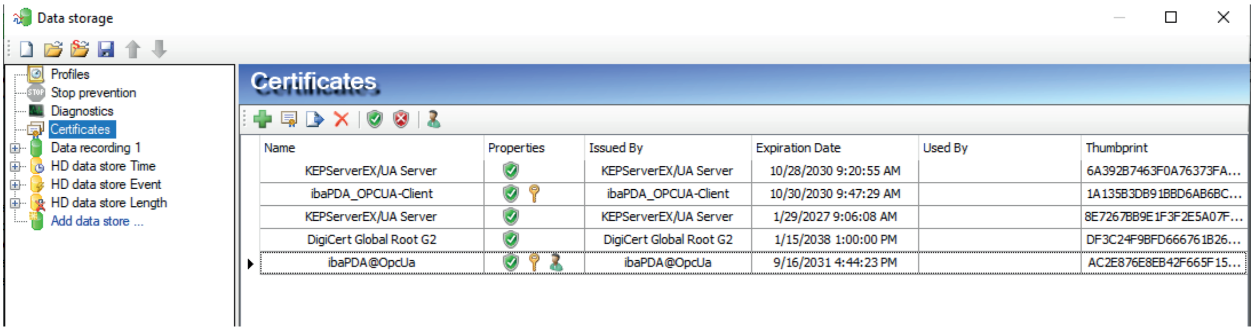
4.2.2 Central certificate store

All registered certificates are listed in a table that is available on the *Certificates* node in I/O Manager and in the data store configuration. The following figure shows the certificate store in the I/O Manager.



	Name	Properties	Issued By	Expiration Date	Used By	Thumbprint
▶	KEPServerEX/UA Server	✓	KEPServerEX/UA Server	10/28/2030 9:20:55 AM		6A392B7463F0A76373...
	ibaPDA_OPCUA-Client	✓ 🔑	ibaPDA_OPCUA-Client	10/30/2030 9:47:29 AM		1A135B3DB91BBD6AB...
	KEPServerEX/UA Server	✓	KEPServerEX/UA Server	1/29/2027 9:06:08 AM		8E7267BB9E1F3F2E5A...
	DigiCert Global Root G2	✓	DigiCert Global Root G2	1/15/2038 1:00:00 PM		DF3C24F9BFD666761...
	ibaPDA@OpcUa	✓ 🔑 👤	ibaPDA@OpcUa	9/16/2031 4:44:23 PM		AC2E876E8EB42F665F...

The following figure shows the certificate store in the data store configuration.

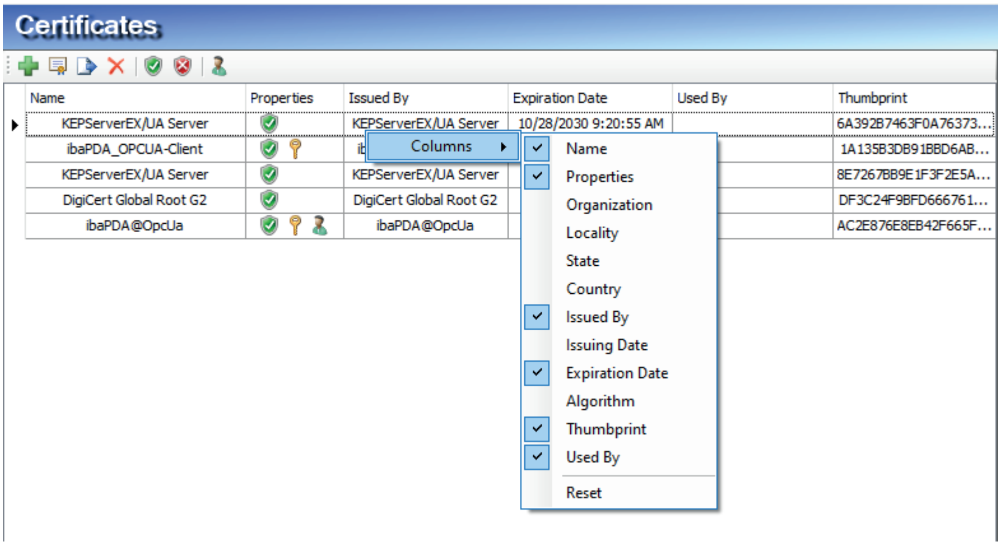


	Name	Properties	Issued By	Expiration Date	Used By	Thumbprint
	KEPServerEX/UA Server	✓	KEPServerEX/UA Server	10/28/2030 9:20:55 AM		6A392B7463F0A76373FA...
	ibaPDA_OPCUA-Client	✓ 🔑	ibaPDA_OPCUA-Client	10/30/2030 9:47:29 AM		1A135B3DB91BBD6AB6BC...
	KEPServerEX/UA Server	✓	KEPServerEX/UA Server	1/29/2027 9:06:08 AM		8E7267BB9E1F3F2E5A07F...
	DigiCert Global Root G2	✓	DigiCert Global Root G2	1/15/2038 1:00:00 PM		DF3C24F9BFD666761B26...
▶	ibaPDA@OpcUa	✓ 🔑 👤	ibaPDA@OpcUa	9/16/2031 4:44:23 PM		AC2E876E8EB42F665F15...

Each line represents one certificate.

By default, the columns *Name*, *Properties*, *Expiration date* and *Used by* are displayed.

If necessary, you can select or deselect additional columns in the table's context menu.



	Name	Properties	Issued By	Expiration Date	Used By	Thumbprint
▶	KEPServerEX/UA Server	✓	KEPServerEX/UA Server	10/28/2030 9:20:55 AM		6A392B7463F0A76373...
	ibaPDA_OPCUA-Client	✓ 🔑	ib			1A135B3DB91BBD6AB...
	KEPServerEX/UA Server	✓	KEPServerEX/UA Server			8E7267BB9E1F3F2E5A...
	DigiCert Global Root G2	✓	DigiCert Global Root G2			DF3C24F9BFD666761...
	ibaPDA@OpcUa	✓ 🔑 👤	ibaPDA@OpcUa			AC2E876E8EB42F665F...

The *Name* column contains the name of the certificate. This is not necessarily unique, because several certificates can have the same name. Only the fingerprint is unique for every certificate.

The symbols in the *Properties* column have the following meaning:

Symbol	Meaning
✓	The certificate is trusted as long as it has not expired.
✗	This certificate is not trusted.
🔑	A private key for this certificate is available.
👤	This certificate can also be used for user authentication.

Table 3: Symbols for certificate properties

The *Used by* column shows by which application/function the certificate is used. In the example shown in the figure above, the certificate ibaPDA003@D is used by the OPC UA server in *ibaPDA*. This means that this certificate was selected during configuration of the OPC UA server.

The display is a combination of the currently open manager (I/O or data storage) and the other one. The field in the *Used by* column has a link function. Double-click on a filled field to jump to the corresponding configuration dialog within the opened manager. If the entry belongs to the other manager, the link will not work. In the example above, double-clicking on the entry "OPC UA-Server" would directly open the configuration dialog of the OPC UA server, if this is done from within the I/O Manager. If you had opened the certificate store in the data logging configuration, the link to the OPC UA server would not work.

Conversely, opening an "MQTT data storage" would only work if the certificate store was opened from within the data storage configuration.

4.2.3 Manage certificates

The central certificate store is used to manage the certificates. Here you can add, create and delete certificates.

