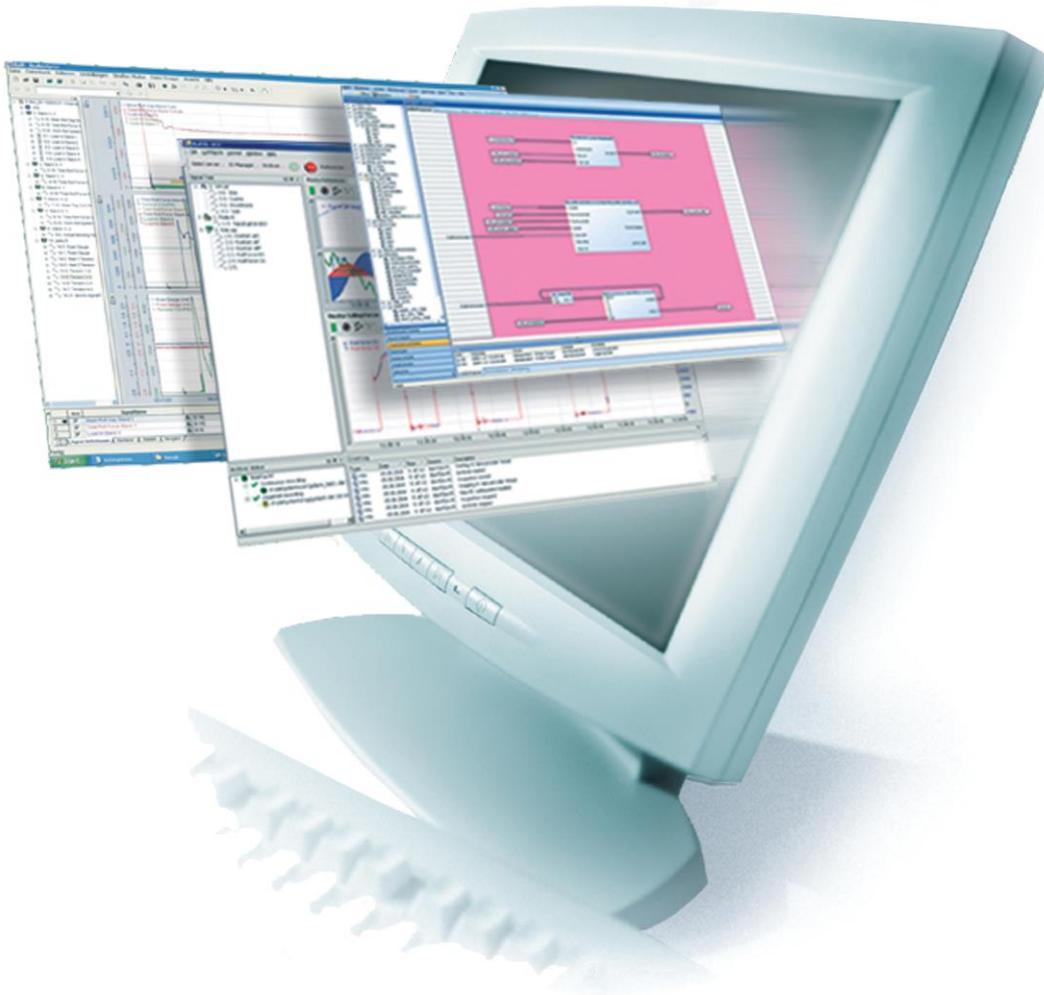


OPC Connection

Security and DCOM Settings



Manual

Issue 2.0.1

Measurement and Automation Systems



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

This manual must not be circulated or copied, or its contents utilized and disseminated, without our express written permission. Any breach or infringement of this provision will result in liability for damages.

©iba AG 2017, All Rights Reserved

The content of this publication has been checked for compliance with the described hardware and software. Nevertheless, deviations cannot be excluded completely so that the full compliance is not guaranteed. However, the information in this publication is updated regularly. Required corrections are contained in the following issues or can be downloaded on the Internet.

The current version is available for download on our web site <http://www.iba-ag.com>.

Issue	Date	Revision	Author	Version SW
2.0.1	07/11/2017	Minor corrections	St	2.0
2.0	06.12.2016	updated, Win2000 removed, Win7-10 new	Ko/KaFe	2.0

Windows® is a label and registered trademark of the Microsoft Corporation. Other product and company names mentioned in this manual can be labels or registered trademarks of the corresponding owners.

Table of Contents

1	About this manual	2
1.1	Target group	2
1.2	Notations	2
1.3	Used symbols	3
2	System requirements	4
3	Introduction	5
3.1	General.....	5
3.1.1	OPC.....	5
3.1.2	OPC and iba products	5
3.1.3	DCOM	6
3.1.4	Firewall	6
3.1.5	Local security policy.....	6
4	Configuration	7
4.1	Part A: Configuration on the OPC server side	7
4.1.1	Step A1: Preparation.....	7
4.1.2	Step A2: Configuring the Windows firewall.....	8
4.1.3	Step A3: Configuring the local security settings	11
4.1.4	Step A4: Open the DCOM configuration	13
4.1.5	Step A5: DCOM settings for OpcEnum	14
4.1.6	Step A6: DCOM settings for OPC server	15
4.1.7	Step A7: Reboot the OPC server PC	16
4.2	Part B: Configuration of OPC client side	17
4.2.1	Step B1: Configuring the Windows firewall.....	17
4.2.2	Step B2: Configuring the local security settings	18
4.2.3	Step B3: User Accounts for OPC Connection	19
4.2.4	Step B4: Reboot the OPC Client PC	19
4.3	Part C: Example of an OPC connection	20
4.3.1	Step C1: Selecting the OPC server.....	20
4.3.2	Step C2: Connecting the OPC server	21
4.3.3	Step C3: Adding signals.....	22
5	Appendix	23
5.1	Specialties for ibaPDA	23
5.2	Specialties for DriveOPC (ABB).....	24
5.3	Troubleshooting	25
5.3.1	Error: No OPC server found.....	26
5.3.2	Error on establishing the connection	28
5.3.3	Error: Client does not receive data.....	30
6	Support and contact	32

1 About this manual

This document describes a few from many possible configurations that are necessary to establish a connection between OPC client and OPC server within a network.

1.1 Target group

This manual addresses in particular the qualified professionals who are familiar with handling electrical and electronic modules as well as communication and measurement technology. A person is regarded as professional if he/she is capable of assessing safety and recognizing possible consequences and risks on the basis of his/her specialist training, knowledge and experience and knowledge of the standard regulations.

1.2 Notations

In this manual, the following notations are used:

Action	Notation
Menu command	Menu <i>Logic diagram</i>
Calling the menu command	<i>Step 1 – Step 2 – Step 3 – Step x</i> Example: Select the menu <i>Logic diagram - Add - New function block</i> .
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:

- From an electric shock!
 - Due to the improper handling of software products which are coupled to input and output procedures with control function!
-

 WARNING

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

 CAUTION

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



Note

A note specifies special requirements or actions to be observed.



Important note

Note if some special features must be observed, for example exceptions from the rule.



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.



Example

Configuration and application examples for a better understanding

2 System requirements

See the system requirements of the OPC server and OPC client applications.

For instance, the *ibaPDA* application requires the following components for the use of the OPC Connection data interface.

Operating system	Framework
Windows XP (x86)	SP3 is required, .NET framework 4.0
Windows 2003 Server (x86)	SP2 with hotfix KB938397 is required, .NET framework 4.0
Windows Vista (x86)	.NET Framework 4.5 required when using OPC interfaces
Windows 2008 Server (x86)	
Windows 7 (x86/x64)	
Windows 2008 Server R2 (x64)	
Windows 8 (x86/x64)	.NET Framework 4.5 integrated in OS When using OPC interfaces activate additional Windows-Feature “.NET Framework 3.5 (includes .NET 2.0 and 3.0)”
Windows 2012 Server (x64)	
Windows 8.1 (x86/x64)	
Windows 2012 Server R2 (x64)	.NET Framework 4.6 integrated in OS When using OPC interfaces activate additional Windows-Feature “.NET Framework 3.5 (includes .NET 2.0 and 3.0)”
Windows 10 (x86/x64)	

See also the *ibaPDA* version compatibility matrix.



