

Integration Objects' DCOM Configuration Guidelines

Published November 2018 Copyright © 2018 Integration Objects. All rights reserved.



TABLE OF CONTENTS

| 1. | Abo | ut This User Guide | 3 |
|-------|------|---|---|
| 2. | Mac | hines Configuration | 3 |
| 2.1. | Inst | all OPC Core Components | 3 |
| 2.2. | Con | figure Users | 3 |
| 2.3. | Ass | ign Permissions | 3 |
| 3. | Win | dows Firewall Configuration in OPC Server Machine | 5 |
| 4. | Net | work Discovery | 8 |
| 5. | DCC | DM Configuration1 | 0 |
| 5.1. | OPO | C Server Machine Configuration1 | 0 |
| 5.1.1 | 1. | Configure System-Wide DCOM settings1 | 0 |
| 5.1.2 | 2. | Configure Server Specific DCOM Settings1 | 3 |
| 5.1.2 | 2.1. | Launch and Activation Permissions1 | 5 |
| 5.1.2 | 2.2. | Access Permissions1 | 6 |
| 5.1.2 | 2.3. | Configuration Permissions1 | 7 |
| 5.1.3 | 3. | OPCEnum Configuration2 | 0 |
| 5.1.3 | 3.1. | Launch and Activation Permissions2 | 1 |
| 5.1.3 | 3.2. | Access Permissions2 | 1 |
| 5.1.3 | 3.3. | Configuration Permissions2 | 1 |
| 5.2. | OPO | Client Machine Configuration2 | 2 |
| 5.2.1 | 1. | Configure System-Wide DCOM Settings2 | 2 |
| 5.2.2 | 2. | Configure Windows Firewall2 | 2 |
| 6. | Sys | tem Restart24 | 4 |
| 7. | Tro | ubleshooting2 | 4 |



1. About This User Guide

OPC Classic standard specifications rely on Microsoft's COM and DCOM to exchange data between automation hardware and software. DCOM needs to be configured properly in order to allow users to establish remote communications between their OPC client and server components. In this document, we describe the necessary steps to get DCOM working properly under Windows Seven in a Workgroup configuration.

2. Machines Configuration

2.1. Install OPC Core Components

OPC Core Components need to be installed on the OPC server and OPC client machines. You need to install OPC Core Components version according to the operating system version (64-bit or 32-bit).

2.2. Configure Users

In a typical scenario, we would have two machines as follows:

| Machine | 1 | 2 |
|---------------|---|--|
| Name | User-IO1 | User-IO2 |
| User Login | IO1 | IO1 |
| User Password | io1 | io1 |
| Workgroup | IOGROUP | IOGROUP |
| Туре | Client Machine | Server Machine |
| Software | Integration Objects' OPC DA Explorer | Integration Objects' OPC Driver for Databases |

Table 1: Platform Configuration

The created users must have the same name and password on both computers. Further on, you should run the OPC client and OPC Server using this user account.

2.3. Assign Permissions

In order to allow the users to work with DCOM, you need to add them to the corresponding "DCOM Users" group in **both client and server machine**. To do so:



1. Click on Computer \rightarrow Manage



Figure 1: Computer Management

- 2. Navigate to 'System Tools' \rightarrow 'Local Users and Groups' \rightarrow 'Groups'
- 3. Right click on 'Distributed COM Users' and then click on properties.



Figure 2: DCOM Group

4. On the properties tab, click on Add \rightarrow Advanced \rightarrow Find Now and select the IO1 user.



| Distributed COM Us | sers Properties | ? × |
|--------------------|---|--------------------------|
| General | | |
| Distribut | ted COM Users | |
| Description: | Members are allowed to launch, activate and Distributed COM objects on this machine. | luse |
| Members: | | |
| 💭 user | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Add | Changes to a user's group m are not effective until the nex user logs on. | embership kt time the |
| | OK Cancel Apply | Help |

Figure 3: Add User to DCOM Group

3. Windows Firewall Configuration in OPC Server Machine

By default, the Windows firewall stops any incoming requests across the network. However, it gives the ability to add exceptions by specifying applications and ports that need to be allowed.