In the certificate store toolbar you will find a number of buttons with the following functions:

Button	Function
✚	This button opens a dialog that allows you to load an existing certificate file. Various file formats are supported (.der, .cer, .crt, .cert, .pem, .pfx, .p12). If you have a certificate with an unknown file extension, expand the file filter to "*.*" and try to open the file anyway. This works in most cases.
📄	This button opens a dialog that lets you create a new certificate file.
➔	This button lets you export a certificate to a file to register it for Windows or another application, e.g. on an OPC UA client. Multiple file formats are supported here as well.
✕	Use this button to remove the selected certificate from the table.
✓	Use this button to designate the selected certificate as "trusted".
✗	Use this button to designate the selected certificate as "not trusted". However, the certificate will still remain in the certificate store table. However, certificates that are not trusted are not available in the selection list for use in the corresponding configuration dialog.
👤	With this button you can define whether a certificate can also be used for user authentication for OPC UA.

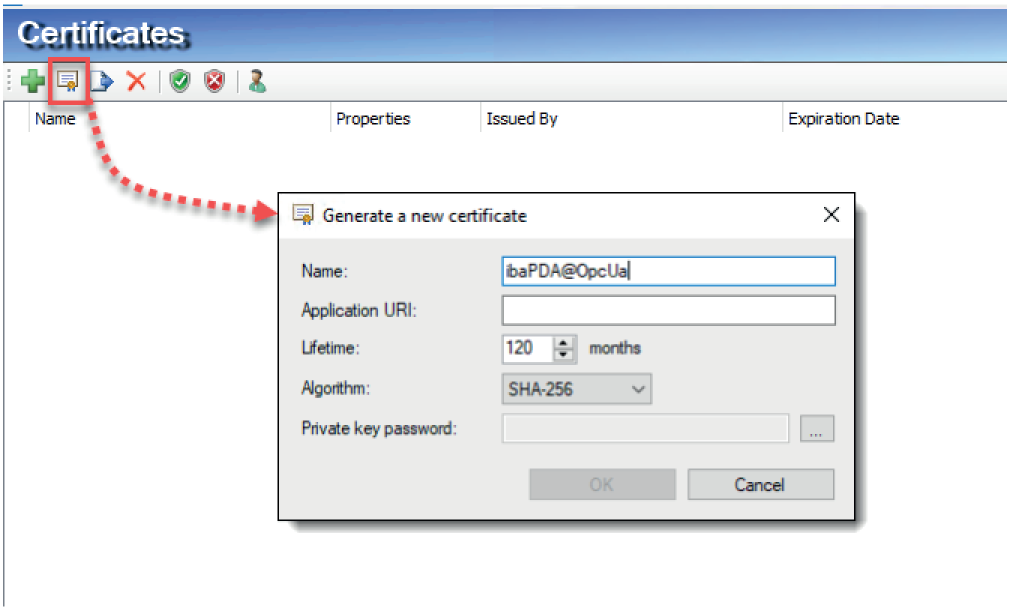
Table 4: Buttons in the toolbar for certificate management

The commands always refer to the certificate selected in the table, which is indicated by an arrow on the left at the start of the line.

4.2.3.1 Create a new certificate

If there are not yet any certificates that you can load, then you will need to create one.

1. Click on the button and the following dialog opens



Generate a new certificate

Name: ibaPDA@OpcUa

Application URI:

Lifetime: 120 months

Algorithm: SHA-256

Private key password:

2. Enter any name for the certificate.
3. Enter an application URI if required.
The URI (Uniform Resource Identifier) is a globally unique identifier for the application, in this case *ibaPDA*. If you do not fill in this field, then – provided that an application URI is verified by the OPC UA client – a default URI will be generated that consists of the machine name and application name:
`urn:machinename:applicationName.`
4. Select the desired validity period for your certificate.
5. Select the desired hash algorithm for encryption.
SHA-1 is an older hash algorithm that is now considered insecure and whose use is no longer recommended. Some older or simpler OPC UA clients only support this algorithm. Increasingly, algorithms in the SHA-2 family, e.g., SHA-256, are being used, which offer a higher encryption depth and thus greater security. For security reasons, this should be the preferred choice, provided that the planned clients also support it.
6. Enter a password of your choice for the private key. If no password has been entered, the <OK> button remains inactive. To assign the password, click the <...> button and enter the password twice and confirm with <OK>. The password field must not be left blank. There are no special requirements for the password. Keep the password in a safe place so that the self-generated certificate can be exported and used for Windows or other applications.
7. Close the dialog with <OK>.

The new certificate is now entered into the list held by the certificate store and immediately assigned the properties "trusted" + private key.

You can now also export the certificate and register it with the communication partner, e.g., an OPC UA client. Afterwards, the client can then connect to *ibaPDA* (OPC UA-Server).

4.2.3.2 Add certificate

1. In the certificate store toolbar, click the button ➕.
   A dialog will open that lets you navigate to the desired certificate file and open it.
   Different file formats are supported (.der, .cer, .crt, .cert, .pem, .pfx, .p12).
   If you have a certificate with an unknown file extension, expand the file filter to "*.*" and try to open the file anyway. This works in most cases.
2. When the certificate is loaded, it appears in the certificate store list.
3. If you have not already done so, trust the certificate.

Certificates can sometimes be added without manual import.

Thus, during the first connection attempt by an OPC UA client to the OPC UA server (ibaPDA), the application certificate of the OPC UA client is automatically added to the certificate list and initially rejected.

Once you have selected the OPC UA client certificate in the list and confirmed it as trusted with the ✓ button, the OPC UA client can subsequently connect automatically.

You can use the ✖ button to reject a certificate at any time or to classify it as not trusted.

4.2.3.3 Export certificates

Certificates created with *ibaPDA* as well as other certificates in the certificate store can be exported individually as a file and subsequently used for Windows or other applications. An exported certificate can also be re-imported into *ibaPDA*.

To export a certificate, first select the desired certificate in the table and then click the button ➡ in the toolbar for the certificate store.

If you wish to export a certificate without a private key, a dialog that lets you save the file opens immediately.

If the certificate to be exported has a private key, there are some options.

First, you will be asked if the existing private key should be exported as well. If you answer "no", the certificate will be saved immediately, just like a certificate without a key.

If you answer "yes", then you must enter the correct password afterwards. The correct password is the password used when importing or generating the certificate. If the password is correct, the certificate can be saved as a .pfx file. This file is password protected and contains the certificate and the private key.

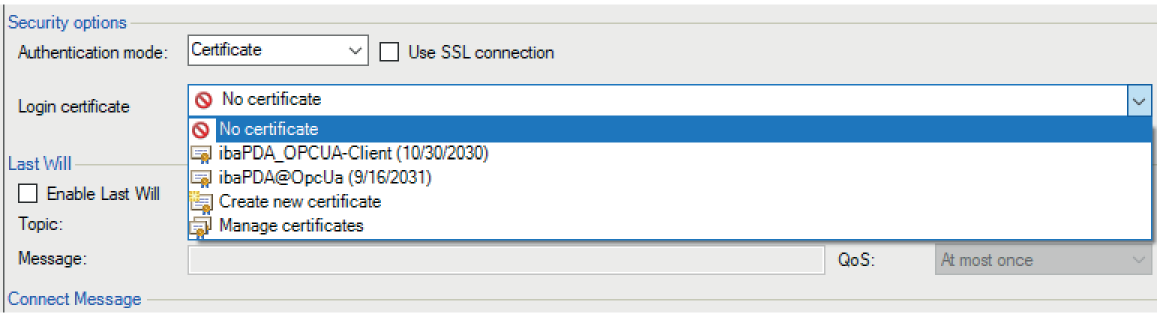
If the password is incorrect, the certificate will not be exported.