Note

It is recommended carrying out the TCP/IP communication on a separate network segment to exclude a mutual influence by other network components.



Important note

You need system administrator rights to change the DCOM settings and security policies on the OPC client PC and OPC server PC.

3 Introduction

This document describes a few from many possible configurations that are necessary to establish a connection between OPC client and OPC server within a network.

There are several ways to achieve this goal. The configurations described in this document were tested and lead to satisfying results.

In case the settings in this document do not work as desired or if you find other settings that are simpler, please contact us.

We are thankful for all hints considering errors in this document.

3.1 General

3.1.1 OPC

OPC stands for "**O**LE for **P**rocess **C**ontrol". This is a standard software interface, which makes it possible that applications of different manufacturers exchange data with one another. OPC is used wherever sensors, control systems and HMIs of different manufacturers shall create a flexible network.

For communication between the different applications, the OPC uses Microsoft's DCOM technology. The transparent DCOM shows whether the data comes from own address space, another process or another computer connected by TCP/IP.

OPC is based on the client/server principle. The process data is generated on the server side (usually a control system) and is made available for the clients.

More information about OPC is found under <http://www.opcfoundation.org/> and in the manuals of *ibaLogic* and *ibaPDA*.

3.1.2 OPC and iba products

The iba-applications *ibaLogic* and *ibaPDA* have OPC-interfaces.

In *ibaLogic* there is an OPC server (specification OPC Data Access 2.0) integrated, which is automatically installed and activated with the start of *ibaLogic*.

In *ibaPDA* there are both an OPC client and an OPC server integrated (of specification DA 1.0 und DA 2.0). The *ibaPDA* OPC server will be activated automatically and makes all configured signals available. Additionally, *ibaPDA* offers an OPC server module that enables an OPC client to send data to *ibaPDA*.



Note

The OPC connection has a non-deterministic data transfer and is therefore not qualified for real-time measurement, although it can be used for slower processes (e.g. temperature changes) or accompanied quality data (e.g. charge numbers, Technostrings).

3.1.3 DCOM

DCOM (Distributed Component Object Model) is a protocol defined by Microsoft, for the communication of program components across networks.

The great potency of this functionality bears the problem. As DCOM is activated as a part of the OS, almost every Internet user can get into contact with a DCOM object, which of course is a security risk.

A solution for this problem was Windows XP. Especially Service Pack 2 improved the security: The DCOM infrastructure now additionally provides access control mechanisms.

To enable data transfer over OPC, permitted accesses have to be specified exactly.

3.1.4 Firewall

Additionally to the DCOM security policy, the Windows XP service pack 2 also comes with a firewall which is activated by default. To enable the data transfer through the firewall we have to configure some exceptions in the firewall.

3.1.5 Local security policy

In the local security policy of Windows, a few predefined options have to be adjusted.

4 Configuration

For configuring the connection, you need administration rights for the OPC server PC and the OPC client PC.

Overview:

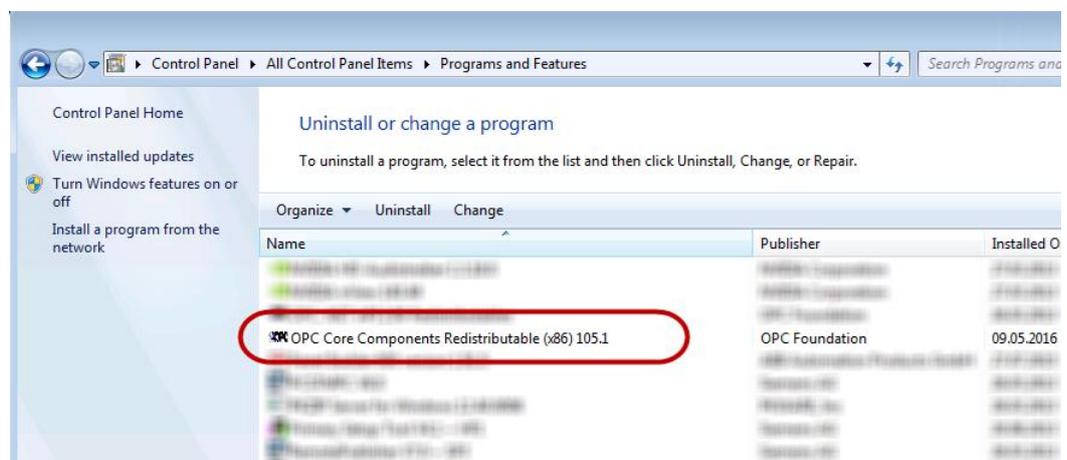
- Part A: Configuration on the OPC server side
- Part B: Configuration on OPC client side
- Part C: Example of an OPC connection

4.1 Part A: Configuration on the OPC server side

4.1.1 Step A1: Preparation

- Check whether the "OPC Core Components" are installed. These are necessary for using the OPC-browser service OpcEnum

Control Panel - Programs and Features



Note

Normally, the "OPC Core Components" are installed automatically with OPC products. Thus, they are installed with the iba products *ibaPDA* and *ibaLogic*.

4.1.2 Step A2: Configuring the Windows firewall

Possibly, the OPC server and client software configures the firewall automatically on their installation. In this case, you do not have to make any changes.

Please check the entries in the firewall rules list.

The following programs and TCP ports must be set enabled in the firewall:

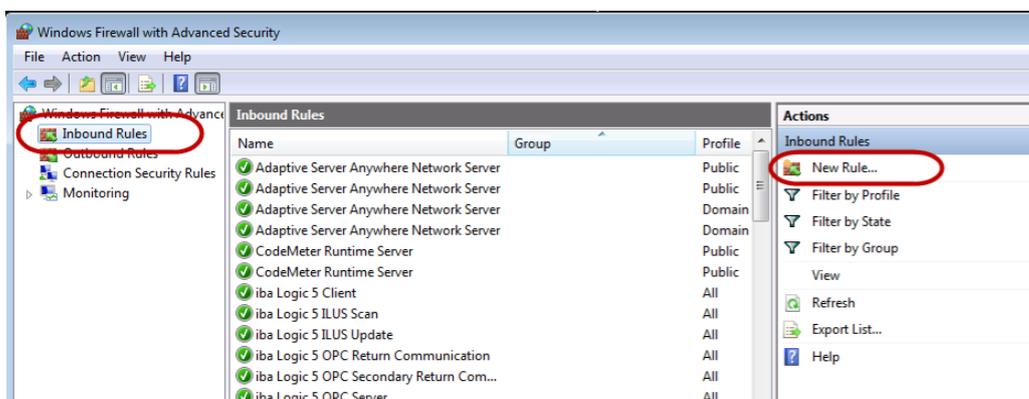
- File and Printer sharing (TCP Ports 139, 445, UDP Ports 137, 138)
- DCOM Port (TCP Port 135)
- Management Console (...WindowsSystem32mmc.exe)
- OpcEnum (on x86:...\\Windows\\System32\\OpcEnum.exe, on x64:...\\Windows\\SysWOW64\\OpcEnum.exe)
- "OPC-Server" (e. g. ...\\ibaLogic.exe)

If necessary, add the missing programs or port.