To add an exception, please proceed to the following steps:

- 1. Go to Control Panel →System and Security→ Windows Firewall
- 2. Check the status of the firewall, in case it is enabled, continue with the following steps. Otherwise, you can skip this section.
- 3. Right click on "Inbound Rule"
- 4. Click on "New Rule"





Figure 4: New Rule

- 5. Select "Program" and click on Next
- 6. Click on "Browse" and select your OPC Server executable





Figure 5: Add Program

- 7. Select "Allow the connection" and then click Next
- 8. Click next then name your rule to "RuleOPCDADriver"



| 🔐 New Inbound Rule Wizard | | — × |
|----------------------------------|--------------------------------------|------------|
| Name | | |
| Specify the name and description | of this rule. | |
| Steps: | | |
| Bule Type | | |
| Program | | |
| Action | | |
| Profile | Name: BuleOPCDADriver | |
| 🧼 Name | Haleor CDADING | |
| | Description (optional): | |
| | Rule for UPC DA Driver for Databases | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | < <u>B</u> ack <u>E</u> inish Cance | el |
| | | |

- 9. Click Finish
- 10. Redo the same procedure to add rule to OPC HDA Driver for Databases.
- 11. Redo the same procedure to add rule to the OPCEnum: Choose This program path, hit Browse, find opcenum.exe, double click it and hit next> The path should be: For 32 bit machine: c:\Windows\system32\opcenum.exe For 64 bit machine: c:\Windows\SysWOW64\opcenum.exe.
- 12. Redo the same procedure to add rule to add the DCOM TCP port "135"
- 13. Make sure to enable both rules

4. Network Discovery

- 1. Click Start | Control Panel | Network and Sharing Center.
- 2. Click Change advanced sharing settings



| 😋 🗢 🖳 🕨 Control Panel 🕨 | All Control Panel Items 🔸 Network and Sharing Center | ✓ ✓ |
|--|---|---|
| Control Panel → Control Panel Home Change adapter settings Change advanced sharing settings | All Control Panel Items Network and Sharing Center View your basic network information and s WM1-TESTSAL7 Unidentified netw (This computer) View your active networks Unidentified network Public network Change your networking settings Set up a new connection or network Set up a wireless, broadband, dial-up, ad hoc, Connect to a network Connect or reconnect to a wireless, wired, dial | Search Control Panel Search Control Panel Search Control Panel Set up connections See full map ork Internet Connect or disconnect Access type: No Internet access Connections: Local Area Connection or VPN connection; or set up a router or access point. I-up, or VPN network connection. |
| See also HomeGroup Internet Options Windows Firewall | Choose homegroup and sharing options Access files and printers located on other network Troubleshoot problems Diagnose and repair network problems, or get | work computers, or change sharing settings. : troubleshooting information. |

3. Click the Turn on network discovery radio button, and then click Save changes button.

| | - • • |
|---|----------|
| 🚱 🗢 💐 « Network and Sharing Center 🔸 Advanced sharing settings 💿 🚽 🐓 Search Control | Panel 🔎 |
| | <u>^</u> |
| Change sharing options for different network profiles | |
| Windows creates a separate network profile for each network you use. You can choose specific options for each profile. | |
| Home or Work | |
| Public (current profile) | E |
| Network discovery | |
| When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. <u>What is network discovery?</u> | |
| Turn on network discovery Turn off network discovery | |
| File and printer sharing | |
| When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network. | |
| Turn on file and printer sharing | |
| Turn off file and printer sharing | |
| Public folder sharing | |
| When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. <u>What are the Public folders?</u> | |
| Turn on sharing so anyone with network access can read and write files in the Public folders | - |
| Save changes Cancel |] |

Figure 6: Turn on the network discovery



Make sure to apply the Network Discovery steps on both server and client machines.

5. DCOM Configuration

5.1. OPC Server Machine Configuration

5.1.1. Configure System-Wide DCOM settings

The system-wide DCOM settings affect all Windows applications that use DCOM, including OPC applications. In fact, any OPC Client application does not have its own DCOM settings, which make it affected by changes of the default DCOM configuration. This is why, system settings must be configured properly. To do so, follow the steps below:

• Click on the Windows Start button, and select Run and then type "dcomcnfg" to open the DCOM configuration dialog box.

| 0.5 | | |
|--|---|-------------|
| >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>> | | |
| | | |
| dcomcnfg | × | Shut down 🕨 |
| | | |