Under certain circumstances, a certificate with a private key may be stored in *ibaPDA*, however the key is not password protected. In this case, the certificate can only be exported without a private key. You will then be notified accordingly.

4.2.4 Use certificates

At the points where certificates are applied, you will find a drop-down list offering the available certificates for selection.

For example, in an MQTT data store, the list looks like this:



Security options

Authentication mode: Certificate ☐ Use SSL connection

Login certificate: No certificate

- No certificate
- ibaPDA_OPCUA-Client (10/30/2030)
- ibaPDA@OpcUa (9/16/2031)
- Create new certificate
- Manage certificates

Last Will

☐ Enable Last Will

Topic:

Message: QoS: At most once

Connect Message

- No certificate: No certificate is used. As a rule, this leads to an invalid configuration.
- Available certificates: All certificates are displayed that are contained in the central certificate store, are valid, and are suitable for use at this point.
- Create a new certificate: The dialog for creation of a certificate opens. If the operation is successful, the new certificate is also selected immediately. If not, "No certificate" is selected.
- Manage certificates: Calling up the central certificate store either in the I/O Manager or in the data storage configuration, depending on where you are.

Note

The selected certificate is saved in the registry file of the computer on which the ibaPDA client is running. In case of a new configuration, the same certificate will be selected unless another certificate is actively selected.

Other documentation

For more information on the use and functions of the certificates, please refer to the descriptions of the relevant interfaces, modules and data stores.

4.2.5 Save and protect certificates

The certificates are stored in the `settings.xml` file, which is located in the program directory of *ibaPDA*, in the Server\Certificates subfolder. This file is automatically encrypted.

There are a number of measures whereby certificates with private keys can be used to protect your identity or that of your organization. Specifically, these are measures that make their simple export and reuse in Windows or other applications more difficult.

- Certificates are always stored in encrypted form.
- For certificates with a private key, the input of a password is required...
  - when a new certificate is generated
  - when a certificate with a private key is exported
  - when a certificate with a private key is imported
- Certificates with a private key can only be exported if there is also a password for the key. If there is no password or the password is unknown, the certificate can no longer be exported. Therefore, keep the passwords in a safe place.
- The password for a private key cannot be changed with *ibaPDA*.
- It is not necessary to enter a password to use a certificate in *ibaPDA*. The `settings.xml` file can be copied from one *ibaPDA* installation to another to transfer the certificates there. Password entry is not required for this either.

Should the private key fall into the wrong hands, many types of misuse are possible. Therefore, make sure that the passwords are kept safe.

4.3 OPC UA Server – Tags

This tab displays the tags that can be published by the OPC UA server. Some of them are always available, even if you do not have the *ibaPDA-OPC-UA-Server+* license. These tags therefore have no selection box:

- Software name and version
- Dongle-specific information in the *Licensing* folder
- Status information for the measurement, e.g., whether the measurement is running or disabled signals are present (*Acquisition*)
- Information about the connected *ibaPDA* clients *(Clients)*
- Information about each configured data store, sorted by type (*Data stores*)

In addition to these standard OPC UA tags, you can publish your own tags if you have the *ibaPDA-OPC-UA-Server+* license. All signals configured in the
ibaPDA system are available. By checking the boxes next to the signals or modules, you can also publish these signals as OPC UA tags.

Furthermore, you can create so-called "writable tags" with the *ibaPDA-OPC-UA-Server+* license.

Publish all signals
If you enable this option, all existing signals in *ibaPDA* will be published automatically. This means that even if new signals have been created, they will be automatically published when the configuration is applied. Manually enabling the new signals is no longer necessary.

Note

By default, the tags in the OPC UA server are refreshed at the same rate as the *ibaPDA* outputs. The fastest refresh cycle results from the smallest common multiple of all module time bases and is equal to or longer than 50 ms. A slower refresh cycle can only be set if the option for a different minimum publishing interval is enabled in the *Configuration* tab.

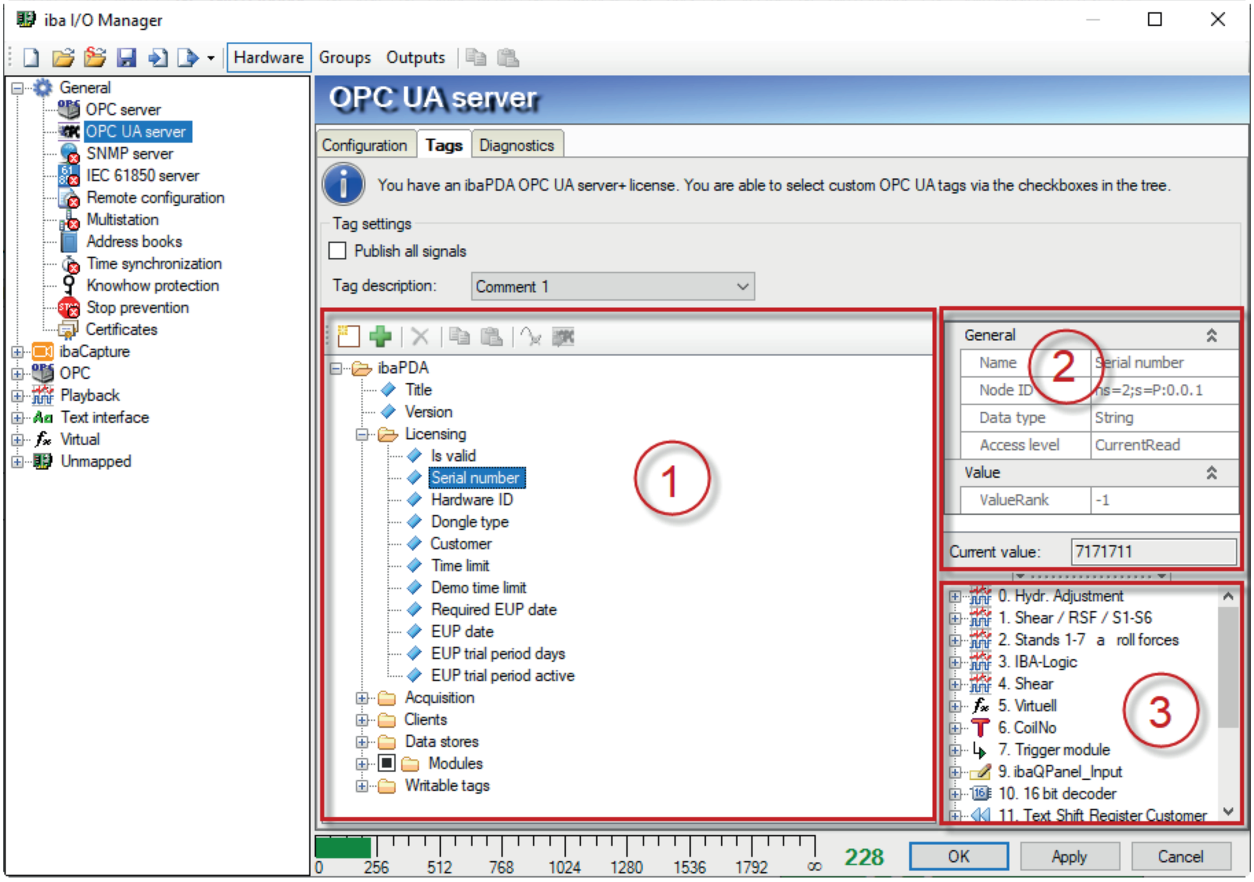
Tag description
This description is shown on an OPC UA client, which connects to the server, when browsing the tags. Thus, a tag could be better described. The user can select either option "Comment 1", "Comment 2" or the combination of both "Comment1 | Comment 2".