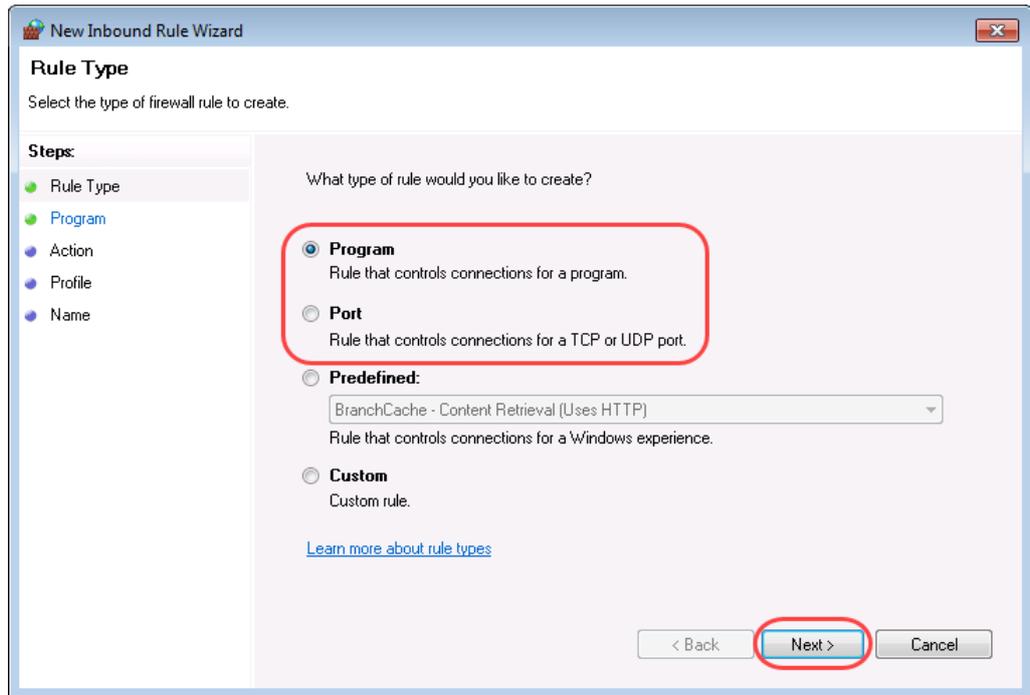
Configuring the firewall in Windows 7, 8, 10:

- Open firewall settings:

Control Panel - Windows Firewall - Advanced settings



- Select "Inbound Rules" and check whether the list includes the programs and ports mentioned above.
- If not, click on "New Rule" to open the Inbound Rule Wizard, select the type "Program" or "Port" and click on <Next>

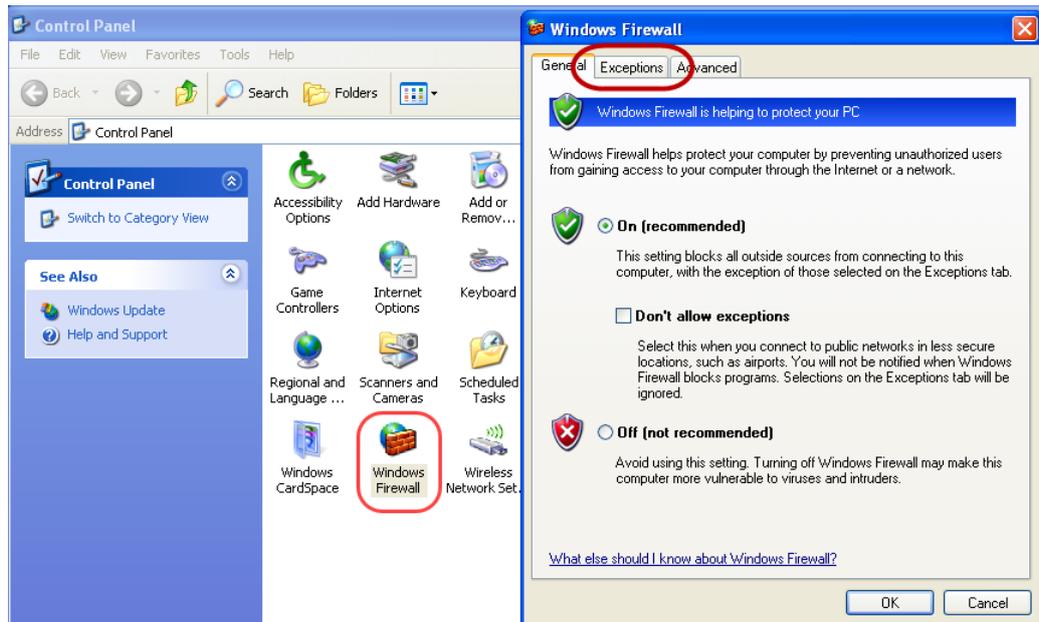


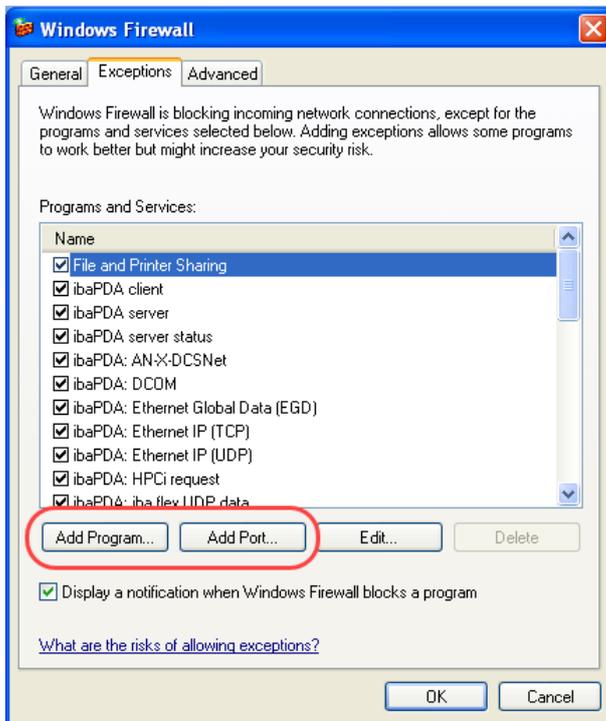
- ❑ Enter the program path resp. the TCP port number and allow the connection for Domain, Private and Public.

Configuring the firewall in Windows XP:

- ❑ Open firewall exceptions:

Control Panel - Windows Firewall - Exceptions





- Check whether the list includes the programs and ports mentioned above.
- If these programs and ports are not included, add them by clicking on the buttons <Add Program...> and <Add Port...>.



Tip

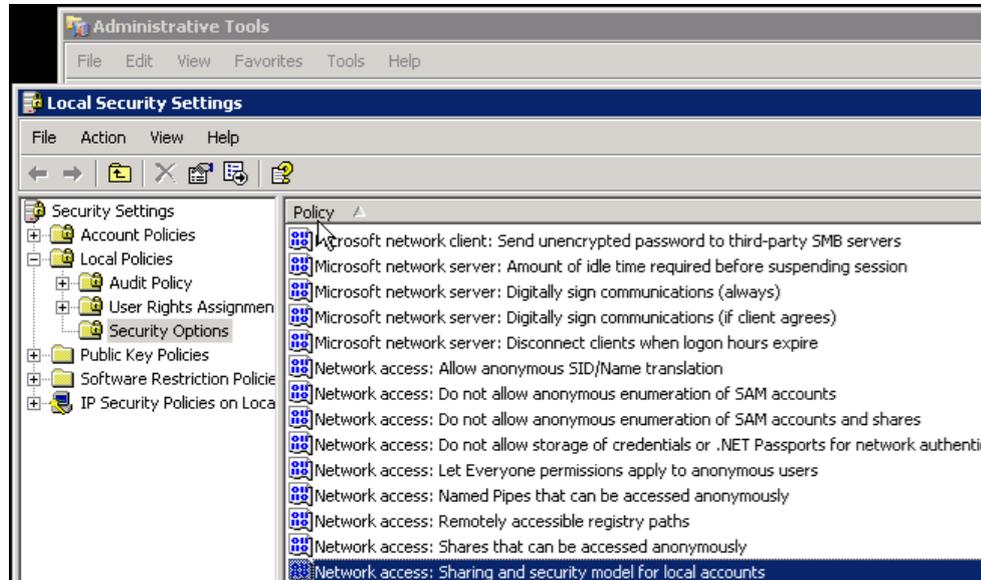
If you have made these entries and still do not have access (e.g. error code 0x800706BA) switch off the firewall completely and try it again. In case you have access now, the reason might be a blocked dynamic TCP port. You can figure it out by using the access protocols of the firewall. Ask your system administrator.