Figure 7: Run dcomcnfg Command

- Navigate inside the Console Root folder to the Component Services folder and then to the Computers folder. Finally, you will find the My Computer tree control inside the Computers folder.
- Right-click on My Computer \rightarrow Properties \rightarrow Default Properties tab
 - Make sure to check the "Enable Distributed COM on this computer' check box
 - Set the 'Default Authentication Level' to 'Connect'
 - Set the 'Default Impersonation Level' to 'Identify'



| My Computer Properties | | × | ? <mark>x</mark> | | | |
|---|--------------------|-------------|------------------|--|--|--|
| Default Protocols COM Security MSDTC | | | | | | |
| General | Options | Defa | ault Properties | | | |
| Enable Distributed COM | on this computer | | | | | |
| Enable COM Internet Se | rvices on this cor | nputer | | | | |
| Default Distributed COM C | Communication Pr | operties | | | | |
| The Authentication Level | specifies security | at the pack | ket level. | | | |
| Default Authentication L | evel: | | | | | |
| Connect | | • | | | | |
| who is calling them, and whether the application can do operations using the client's identity. Default Impersonation Level: | | | | | | |
| Identify 🗸 | | | | | | |
| Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous. | | | | | | |
| Leam more about <u>setting these properties</u> . | | | | | | |
| | ОК | Cance | Apply | | | |

Figure 8: My Computer Default Properties

- Right-click on My Computer → Properties →COM Security tab → Access permissions → Edit limits :
 - 1. You need to add the user IO1 to the list and give it all local and remote access rights.
 - 2. You need to check the remote Access for the User "ANONYMOUS LOGON" and for the "Distributed Com Users" as shown below:



| My Computer Properti | es 🖓 | | ? 🕱 |
|---|--|-----------------------------------|-----------------------------|
| General | Options | Default | Properties |
| Default Protocols | COM Se | curity | MSDTC |
| Access Permissio | on | | ? 💌 |
| Security Limits | | | |
| Group or user r | names: | | |
| Everyone Reformar Solution ANONYM | nce Log Users (SERVE d COM Users (SERVE IOUS LOGON | RM\Performanc RM\Distributed (| ce Log Users) COM Users) |
| â lo1 (SER | VERM' \lo1) | | |
| Permissions for LOGON | ANONYMOUS | Add | Remove Deny |
| Local Acces | s | v | |
| Remote Acc | ress | V | |
| Leam about ad | ccess control and perm | OK | Cancel |
| | ОК | Cancel | Apply |

Figure 9: Access Permission

Under the 'Launch and activation permissions' tab:

- You need to add the user IO1 to the list and give him all local and remote access.
 You need to check the remote boxes for the User labeled "Everyone" and for the "Distributed Com Users" as shown in the figure below.



| y Computer Propert | ies | | 8 |
|--------------------|---|-----------------------------------|-----------------|
| General | Options | Defa | ault Properties |
| Launch and Activ | ation Permission | | ? 💌 |
| Security Limits | | | |
| Group or user na | imes: | | |
| Everyone | | | |
| Administration | ORS (SERVERM\Ad COM Users (SERV OUS LOGON | ministrators) 'ERM\Distributed | I COM Users) |
| 👗 lo1 (SERVI | ERM' \lo1) | | |
| | | Add | Remove |
| Permissions for E | Everyone | Allow | Deny |
| Local Launch | | V | |
| Remote Laun | ch | | |
| Local Activati | on | V | |
| Remote Activ | ation | \checkmark | |
| | | | |
| | | | |
| | | | |
| Leam about acc | ess control and pe | missions | |
| | | ОК | Cancel |
| | ОК | Cance | I Apply |

Figure 10: Launch and Activation Permission

5.1.2. Configure Server Specific DCOM Settings

In this section, we will see how to configure the OPC server specific DCOM settings to allow access only for the user (login: IO1, password: io1).