Tag directory and info area
The tag directory shows all available tags in a tree structure.

You can perform the following actions here:

- Select the acquired measurement signals in order to publish them
- Add writable tags
- Add custom information models

The info area is located to the right. If you select a tag in the directory, its actual value and additional information, such as the name, node ID and data type, are displayed in the info area.



You have an ibaPDA OPC UA server+ license. You are able to select custom OPC UA tags via the checkboxes in the tree.

Tag settings

☐ Publish all signals

Tag description: Comment 1

General	
Name	Serial number
Node ID	ns=2;s=P:0.0.1
Data type	String
Access level	CurrentRead
Value	
ValueRank	-1

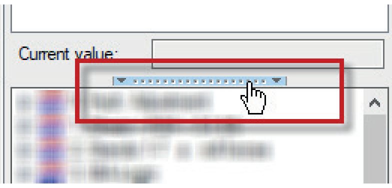
Current value: 7171711

1 Tag directory with standard tags, acquired signals and writable tags as well as information models

2 Info area with tag name, node ID, data type and access level as well as the current value

3 Signal tree window for assigning acquired signals to the tags of a user-defined information model

Click the narrow button on the window frame to show or hide the window.



Above the tag directory is a toolbar with the following functions:

□	Create a new configuration	All configured signals and imported tags are deleted. ibaPDA standard tags are retained.
✚	Add an OPC UA node set	Opens the dialog to import a node set file (*.xml).
✕	Delete selected tag or element	Only available for writable tags folder, writable tags and node set
	Copy selected element to the clipboard	Only available if a copyable element is marked (writable tag or writable tag folder)
📋	Paste clipboard content	Only available if a folder is selected to which the item can be pasted from the clipboard. For example, a copied writable tag can only be pasted to an *Analog* or *Digital* folder.
	Disconnect the signal links to the tags in a node set	Only available if at least one node set exists and either the root folder of the node set, a subfolder within the information model, or a tag is selected. One or more tags selected: The signal links to these tags will be disconnected; Folder selected: The signal links to all tags in this folder will be disconnected; Root node set selected: All signal links to all tags in this node set will be disconnected;
	Assign OPC UA server module	Only available if a writable tags folder is selected. Clicking on this button will create an OPC UA server module with the name of the folder in the I/O Manager under the OPC UA interface. All tags contained in the folder will be transferred to the module's *Analog* and *Digital* signal tables with the name, node ID and data type.

4.3.1 Standard Tags

Licensing

These tags provide information about the dongle, the license number (serial number) and demo or EUP data.

Acquisition

These tags provide information about whether the acquisition is running, whether there are disabled signals, the reason for most recently started acquisition, and how long the acquisition has been running since the last start (in seconds).

Enumeration	Description	Values
IbaEnumPDAStartReason	Possible reasons for the start of the data acquisition	0...none (none) 1...start button (startButton) 2... new I/O configuration (newIOConfig) 10...automatic start (automaticStart) 11. Remote configuration (remoteConfig)

Table 5: Enumerations for start reason for acquisition

Clients

These tags provide information about how many and which *ibaPDA* clients are connected to the *ibaPDA* server. Additional information is provided, such as the logged-in user, IP address, time when the client connected, and the number of currently requested signals. For multiple clients, the corresponding values are separated by commas. The number of values depends on the number of client licenses.

Data Stores

These tags provide information about which data stores are defined and their status. There is a separate branch for each type of data store. If several data stores of one type are defined, the corresponding current values are separated by commas.

Enumeration	Description	Values
IbaEnumDBTimeStoreStatus	The possible states of an DB/Cloud data storage	0...stopped (stopped) 1...wait for trigger (waitForTrigger) 2...recording (recording) 3...post trigger (stopCountDown)
IbaEnumPDAStoreStatus	The possible states of an ibaPDA data storage	0...stopped (stopped) 1...wait for trigger (waitForTrigger) 2...recording (recording) 3...post trigger (stopCountDown)
IbaEnumQDRStoreStatus	The possible states of an ibaQDR data storage	0...stopped (stopped) 1...unsynced (unsynced) 2...synced (synced)
IbaEnumHDStoreStatus	The possible states of an ibaHD data storage	0...stopped (stopped) 1...disconnected (disconnected) 2...recording (recording)

Table 6: Enumerations for status values of data store types

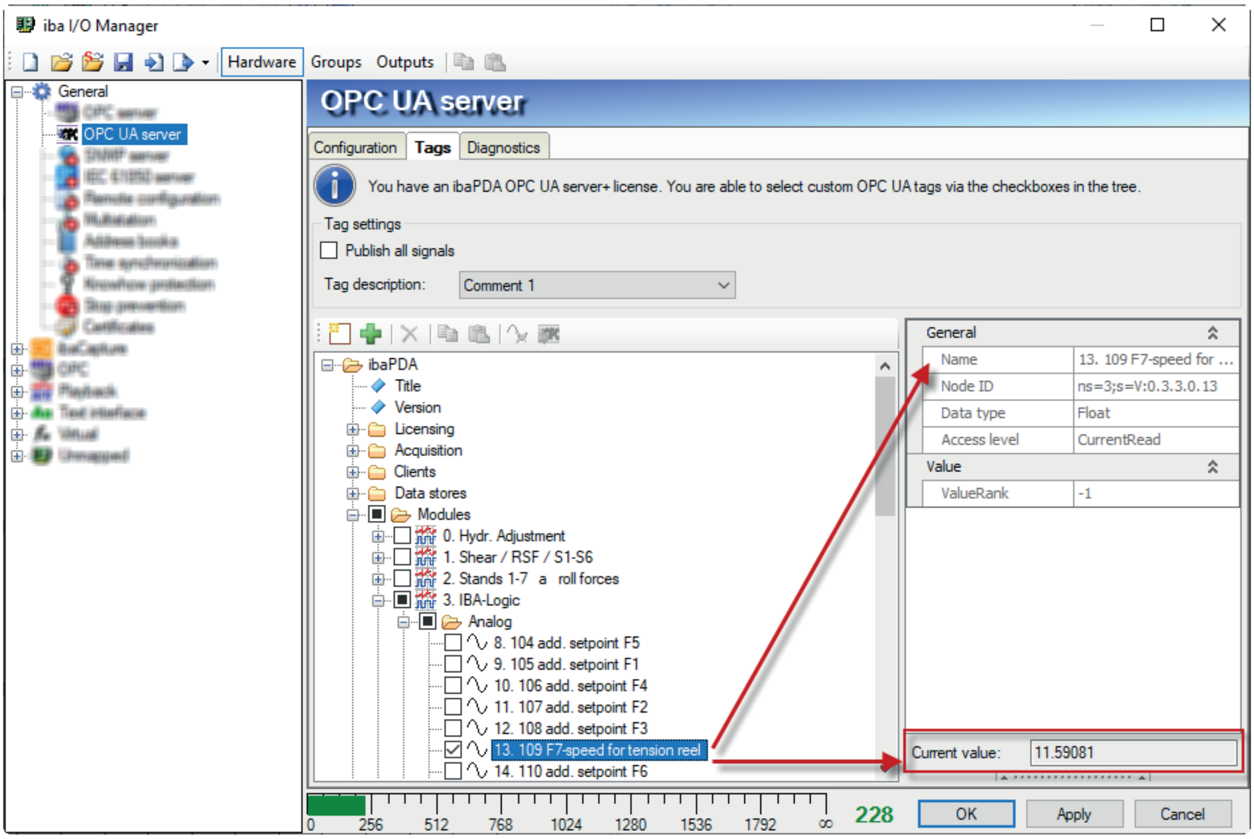
4.3.2 Acquired Signals (Modules)

All signals configured in *ibaPDA*, i.e., analog, digital and text signals, input, output and virtual signals, can be published via the OPC UA server.