4.1.3 Step A3: Configuring the local security settings

- ❑ Open the "Local Security Settings":

Control Panel - Administrative Tools - Local Security Settings - Local Policies - Security Options

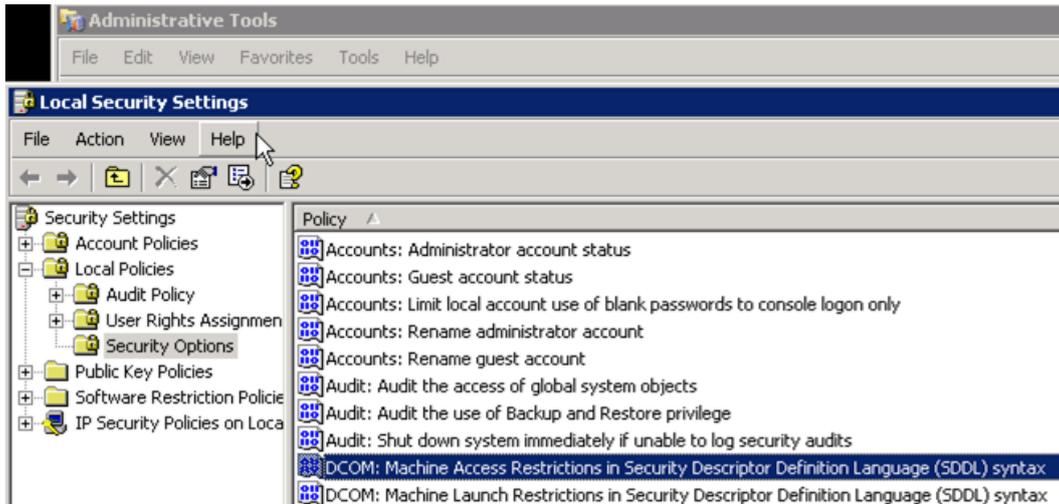
- ❑ Select the "Security Options"
"Network access: Sharing and security model for local accounts"



- ❑ Set the option to:
"Classic – local users authenticate as themselves":



- ❑ Select the "Security Options"
"DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax"



- Select with a right click "Properties", click on <Edit Security> to set the following permissions:

Security Limits / Groups	ANONYMOUS LOGON	Everyone
Local access	allow	allow
Remote access	allow	allow

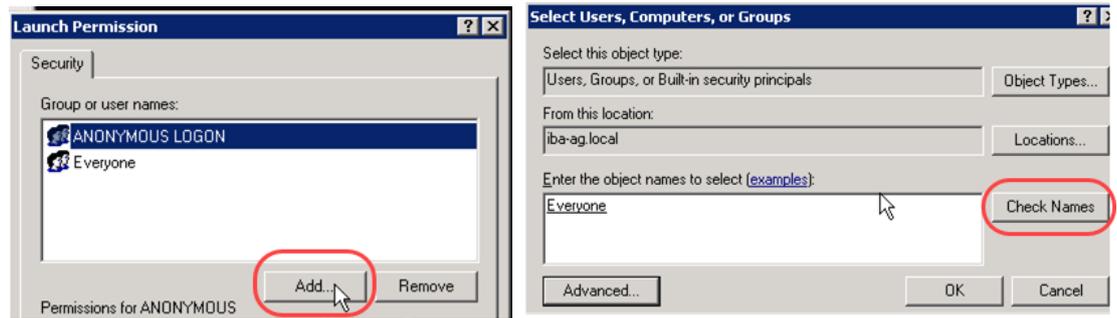
- ❑ Select the "Security Options"
"DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax"
- ❑ Select with a right click "Properties", click on <Edit Security> to set the following permissions:

Security Limits / Groups	ANONYMOUS LOGON	Everyone
Local Launch	allow	allow
Remote Launch	allow	allow
Local Activation	allow	allow
Remote Activation	allow	allow



Note

If you cannot find "ANONYMOUS LOGON" or "Everyone" in the Group or users names field, they have to be added (button):

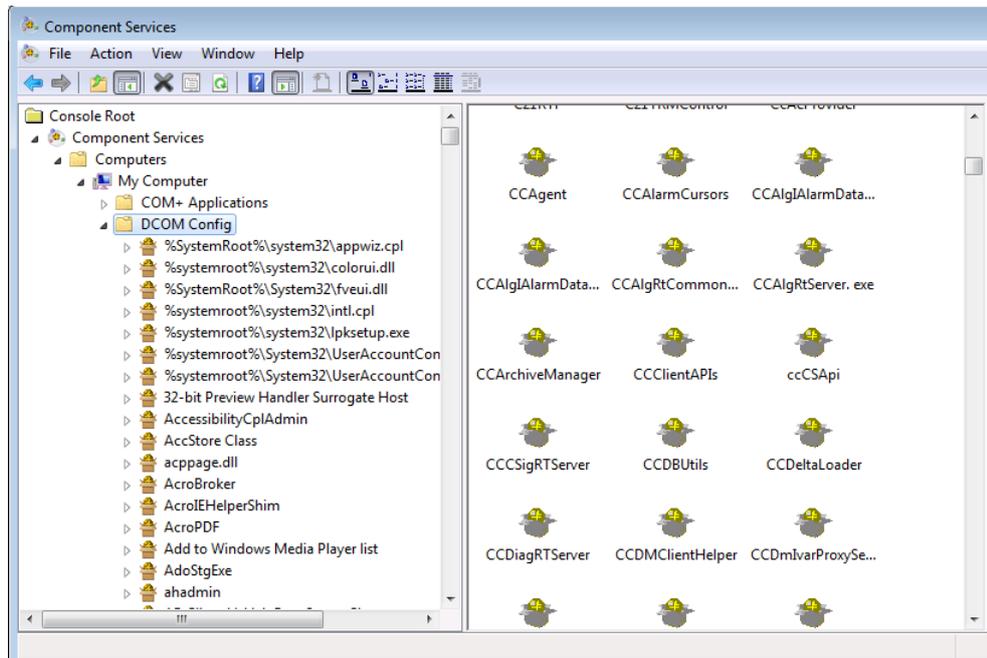


4.1.4 Step A4: Open the DCOM configuration

- ❑ Start the configuration program

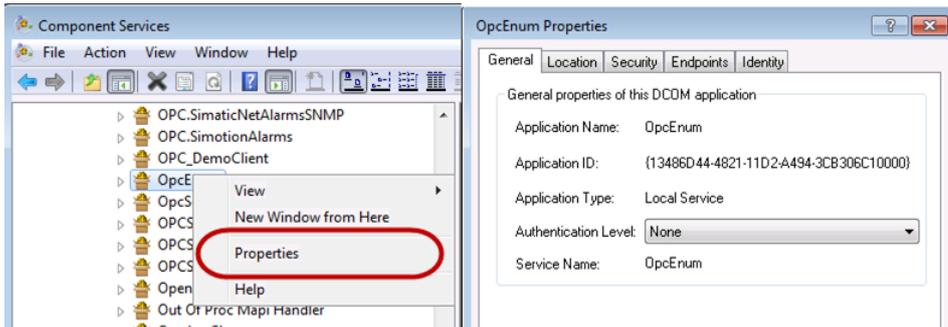
Control Panel - Administrative Tools - Component Services.

- ❑ Open *Component Services - Computers - My Computer - DCOM Config*. The DCOM objects are shown in the left tree view or in the right window. With a right-click on the object, you can see and change its properties.



4.1.5 Step A5: DCOM settings for OpcEnum

- ❑ Select the object OpcEnum in the DCOM objects and choose the properties with the right mouse button.