- Go to Windows start button → select the 'run' menu → type "DCOMCNFG" and then click on 'OK'.
- On the Component Services window, navigate inside the Console Root folder to the Component Services folder and then to the Computers folder.
- Open My Computer folder and then the DCOM Config folder
- Locate the server your need to allow remote access on
- Right click on it and select the 'Properties' tab:
 - ➔ Go to "General" tab and set the "Authentication level" to "Connect" as illustrated in the figure below:



| Integration Objects' OPC Driver for Databases; http://www.i | | | |
|--|--|--|--|
| General Location Security Endpoints Identity | | | |
| General properties of this DCOM application | | | |
| Application Name: Integration Objects' OPC Driver for Databases; h | | | |
| Application ID: {81ACD3D7-9F39-4776-845E-0AD85AB3306B} | | | |
| Application Type: Local Service | | | |
| Authentication Level: Connect 🔹 | | | |
| Service Name: Integration Objects' OPC Driver for Databases Si | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| Learn more about <u>setting these properties</u> . | | | |
| | | | |
| | | | |

Figure 11: General Tab

→ Go to the "Security" tab. For each permission type, choose the 'Customize' radio button and then click on the "Edit" button



| Integration Objects' OPC Driver for Databases; http://www.i 🔋 💌 | | | |
|---|--|--|--|
| General Location Security Endpoints Identity | | | |
| Launch and Activation Permissions | | | |
| © ∐se Default | | | |
| © Customize | | | |
| Access Permissions | | | |
| O Use De <u>f</u> ault | | | |
| Customize Edit | | | |
| Configuration Permissions | | | |
| 🔘 Use Default | | | |
| Customize Edit | | | |
| | | | |
| | | | |
| Learn more about <u>setting these properties</u> . | | | |
| | | | |

Figure 12: Security Tab

5.1.2.1. Launch and Activation Permissions

Click on the "add" button \rightarrow add the user (IO1, io1) to the group or users names, give all the permissions for IO1(Local Launch, Remote Launch, Local Activation, Remote Activation), and make sure to add Everyone to the list as illustrated in the figure below:



| Integration Objects' OPC Driver for Databases; http://www.i 🔋 🖾 | | |
|---|--|--|
| General Location Security Endpoints Identity | | |
| Launch and Activation Permission | | |
| Security | | |
| Group or user names: | | |
| Let (USER Leguet) | | |
| & IDT (USER-ID2XIDT) & SYSTEM | | |
| A NETWORK | | |
| & Administrators (USER-102\Administrators) | | |
| Add Remove | | |
| | | |
| Permissions for Everyone Allow Deny | | |
| Local Launch | | |
| Lead Activitian | | |
| Remote Activation | | |
| | | |
| | | |
| | | |
| Learn about access control and permissions | | |
| OK Cancel | | |
| | | |

Figure 13: Launch and Activation permission

5.1.2.2. Access Permissions

Perform the same steps as the previous section. Make sure to remove Everyone from the list add user IO1and give it all permissions



| itegration Objects' OPC Driver for Databases; http://www.i 😰 🖾 General Location Security Endpoints Identity | | |
|--|---|--|
| Access Permission | () () () () () () () () () () () () () (| |
| Security | | |
| Group or user names: | | |
| SYSTEM | | |
| NETWORK | | |
| & Administrators (USER-IO2\Administrators) | | |
| | | |
| | | |
| | Add Remove | |
| Permissions for IO1 | Allow Deny | |
| Local Access | | |
| Remote Access | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Learn about access control and permissions | | |
| _ | OK Cancel | |
| | | |

Figure 14: Access Permission

5.1.2.3. Configuration Permissions

Make sure to remove Everyone from the list, add user IO1 and give it all access rights



| Integration Objects' OPC Driver for Databases; http://www.i 👔 🖾 | | |
|--|--|--|
| General Location Security Endpoints Identity | | |
| Change Configuration Permission | | |
| Security | | |
| Group or user names: | | |
| & CREATOR OWNER | | |
| SYSTEM | | |
| & Administrators (USER-102\Administrators) & Users (USER-102\Users) | | |
| Add Remove | | |
| Permissions for IO1 Allow Deny | | |
| Full Control | | |
| Read 🔽 🗖 | | |
| Special permissions | | |
| For special permissions or advanced settings, Advanced click Advanced. | | |
| Learn about access control and permissions | | |
| OK Cancel | | |
| | | |

Figure 15: Change Configuration Permission

- → Go to the "Identity" tab:
 - 1. If your OPC server is running as a service, choose "The system account (service only)" option and make sure to set the logon for your service to IO1 user.
 - 2. Otherwise, choose "The interactive user" option.