In the *Modules* folder in the tag directory, all modules with their signals can be found in the form of the signal tree.

To publish signals, the desired signals or modules must be selected by adding a checkmark.

If you click on a signal tag, the tag data is shown in the info area. The current signal value is only displayed when the acquisition is running.



You have an ibaPDA OPC UA server+ license. You are able to select custom OPC UA tags via the checkboxes in the tree.

Tag settings

□ Publish all signals

Tag description: Comment 1

General	
Name	13. 109 F7-speed for ...
Node ID	ns=3;s=V:0.3.3.0.13
Data type	Float
Access level	CurrentRead
Value	
ValueRank	-1

Current value: 11.59081

4.3.3 Writable Tags

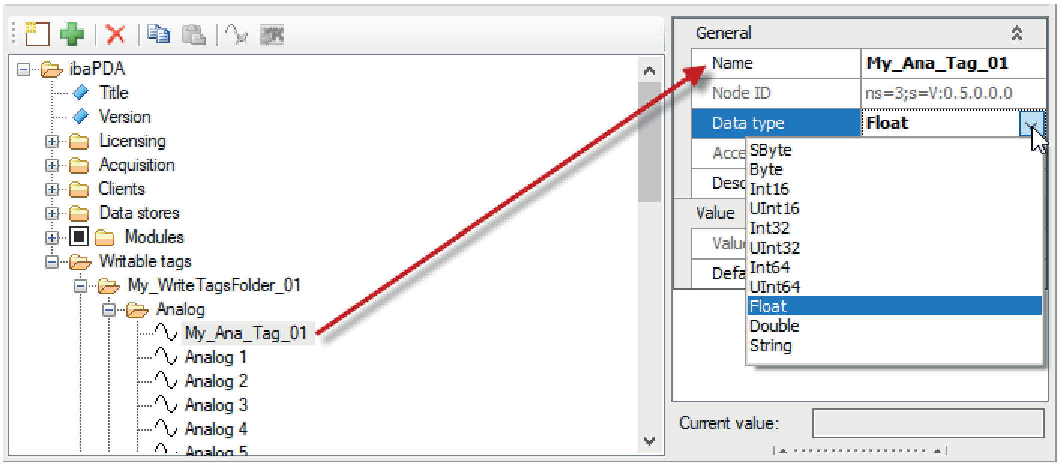
Writable tags are tags that are defined on the OPC UA server but can be read and written by OPC UA clients.

Configuration

You can create as many folders with writable tags as you wish. To do this, expand the *Writable Tags* node and click *Add new writable tag folder*. A new folder will be created with 32 analog and 32 digital signals by default.

Select the folder and give it a suitable name in the *Name* field in the info area.

You can also configure the writable tags here by giving them names, assigning a data type, and specifying a default value if necessary.



Name: My_Ana_Tag_01
Node ID: ns=3;s=V:0.5.0.0.0
Data type: Float

You can also add more tags individually and – by right-clicking – copy or delete them. To paste a copied tag, right-click the desired folder icon and then select *Paste*.

Tip

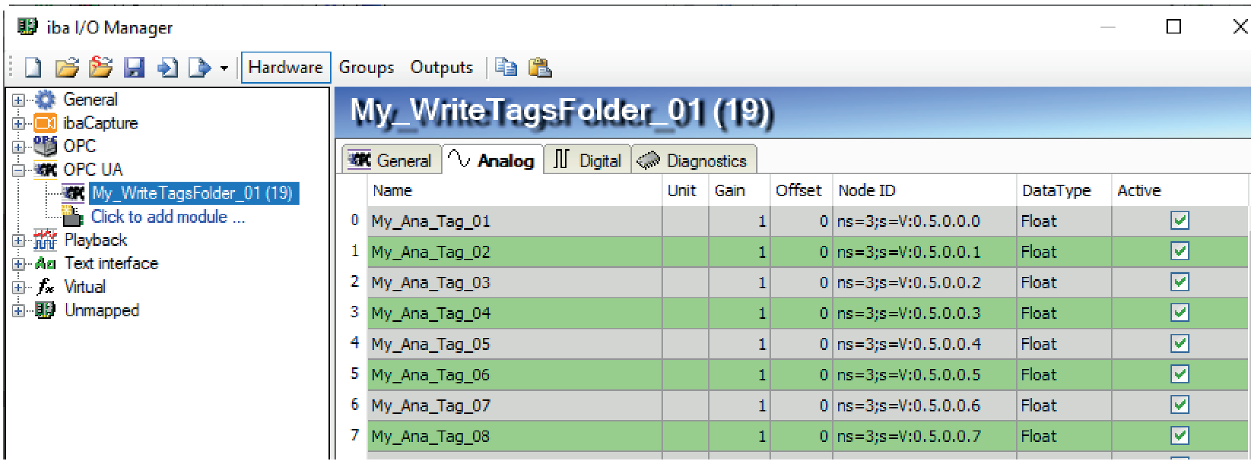
It is advisable to configure the tags fully at this point, i.e., with meaningful names, the data type and, if necessary, a default value. When the OPC UA server is accessed from the client side, the tags will then appear in a readable, understandable form.

Display and record writable tags as signals in ibaPDA

As soon as the writable tags have been defined, they will be available at the OPC UA level. However, in order to display and/or record these tags or their values in *ibaPDA*, they must be assigned to an OPC UA server module.

This can be done very easily by right-clicking on the folder and selecting *Map to OPC UA Server module* from the context menu. Alternatively, you can click the corresponding button.

A corresponding module with the same name as the folder will be created under the OPC UA interface in the I/O manager. For all included tags, the corresponding signals are also automatically created in the module. The name, node ID and data type are inherited as previously configured in the OPC UA server.



	Name	Unit	Gain	Offset	Node ID	DataType	Active
0	My_Ana_Tag_01		1	0	ns=3;s=V:0.5.0.0.0	Float	☑
1	My_Ana_Tag_02		1	0	ns=3;s=V:0.5.0.0.1	Float	☑
2	My_Ana_Tag_03		1	0	ns=3;s=V:0.5.0.0.2	Float	☑
3	My_Ana_Tag_04		1	0	ns=3;s=V:0.5.0.0.3	Float	☑
4	My_Ana_Tag_05		1	0	ns=3;s=V:0.5.0.0.4	Float	☑
5	My_Ana_Tag_06		1	0	ns=3;s=V:0.5.0.0.5	Float	☑
6	My_Ana_Tag_07		1	0	ns=3;s=V:0.5.0.0.6	Float	☑
7	My_Ana_Tag_08		1	0	ns=3;s=V:0.5.0.0.7	Float	☑

If required, you can change the signal names afterwards in the signal tables in the OPC UA server module. This has no effect on the tag names.