- ❑ Set the following properties:

- Tab *General* Authentication Level: *none*
- Tab *Location* Run Application on this computer
- Tab *Security* Launch and Activation Permissions: *Customize, Edit:*

Security Limits / Groups	ANONYMOUS LOGON	Everyone
Local Launch	allow	allow
Remote Launch	allow	allow
Local Activation	allow	allow
Remote Activation	allow	allow

Access Permission:
Customize, Edit

Security Limits / Groups	ANONYMOUS LOGON	Everyone
Local Launch	allow	allow
Remote Launch	allow	allow

Configuration Permission: *default*

- Tab *Endpoints* no change
- Tab *Identity* The system account (services only)

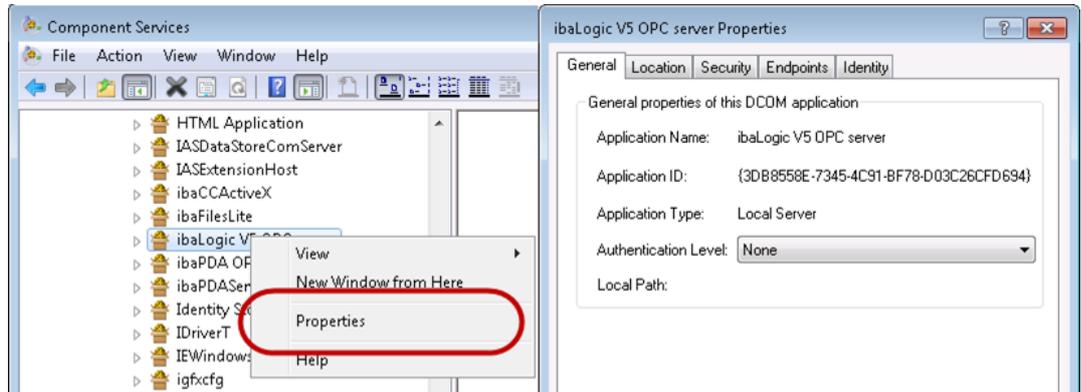


Note

If you cannot find "ANONYMOUS LOGON" or "Everyone" in the Group or users names field, they have to be added, see *Step A4: Open the DCOM configuration*, page 13.

4.1.6 Step A6: DCOM settings for OPC server

- ❑ Search the DCOM object for the OPC server, see the table in *Troubleshooting*, page 25.
- ❑ Select the DCOM object of the OPC server and choose the properties with the right mouse button.



- ❑ Set the following properties:

- Tab *General* Authentication Level: *none*
- Tab *Location* *Run Application on this computer*
- Tab *Security* Launch and Activation Permissions:
Customize, Edit:

Security Limits / Groups	ANONYMOUS LOGON	Everyone
Local Launch	allow	allow
Remote Launch	allow	allow
Local Activation	allow	allow
Remote Activation	allow	allow

Access Permissions:
Customize, Edit:

Security Limits / Groups	ANONYMOUS LOGON	Everyone
Local Launch	allow	allow
Remote Launch	allow	allow

Configuration Permission: *default*

- Tab *Endpoints* no change
- Tab *Identity* *"The interactive user"*
(if possible, e. g. *ibaLogic*) or
"The system account (services only)" (e.g. *ibaPDA*).

**Note**

If you cannot find "ANONYMOUS LOGON" or "Everyone" in the Group or users names field, they have to be added, see *Step A4: Open the DCOM configuration*, page 13.

4.1.7 Step A7: Reboot the OPC server PC

4.2 Part B: Configuration of OPC client side

4.2.1 Step B1: Configuring the Windows firewall

Usually, the OPC server and client software configures the firewall automatically on their installation. Thus, you do not have to make changes.

Please check the entries in the firewall.

The following ports and programs must be entered and be active in the list:

- File and Printer sharing (TCP-Ports 139, 445, UDP-Ports 137, 138)
- DCOM Port (TCP Port 135)
- Management Console (...WindowsSystem32mmc.exe)
- "OPC-Client" (e.g. ibaPda.exe)

Add missing ports and programs as needed.

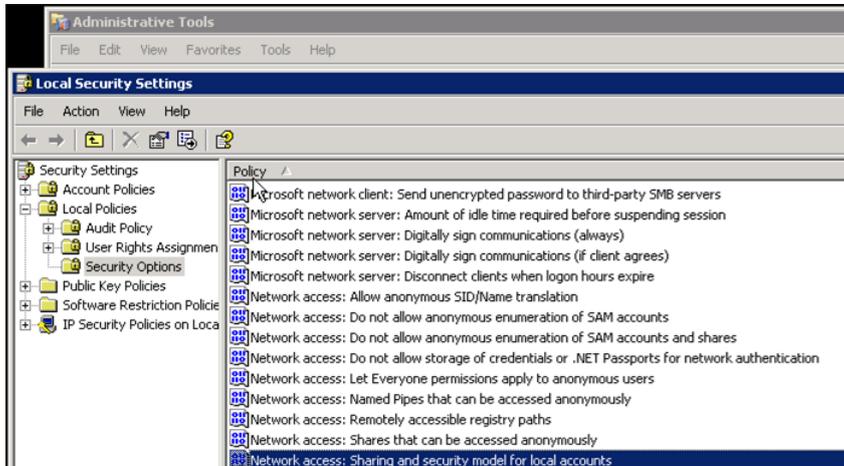
Proceed as described in *Step A2: Configuring the Windows firewall*, page 8.

4.2.2 Step B2: Configuring the local security settings

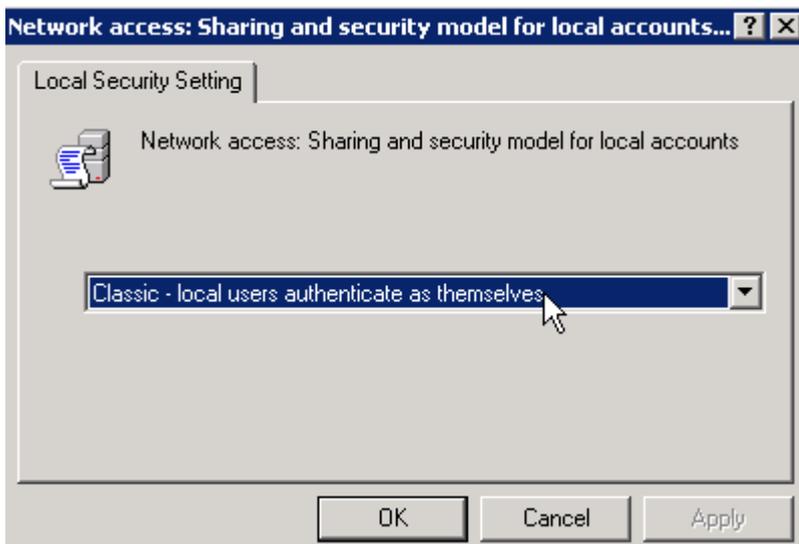
- ❑ Open the "Local Security Settings:

Control Panel - Administrative Tools - Local Security Settings- Local Policies - Security Options

- ❑ Select the "Security Options"
"Network access: Sharing and security model for local accounts"



- ❑ Set the option to:
"Classic - local user authenticate as themselves".



4.2.3 Step B3: User Accounts for OPC Connection

The account of the OPC client must be known by the OPC server, therefore you need to do the following settings, dependent on the network configuration.

See also *Specialties for ibaPDA*, page 23.

Case 1: Both PCs, OPC Server and OPC Client are in the same Domain:

- All services and programs have to run with accounts registered in the domain.

Case 2: Both, the OPC Server PC and the OPC Client PC are in Workgroups.

- Both are to be within the same Workgroup:
If not, change Network settings on the OPC client or OPC server PC:
Computer - Properties - Computer name, domain, and workgroup settings - Change settings
- Both, the OPC server and the OPC client have to run with the same user account and password.
The password must not be empty!

If not, you have to create a local user account on the **OPC client PC** with the same properties as the account of the OPC server. Both, the OPC client and the OPC server must have the same rights (Administrator!), the same user name and the same password.

Alternatively:

On the **OPC server PC**, create an user account with the same properties as the OPC client uses.

It is not necessary to log on the OPC server with this account. It is enough when it exists.

Case 3: OPC Server in a Workgroup, OPC Client in a Domain:

- On the **OPC server PC**, create the account with that the OPC client runs in the domain as local user account.
It is not necessary to log on the OPC server with this account. It is enough when it exists.

Case 4: OPC Server in a Domain, OPC Client in a Workgroup

- Connection is not possible.