Furthermore, you can reconfigure the OPC UA server module by deleting signals or connecting completely different tags to the module via the OPC UA symbol browser.

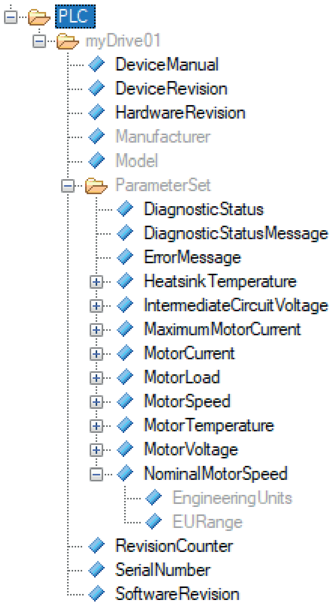
4.3.4 Custom Information Models

ibaPDA-OPC UA-Server supports the import of so-called "UA node sets". After the import, signals from the *ibaPDA* signal tree can be assigned to the tags in this node set.

Introduction

UA node sets map certain information models that are very helpful with regard to standardizing communication interfaces. A UA node set is a structured set of relevant tags designed for a specific application, such as a machine.

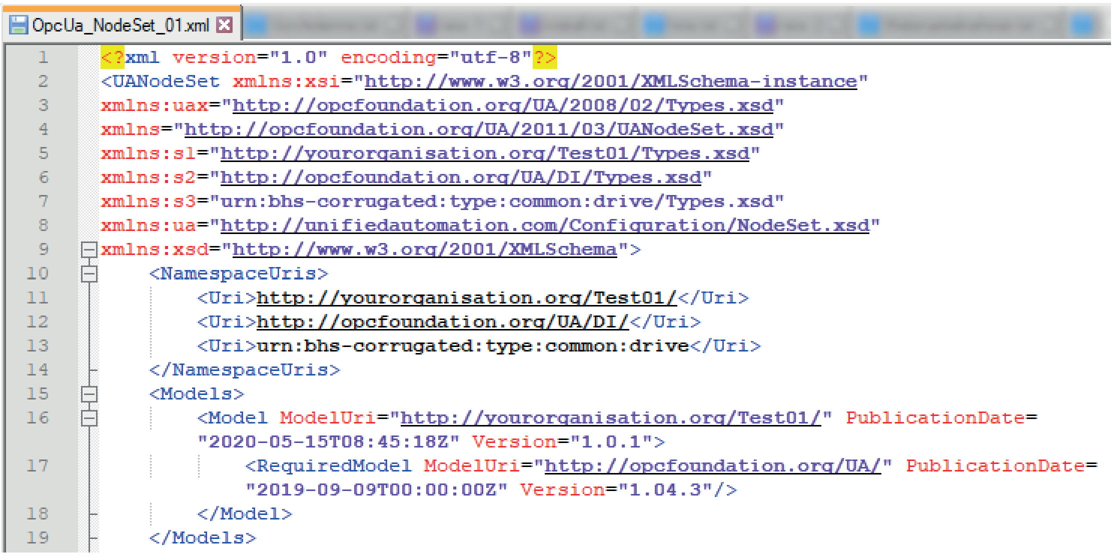
The following figure shows an example of an information model for a drive whose device data, status information and parameters are to be exchanged with a PLC.



```
PLC
  myDrive01
    DeviceManual
    DeviceRevision
    HardwareRevision
    Manufacturer
    Model
    ParameterSet
      DiagnosticStatus
      DiagnosticStatusMessage
      ErrorMessage
      HeatsinkTemperature
      IntermediateCircuitVoltage
      MaximumMotorCurrent
      MotorCurrent
      MotorLoad
      MotorSpeed
      MotorTemperature
      MotorVoltage
      NominalMotorSpeed
        EngineeringUnits
        EURange
    RevisionCounter
    SerialNumber
    SoftwareRevision
```

Special modeling tools are available for the creation of these UA node sets, such as Siemens OPC UA Modeling Editor (SiOME) or Unified Automation UaModeler. Using so-called "companion specifications", these tools allow information models to be created and saved as an XML file (node set file). This file can then be imported into ibaPDA.

The following figure shows an example of the header of a node set file.



```
<?xml version="1.0" encoding="utf-8"?>
<UANodeSet xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:uax="http://opcfoundation.org/UA/2008/02/Types.xsd"
xmlns="http://opcfoundation.org/UA/2011/03/UANodeSet.xsd"
xmlns:s1="http://yourorganisation.org/Test01/Types.xsd"
xmlns:s2="http://opcfoundation.org/UA/DI/Types.xsd"
xmlns:s3="urn:bhs-corrugated:type:common:drive/Types.xsd"
xmlns:ua="http://unifiedautomation.com/Configuration/NodeSet.xsd"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
    <NamespaceUris>
        <Uri>http://yourorganisation.org/Test01/</Uri>
        <Uri>http://opcfoundation.org/UA/DI/</Uri>
        <Uri>urn:bhs-corrugated:type:common:drive</Uri>
    </NamespaceUris>
    <Models>
        <Model ModelUri="http://yourorganisation.org/Test01/" PublicationDate=
        "2020-05-15T08:45:18Z" Version="1.0.1">
            <RequiredModel ModelUri="http://opcfoundation.org/UA/" PublicationDate=
            "2019-09-09T00:00:00Z" Version="1.04.3"/>
        </Model>
    </Models>
```

Importing and deleting a UA node set

1. Click the green cross in the toolbar above the tag directory.
2. Select the desired node set file (*.xml) and click <Open>.
3. The complete node set is then added to the tag directory as a new main branch under the ibaPDA root branch, as shown in the image above “PLC”.

With each import, a new node set is added. If several objects of the same type, such as identical drives, need to be mapped, you must perform the import several times.

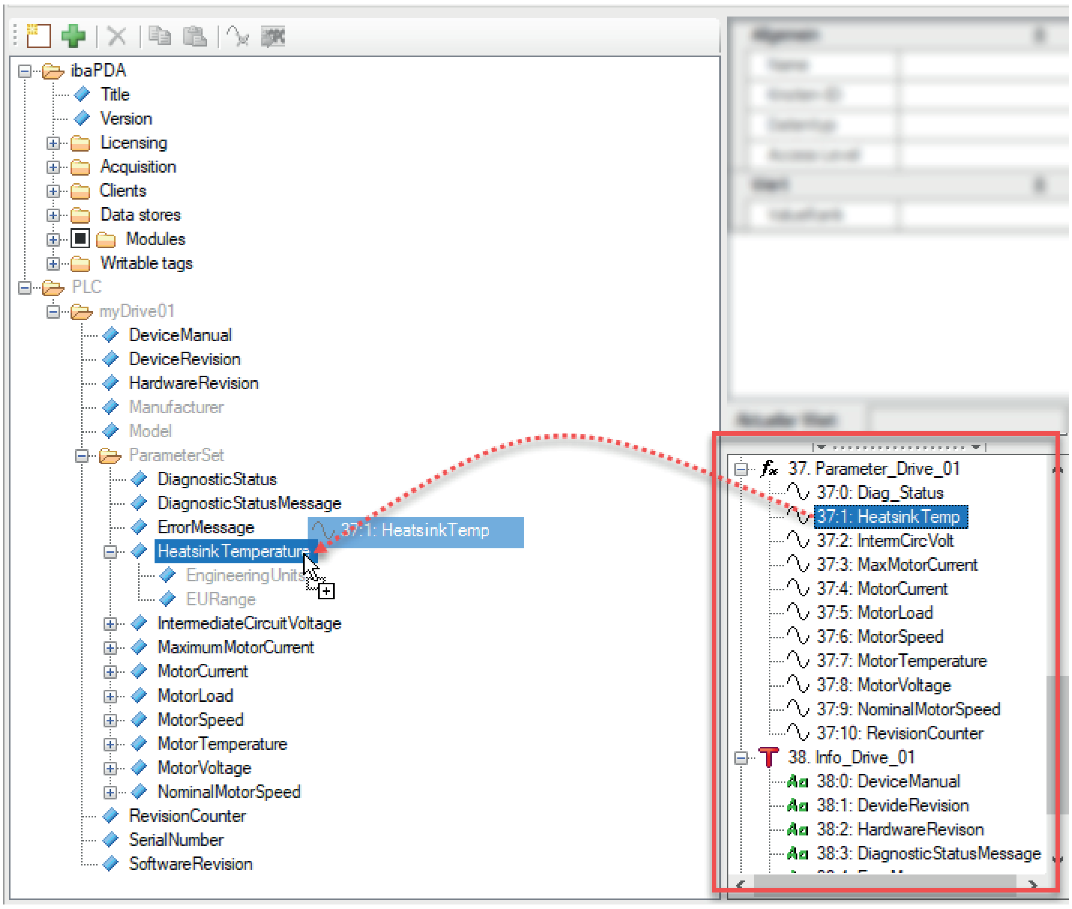
As long as there is at least one node set, the buttons for deleting node sets and removing signal shortcuts are available.

If you want to delete a node set, select the main node of the relevant node set and click on the red X.

Connecting ibaPDA signals to the node set

Imported tags that cannot be associated with signals are grayed out. These are, for example, folders or tags with data types that are not supported.

To link a signal to a tag, simply drag and drop the desired signal from the signal tree window on the right to the appropriate tag in the tag directory on the left.

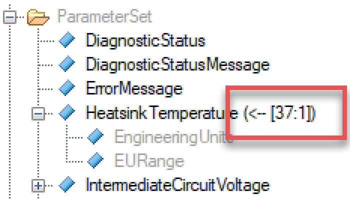


```
ibaPDA
  Title
  Version
  Licensing
  Acquisition
  Clients
  Data stores
  Modules
  Writable tags
PLC
  myDrive01
    DeviceManual
    DeviceRevision
    HardwareRevision
    Manufacturer
    Model
    ParameterSet
      DiagnosticStatus
      DiagnosticStatusMessage
      ErrorMessage
      HeatsinkTemperature        37:1: HeatsinkTemp
        EngineeringUnits
        EURange
      IntermediateCircuitVoltage
      MaximumMotorCurrent
      MotorCurrent
      MotorLoad
      MotorSpeed
      MotorTemperature
      MotorVoltage
      NominalMotorSpeed
    RevisionCounter
    SerialNumber
    SoftwareRevision
```

```
37. Parameter_Drive_01
  37:0: Diag_Status
  37:1: HeatsinkTemp
  37:2: IntermCircVolt
  37:3: MaxMotorCurrent
  37:4: MotorCurrent
  37:5: MotorLoad
  37:6: MotorSpeed
  37:7: MotorTemperature
  37:8: MotorVoltage
  37:9: NominalMotorSpeed
  37:10: RevisionCounter
38. Info_Drive_01
  38:0: DeviceManual
  38:1: DevideRevision
  38:2: HardwareRevison
  38:3: DiagnosticStatusMessage
```

In the example (see figure above), the heat sink temperature ("HeatsinkTemp") of a drive measured with *ibaPDA* is assigned to the matching tag "HeatsinkTemperature".

If a link exists, the signal ID (Module no.:Signal no.) is displayed after the tag name.



```
ParameterSet
  DiagnosticStatus
  DiagnosticStatusMessage
  ErrorMessage
  HeatsinkTemperature (<-- [37:1])
    EngineeringUnits
    EURange
  IntermediateCircuitVoltage
```

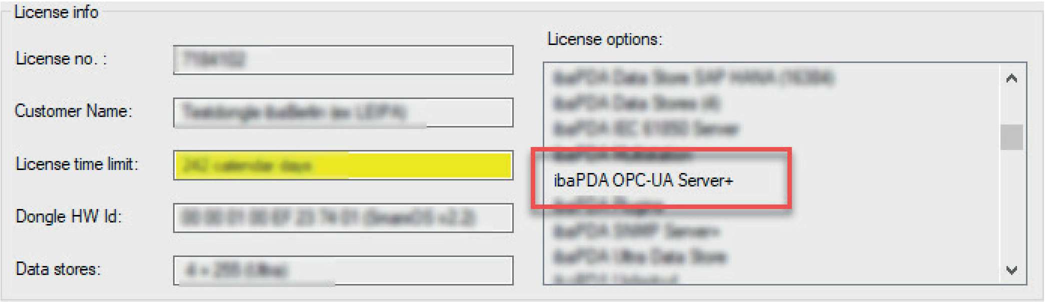
If you want to replace a previously assigned signal with another one, simply drag the new signal onto the tag.

You can remove a signal link at any time by selecting the tag and clicking the *Remove links to signals* icon button.

5 Diagnostics

5.1 License

If you cannot publish the configured signals as OPC UA variables, check whether your “ibaPDA-OPC-UA-Server+” license is detected correctly in the *ibaPDA* I/O Manager under *General – Settings -– License Info* or in the *ibaPDA* Service Status application.



License info

License no. : [illegible]

Customer Name: [illegible]

License time limit: [illegible]

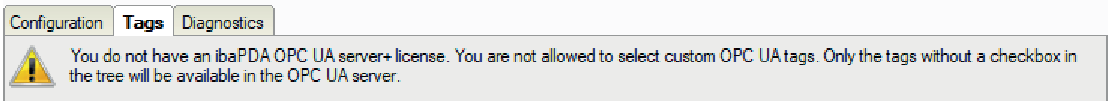
Dongle HW Id: [illegible]

Data stores: [illegible]

License options:

ibaPDA OPC-UA Server+

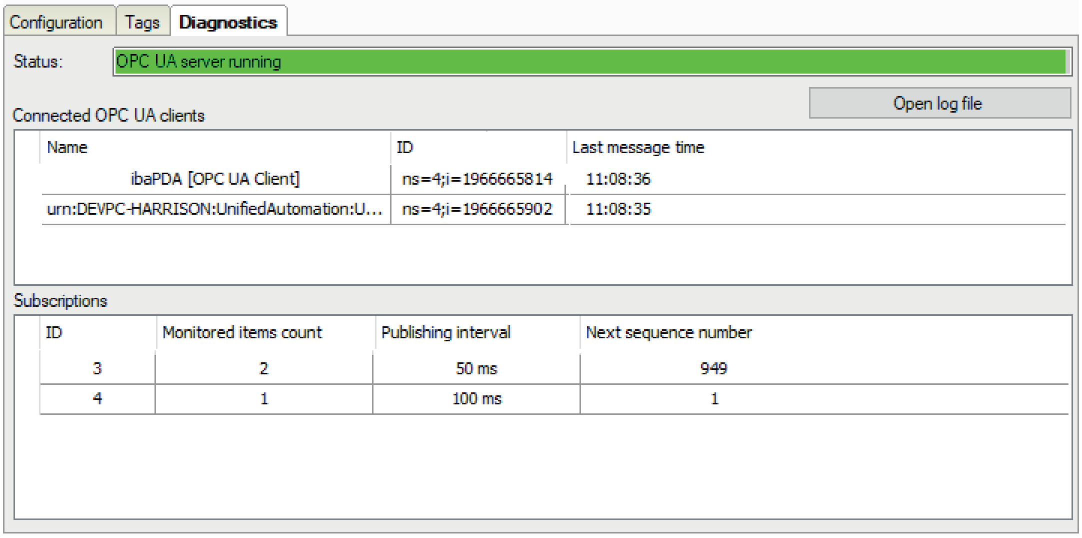
If no license is available, you will be also be notified in the I/O Manager under *General – OPC UA Server*, *Tags* tab:



You do not have an ibaPDA OPC UA server+ license. You are not allowed to select custom OPC UA tags. Only the tags without a checkbox in the tree will be available in the OPC UA server.