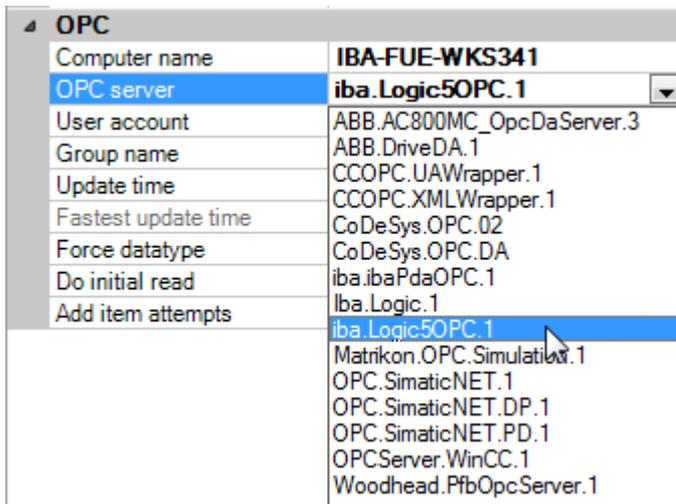
4.2.4 Step B4: Reboot the OPC Client PC

4.3 Part C: Example of an OPC connection

"*ibaPDA* OPC client and *ibaLogic V5* OPC server"

4.3.1 Step C1: Selecting the OPC Server

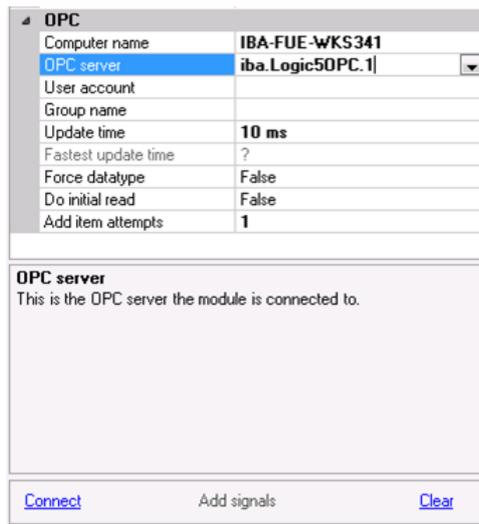
- ❑ Start the OPC client *ibaPDA*, open the I/O manager and add an OPC client module.
- ❑ Enter the computer name of the OPC server PC or its IP address or select it with the network browser.
After that, all available OPC servers are displayed and you can select one of them. Normally, it is not necessary to enter an user account and a group name.



- ❑ If you do not see any OPC server in the box, then a conflict with the security policies exists. See *Error: No OPC server found*, page 26

4.3.2 Step C2: Connecting the OPC Server

- ❑ After selecting the OPC server click on the hyperlink "Connect".



The screenshot shows a dialog box titled "OPC" with the following fields and values:

Computer name	IBA-FUE-WKS341
OPC server	iba.Logic50PC.1
User account	
Group name	
Update time	10 ms
Fastest update time	?
Force datatype	False
Do initial read	False
Add item attempts	1

Below the table is a section titled "OPC server" with the text: "This is the OPC server the module is connected to."

At the bottom of the dialog are three buttons: "Connect", "Add signals", and "Clear".

- ❑ After the connection is established successfully, the link "Connect" changes to "Disconnect" and the Link "Add signals" becomes activated.



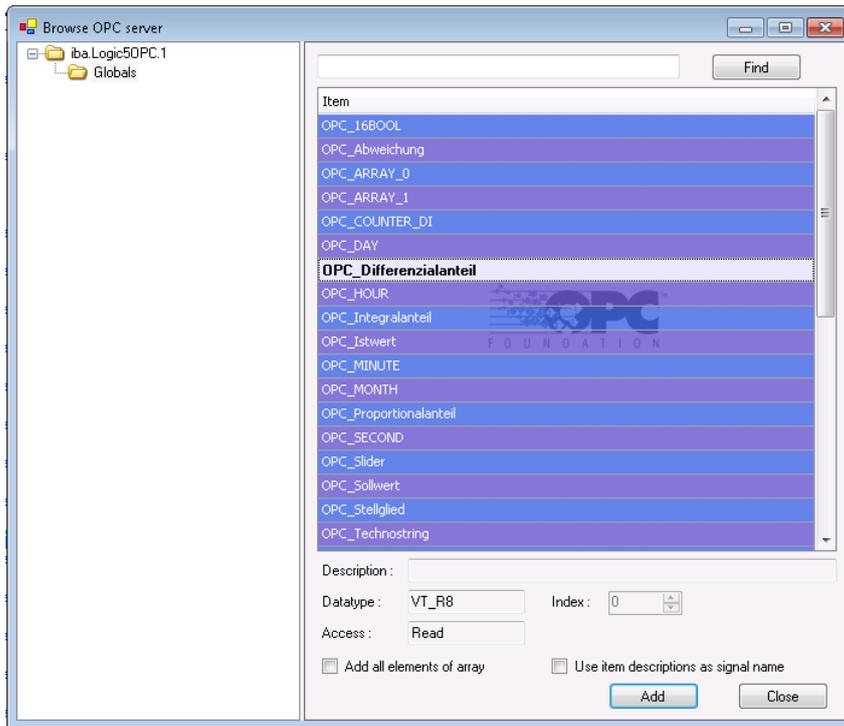
The screenshot shows the same dialog box as above, but with the following changes:

- The "Connect" button is now "Disconnect".
- The "Add signals" button is now activated (highlighted).
- The "Clear" button remains the same.

- ❑ When the connection fails, an error message appears. See *Error on establishing the connection*, page 28.

4.3.3 Step C3: Adding signals

- ❑ The OPC item browser will be started by clicking the "Add Signals" link. All available items are displayed.



- ❑ If you do not find any OPC items in the OPC server's item list, see the section *Error on establishing the connection*, page 28
- ❑ With a double click or with the button <Add>, the marked item is entered into the table of analog or digital signals. As long as the connection is established, you can see the actual values of the items in the item list.

OPC client module (1)						
General Analog Digital						
Name	Item ID	Unit	Gain	Offset	A...	Actual
0	Globals.OPC_Differenzialanteil			1	0	16,0232
1	Globals.OPC_Integralanteil			1	0	12,6534
2	Globals.OPC_Proportionalanteil			1	0	52,0095
3	Globals.OPC_Sollwert			1	0	430,84
4	Globals.OPC_Stellglied			1	0	80,6861
*						

- ❑ If you do not see the actual values, the OPC server cannot access the OPC client (error on callback), see *Error: Client does not receive data*, page 30.

5 Appendix

5.1 Specialties for ibaPDA

The *ibaPDA* service runs with the system account by default.

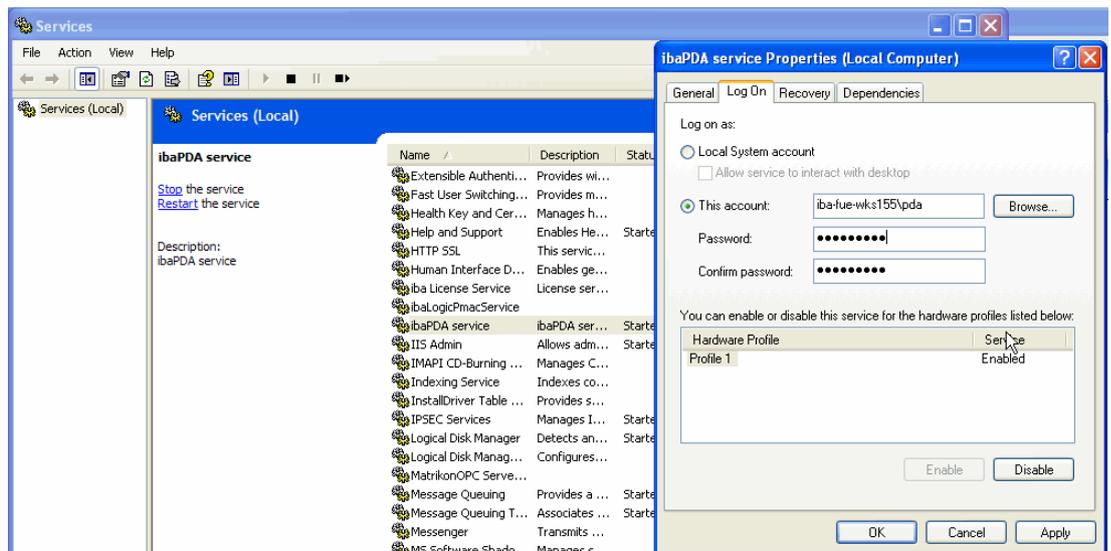
When using *ibaPDA* as OPC server or client, the *ibaPDA* service must run under the same user account that is used by the OPC server.