5.2 Diagnostics tab

The current status of the OPC UA server is displayed in the *Diagnostics* tab (I/O Manager, *General – OPC-UA server*). You will also see a list of connected OPC UA clients and subscriptions there.



Status: OPC UA server running

Connected OPC UA clients

Name	ID	Last message time
ibaPDA [OPC UA Client]	ns=4;i=1966665814	11:08:36
urn:DEVPC-HARRISON:UnifiedAutomation:U...	ns=4;i=1966665902	11:08:35

Subscriptions

ID	Monitored items count	Publishing interval	Next sequence number
3	2	50 ms	949
4	1	100 ms	1

For each connection, the name and ID of the session are displayed along with the time stamp of the most recent communication.

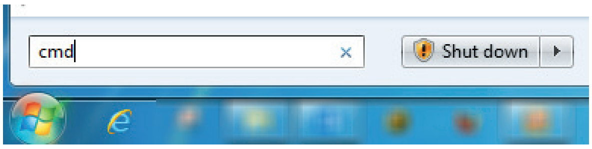
For each subscription, the subscription ID, the number of monitored tags, the publication interval and the next sequence number are displayed. The latter value is increased each time new data is sent for a particular subscription.

If you select an OPC UA client in the upper list, the subscriptions are filtered so that only subscriptions that are relevant for this client are displayed in the lower list.

5.3 Connection diagnostics with PING

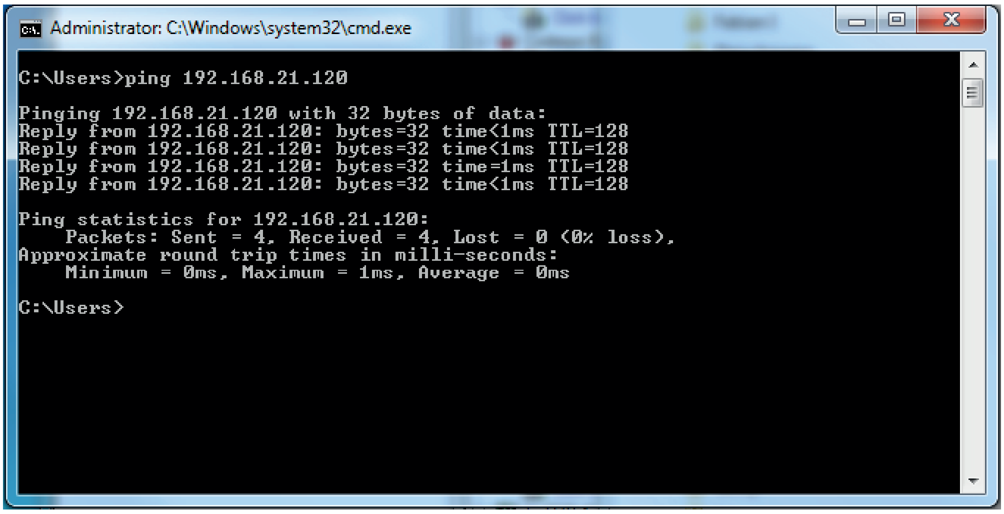
PING is a system command with which you can check if a certain communication partner can be reached in an IP network.

Open a Windows command prompt.



Enter the command “ping” followed by the IP address of the communication partner and press <ENTER>.

With an existing connection you receive several replies.



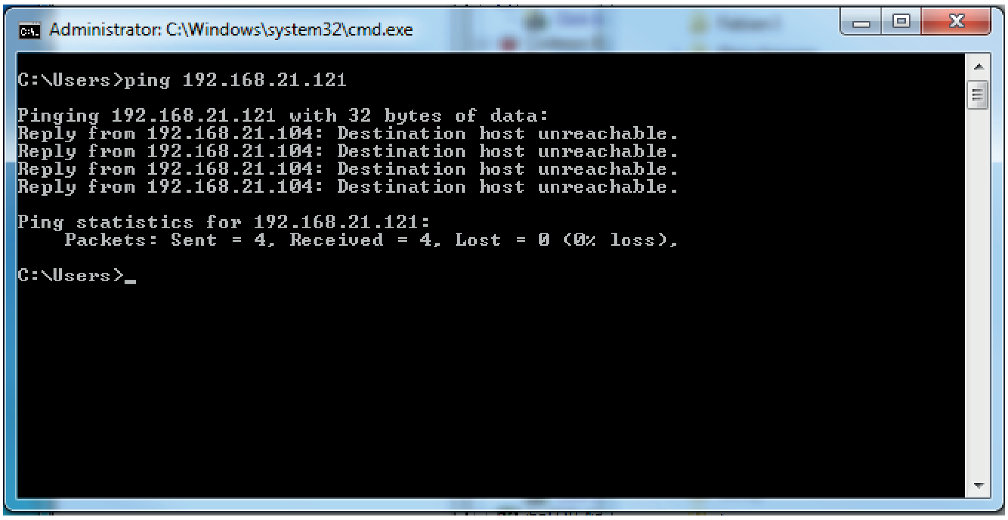
```
C:\Users>ping 192.168.21.120

Pinging 192.168.21.120 with 32 bytes of data:
Reply from 192.168.21.120: bytes=32 time<1ms TTL=128
Reply from 192.168.21.120: bytes=32 time<1ms TTL=128
Reply from 192.168.21.120: bytes=32 time=1ms TTL=128
Reply from 192.168.21.120: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.21.120:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users>
```

With no existing connection you receive error messages.



```
C:\Users>ping 192.168.21.121

Pinging 192.168.21.121 with 32 bytes of data:
Reply from 192.168.21.104: Destination host unreachable.
Reply from 192.168.21.104: Destination host unreachable.
Reply from 192.168.21.104: Destination host unreachable.
Reply from 192.168.21.104: Destination host unreachable.

Ping statistics for 192.168.21.121:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users>_
```

6 Support and contact

Support

Phone:	+49 911 97282-14
Fax:	+49 911 97282-33
Email:	support@iba-ag.com

Note

If you need support for software products, please state the license number or the CodeMeter container number (WIBU dongle). For hardware products, please have the serial number of the device ready.

Contact

Headquarters

iba AG
Koenigswarterstrasse 44
90762 Fuerth
Germany

Phone:	+49 911 97282-0
Fax:	+49 911 97282-33
Email:	iba@iba-ag.com

Mailing address

iba AG
Postbox 1828
D-90708 Fuerth, Germany

Delivery address

iba AG
Gebhardtstrasse 10
90762 Fuerth, Germany

Regional and Worldwide

For contact data of your regional iba office or representative please refer to our web site

www.iba-ag.com.