Perform the following steps to log on *ibaPDA* with a local user account:

- ❑ Open the Service manager:

Control Panel - Administrative Tools - Services

- ❑ Select "ibaPDA service" and open the properties (double click)
- ❑ Activate the option "This account" on the *Log On* tab and enter the defined account and the password.



- ❑ Restart the "ibaPDA service".



Important note

Also the domain is part of the user account, e. g. "Domain\User".
In case you are not logged on to a domain, please use "PC name\User" or ".\User".



Note

The user account of the OPC partner must be known by *ibaPDA*. That means, you must create a local user account on the *ibaPDA* PC if required. This local account needs to have the same properties as the account of the OPC partner.

5.2 Specialties for DriveOPC (ABB)

Beginning with *ibaPDA* version 6.10.0, the *ibaPDA* OPC client can communicate with the service tool DriveWindow (Version V2.01 and higher) via the OPC server DriveOPC Version 2.02.

With the standard installation of DriveWindow, the OPC server is installed as "in-process server". The *ibaPDA* client **cannot** be connected in this mode.

You must stop the DriveOPC Server and reinstall it as "local server".

Proceed as follows:

1. Stop "In-process server":

The server DLL "smp.dll" is normally located under "C:\Program Files\Common Files\DriveWare\DriveOPC".

Stop the server with this command:

```
Regsvr32 -  
u "C:\Program Files\Common Files\DriveWare\DriveOPC\SMP.DLL"
```

2. Start "Local server":

The server-exe "smp.exe" is normally located under "C:\Program Files\Common Files\DriveWare\DriveOPC".

Start the "Local Server" with this command:

```
"C:\Program Files\Common Files\DriveWare\DriveOPC\SMP.EXE" -  
RegServer
```

The server is found in the DCOM configuration under the name "DriveOPC". You can find the OPC server in the OPC browser under the name "ABB.SMP.1".

5.3 Troubleshooting

We recommend the following procedure:

- 1 Reboot the PC, after having performed all described settings.
- 2 Pay attention to all error messages from OPC client and OPC server, while connecting to the OPC server.
- 3 You can find additional error messages in the windows event viewer (Control panel Administrative Tools Event Viewer System) of the OPC client and OPC server PC



Note

The CLSID numbers you find in event messages represent the following programs (examples):

CLSID	Application	OPC server name	DCOM object name
{B03978E3-6BF7-4152-B1BA-0D890A87B474}	ABB OPC Server DriveDA	ABB.DriveDA.1	DriveDA
{68AEC2C4-93CD-11D1-94E1-0020AFC84400}	ABB OPC Server AC800M	ABB.AC800MC_OpcDa Server.3	OPC Server for AC 800M
{4C68190E-91E0-11D3-8D47-0060084A056F}	ibaLogic V3 OPC Server	iba.Logic.1	OPC ibaLogic Data Access Server
{35540D3D-CB96-4EDA-A556-A676EA29D4AD}	ibaLogic V4 OPC Server	iba.Logic4OPC.1	ibaLogic V4 OPC Server
{3DB8558E-7345-4C91-BF78-D03C26CFD694}	ibaLogic V5 OPC Server	iba.Logic5OPC.1	ibaLogic V5 OPC Server
{66122DF4-1F41-421A-BE1D-4E4466C551D4}	ibaPDA OPC Server	iba.ibaPdaOPC.1	ibaPDA OPC Server
{F8582CF2-88FB-11D0-B850-00C0F0104305}	Matrikon OPC Server	Matrikon.OPC.Simulation.1	MatrikonOPC Server for ...
{13486D44-4821-11D2-A494-3CB306C10000}	OpcEnum	OPC.ServerList.1	OpcEnum
{B6EACB30-42D5-11D0-9517-0020AFAA4B3C}	SIMATIC S7 OPC Server	OPC.SimaticNET.1	OPC.SimaticNET
{75D00BBB-DDA5-11D1-B944-9E614D000000}	WinCC OPC Server	OPCServer.WinCC.1	OPCServer.WinCC

5.3.1 Error: No OPC server found

No.	Error messages client side	Event messages server side	Reasons and remedy
1.1	Error messages OPC client: none Event messages DCOM: none	none	<ul style="list-style-type: none"> ▪ Invalid user account. Remedy: Enter a valid user account for the connection, <i>Step B3: User Accounts for OPC Connection</i>, page 19 ▪ When connecting via a workgroup, the network access is not released in the local security settings Remedy: Change the local security settings, see <i>Step A3: Configuring the local security settings</i>, page 11 and <i>Step B2: Configuring the local security settings</i>, page 18 ▪ On OPC server side, the service OpcEnum is blocked by the firewall. Remedy: See <i>Step A2: Configuring the Windows firewall</i>, page 8.
1.2	Error message OPC client: none Event message DCOM: none	Event message DCOM 10024: The machine wide group policy <policy> Limits security descriptor start and activation is invalid....	<p>The access to the DCOM settings is blocked.</p> <p>Remedy: Enable the remote access to DCOM in the local security settings, see <i>Step A3: Configuring the local security settings</i>, page 11</p>
1.3	Error message OPC Client: "Access is denied" (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED)) Event message DCOM 1006: DCOM got error "General access denied error " from the computer 'opc_server' when attempting to activate the server: {CLSID OpcEnum}	Event message DCOM 10016: The application-specific permission settings do not grant the activation permission (Remote) for the COM server application with CLSID {CLSID OpcEnum} to the SID (S-1-5-21-3806943333-4088478091-3229395360-1137) for the "user".	<p>The user does not have an access permission for the OPCEnum service of the OPC server.</p> <p>Remedy: Check the user names. See <i>Step B3: User Accounts for OPC Connection</i>, page 19</p>

No.	Error messages client side	Event messages server side	Reasons and remedy
1.4	<p>Error message OPC Client: "The RPC server is unavailable" (Exception from HRESULT: 0x800706BA) or "Create Instance Failed: (Exception from HRESULT: 0x800706BA)" Event message DCOM 10006: DCOM got error "The RPC Server is Unavailable" from the computer 'opc_server' when attempting to activate the server: {CLSID OpcEnum}</p>	none	<ul style="list-style-type: none"> ▪ The computer 'opc_server' is not reachable in the network. Remedy: Check the network connection. ▪ The host name of the 'opc_server' is not known by the client. Remedy: Enter the IP address instead of the host name. ▪ The service OpcEnum is blocked by the firewall on the OPC server side. Remedy: Make sure that the accesses are activated in the firewall of the OPC server, see <i>Step A2: Configuring the Windows firewall</i>, page 8 ▪ The user has no access rights to the service OpcEnum on the OPC server PC. Remedy: Check the user accounts, see <i>Step B3: User Accounts for OPC Connection</i>, page 19.
1.5	<p>Error message OPC client: none Event message DCOM 10006: DCOM got error "The service cannot find the file specified" from the computer 'opc_server' when attempting to activate the server: {CLSID OpcEnum}</p>	<p>Event message DCOM 10000: A DCOM-Server could not be started: {CLSID OpcEnum}. Error: "The service cannot find the file specified", caused by start of this command: "C:\WINDOWS\system32\OpcEnum.exe"-Embedding</p>	<p>No access to the service OpcEnum on the computer 'opc_server'. The service OpcEnum is not installed on the OPC server PC. Remedy Install the "OPC Core Components" on the OPC server PC (implicit by re-installing the OPC server).</p>
1.6	<p>Error message OPC client:none Event message DCOM 100006: DCOM got error "The service is not installed" from the computer 'opc_server' when attempting to activate the server: {CLSID OpcEnum}</p>	none	
1.7	<p>Error message OPC client: none Event message DCOM 10009: DCOM was unable to communicate with the computer 'opc_server' using any of the configured protocols.</p>	none	<ul style="list-style-type: none"> ▪ The computer 'opc_server' is not reachable in the network. Remedy: Check the network connection. ▪ The access to the OPC server is blocked by the firewall. Remedy: Make sure that the file and printer accesses are activated in the firewall of the OPC server, see <i>Step A2: Configuring the Windows firewall</i>, page 8

5.3.2 Error on establishing the connection

No.	Error messages client side	Event messages server side	Reasons and remedy
2.1	<p>Error message OPC client: "Error connecting to OPC server: Access denied. (HRESULT: 0x80070005 (E_ACESSDENIED)</p> <p>Event message DCOM 1006: DCOM got error "General access denied error " from the computer 'opc_server' when attempting to activate the server: {CLSID OPC Server}</p>	<p>Event message DCOM 10016: The machine default permission settings . . do not grant remote activation permission for the COM server application with CLSID {CLSID OPC Server} and APPID {CLSID OPC Server} to the user 'opc_client' SID for users 'opc_client' of address 'ip_adresse'. This security permission can be modified using the Component Services administrative tool.</p>	<p>The user does not have access permission. Remedy:</p> <ul style="list-style-type: none"> ▪ Check the user accounts, see <i>Step B3: User Accounts for OPC Connection</i>, page 19 ▪ Enter the access rights for "Everyone" and "ANONYMOUS LOGON" into the DCOM properties of the OPC server, see <i>Step A6: DCOM settings for OPC server</i>, page 15
2.2	<p>Error message OPC client: "Error connection to OPC server: System cannot find the file specified"</p> <p>Event message DCOM 10006: DCOM got an error "System cannot find the file specified" from the computer 'opc_server' while trying to activate the following server: {CLSID OpcEnum }</p>	<p>Event message DCOM 10000: A DCOM-Server could not be started: {CLSID OpcEnum}. Error: "System cannot find the file specified" appeared while starting "C:\WINDOWS\system32\Opc Enum.exe" -Embedding</p>	<p>No access to the service OpcEnum on the computer 'opc_server'. The service OpcEnum is not installed on the computer. Remedy: install the "OPC core components" on the OPC server side (implicit by re-install the OPC server application)</p>
2.3	<p>Error message OPC client: "Error connection to OPC server: Server execution failed" (HRESULT: 0x80080005 (CO_E_SERVER_EXEC_FAILURE)</p> <p>Event message DCOM 10006: DCOM got error "Server execution failed " from the computer 'opc_server' when attempting to activate the server: {CLSID OPC Server}</p> <p>or</p> <p>Event message DCOM 10010: The server {CLSID OPC Server} did not register with DCOM within the required timeout.</p>	<p>On OPC server (ibaLogic V3) appears the error "It is not allowed to start ibaLogic embedded, please start ibaLogic first". and/or</p> <p>Event message DCOM 10010: The server {CLSID OPC Server} did not register with DCOM within the required timeout.</p>	<ul style="list-style-type: none"> ▪ The OPC server (e.g. ibaLogic) is not running and cannot be started. Remedy: Start the OPC server. ▪ The OPC server has an incorrect identity. Remedy: Set the DCOM identity of the OPC server on the "<i>Identity</i>" tab to "interactive user", see <i>Step A6: DCOM settings for OPC server</i>, page 15 <i>Step A6: DCOM settings for OPC server</i>, page 15

No.	Error messages client side	Event messages server side	Reasons and remedy
2.4	Error message OPC client: "Error connecting to OPC server: The RPC server is unavailable " (HRESULT: 0x800706BA) Event message DCOM 10006: DCOM got error "The RPC Server is Unavailable" from the computer 'opc_server' when attempting to activate the server: {CLSID OPC Server}	none	<ul style="list-style-type: none"> ▪ The OPC server cannot be reached over the network. Remedy: Check the network connection. ▪ The host name of the OPC server computer is unknown. Remedy: Use the IP address instead of the host name. ▪ The service OpcEnum or the OPC server is blocked by the firewall. Remedy: See <i>Step A2: Configuring the Windows firewall</i>, page 8
2.5	Error message OPC client: none Event message DCOM 10009: DCOM was unable to communicate with the computer 'opc_server' using any of the configured protocols.	none	The OPC server cannot be reached in the network. Remedy: Check network and firewall settings.
2.6	Error message OPC client: "Error connecting to OPC server: Create Instance Failed: 0x80040154 Event message DCOM 10006: DCOM got error "The class is not registered " from the computer 'opc_server' when attempting to activate the server:	none	Occurs on ibaPDA OPC server: The ibaPDA server runs with a local system account. Remedy: Logon the ibaPDA service with a Windows user account see <i>Specialties for ibaPDA</i> , page 23
2.7	Error message OPC client: none Event message DCOM: none	Event message DCOM 10024: The machine wide group policy <policy> Limits security descriptor Start and Activation is invalid.	The remote access to the DCOM settings is blocked. Remedy: Enable the remote access to DCOM in the local security settings, see <i>Step A4: Open the DCOM configuration</i> , page 13

5.3.3 Error: Client does not receive data

No.	Error messages client side	Event messages on server	Reasons and remedy
3.1	Error message OPC client: none Event message DCOM: none	none	<ul style="list-style-type: none"> Network access is not enabled in the local security settings on the client PC. Remedy: Change the local security policy, see <i>Step B2: Configuring the local security settings</i>, page 18.
3.2	Error message OPC client: Error at activating the callback of the OPC server: (Exception from HRESULT: 0x80040202) Event message DCOM: none	none	<ul style="list-style-type: none"> The OPC user account (or account with that the OPC server and client are logged in) does not have a password. Remedy: Enter a valid user account and a password See <i>Step B3: User Accounts for OPC Connection</i>, page 19.
3.3	Error message OPC client: Error at activating the callback of the OPC server: Access denied (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED)) Event message DCOM: none	none	<p>The user 'opc_client' does not have access rights.</p> <ul style="list-style-type: none"> Remedy: Check the user accounts, see <i>Step B3: User Accounts for OPC Connection</i>, page 19. Set the DCOM property <i>Identity</i> of the OPC server to: "This user: [...] <OPC-Client>"
3.4	Error message OPC client: Error at activating the callback of the OPC server: The RPC server is unavailable (Exception from HRESULT: 0x800706BA) Event message DCOM 10006: DCOM got error "The RPC Server is Unavailable" from the computer 'opc_server' when attempting to activate the server: {CLSID OpcEnum}	none	<ul style="list-style-type: none"> The service OPCEnum.exe is blocked on the server side by a firewall. Remedy: Enter OpcEnum in the firewall, see <i>Step A2: Configuring the Windows firewall</i>, page 8. The OPC client is blocked by the firewall. Remedy: Enter the OPC client in the firewall, see <i>Step B1: Configuring the Windows firewall</i>, page 17

No.	Error messages client side	Event message server side	Reasons and remedy
3.5	<p>Error message OPC client: "Connection to OPc server failed" with error: "System cannot find the file specified"</p> <p>Event message DCOM 1000: A DCOM-Server could not be started {CLSID OpcEnum}. Error: "System cannot find the file specified"</p>	none	<p>No access to the service OpcEnum on the computer 'opc_server'. The service OpcEnum cannot be installed on the server.</p> <p>Remedy: install the "OPC core components" on the OPC server side (implicit by reinstalling the OPC server)</p>
3.6	<p>Error message OPC client: none</p> <p>Event message DCOM 10006: DCOM got error "Server execution failed " from the computer 'opc_server' when attempting to activate the server: {CLSID OPC Server}</p>	<p>Event message DCOM 10010: The server {CLSID OPC Server} OPC Server did not register with DCOM within the required time period.</p>	<p>The OPC server (e. g. ibaLogic V3) is not running.</p> <p>Remedy: Start the OPC server, e. g. ibaLogic and start evaluation.</p>
3.7	<p>Error message OPC client: none</p> <p>Event message DCOM 10020: The machine wide Default Launch and Activation security descriptor (default) is invalid. It contains Access Control Entries with permissions that are invalid. The requested action was therefore not performed. This security permission can be corrected using the Component Services administrative tool.</p>	none	<p>Non permissible entries in the DCOM default settings :</p> <p>Remedy: Change the DCOM default settings.</p>

6 Support and contact

Support

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



Note

If you require support, indicate the serial number (iba-S/N) of the product.

Contact

Headquarters

iba AG
Koenigswarterstr. 44
90762 Fuerth
Germany

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

Regional and worldwide

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

www.iba-ag.com.