| Integration Objects' Advanced OPC DA HDA Server Simulat 📰 💌 | | |
|--|--|--|
| General Location Security Endpoints Identity | | |
| Which user account do you want to use to run this application? | | |
| The interactive user. | | |
| The launching user. | | |
| This user. | | |
| User: Browse | | |
| Password: | | |
| Confirm password: | | |
| The system account (services only). | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Learn more about <u>setting these properties</u> . | | |
| | | |
| OK Cancel Apply | | |

Figure 16: Identity Rab

➔ Go to the "Endpoints" tab and choose Connection-oriented TCP/IP

| Integration Objects' OPC Server Enterprise; http://www.inte 👔 🖾 | | |
|---|--|--|
| General Location Security Endpoints Identity | | |
| | | |
| | | |
| T default system protocols | | |
| Select DCOM protocol and endpoint | | |
| Select the DCOM network protocol sequence that you want to add. Enter the endpoint details and click OK when you have finished. | | |
| Protocol Sequence: Connection-oriented TCP/IP | | |
| Disable protocol sequence. | | |
| O Use default endpoints. | | |
| ◯ Use static endpoint | | |
| O Use intranet range of dynamic endpoints. | | |
| Use internet range of dynamic endpoints. | | |
| OK Cancel | | |
| Leam more about <u>setting these properties</u> . | | |
| OK Cancel Apply | | |

Figure 17: Endpoints Tab



5.1.3. OPCEnum Configuration

Using the Component services window, right click on OPCEnum. The following window will appear:

| OpcEnum Properties | | |
|--|--|--|
| General Location Security Endpoints Identity | | |
| General properties of this DCOM application | | |
| Application Name: OpcEnum | | |
| Application ID: {13486D44-4821-11D2-A494-3CB306C10000} | | |
| Application Type: Local Service | | |
| Authentication Level: Connect | | |
| Service Name: OpcEnum | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| Leam more about <u>setting these properties</u> . | | |
| | | |
| OK Cancel Apply | | |

Figure 18: DCOM OPC Enum - General

- Make sure to select Connect as Authentication level.
- Select "Security" tab. The following window will appear:



| OpcEnum Properties | ? <mark>- × -</mark> |
|---|----------------------|
| General Location Security Endpoints Identity | |
| Launch and Activation Permissions | |
| Use Default | |
| Oustomize | Edit |
| Access Permissions | |
| ─ Use Default | |
| Oustomize | Edit |
| Configuration Permissions | |
| 🔘 Use Default | |
| Oustomize | Edit |
| Leam more about <u>setting these properties</u> . | |
| OK Can | Apply |

Figure 19: OPCEnum Security

5.1.3.1. Launch and Activation Permissions

Click on the "add" button, add everyone and ANONYMOUS LOGON, give them all permissions: Local Launch, Remote Launch, Local Activation, and Remote Activation.

5.1.3.2. Access Permissions

Perform the same steps as the section 5.1.2.2.

5.1.3.3. Configuration Permissions

Perform the same steps as the section 5.1.2.3.



5.2. OPC Client Machine Configuration

5.2.1. Configure System-Wide DCOM Settings

Perform the same steps as described in the section 5.1.1.

5.2.2. Configure Windows Firewall

On the client machine, follow the steps below:

- Make sure that OPC core component is installed and configure windows firewall by adding the following rules:
 - 1. Go to Control Panel →System and Security→ Windows Firewall
 - 2. Check the status of the firewall, in case it is enabled, continue with the following steps. Otherwise, you can skip this section.
 - 3. Right click on "Inbound Rule"
 - 4. Click on "New Rule"



Figure 20 : New Rule (Client side)

- 5. Select "Program" and click on Next
- 6. Click on "Browse" and select your OPC Client executable



| 🔗 New Inbound Rule Wizard | | |
|-----------------------------------|---|--|
| Program | | |
| Specify the full program path and | executable name of the program that this rule matches. | |
| Steps: | | |
| Bule Type | Does this rule apply to all programs or a specific program? | |
| Program | | |
| Action | All programs Determine a structure of the second structure of the second second structure of the second | |
| Profile | Nule applies to all connections on the computer that match other rule properties. | |
| Name | ◎ <u>T</u> his program path: | |
| | %ProgramFiles% (x86)\Integration Objects\Integration Objects' OPC DA HD. Browse | |
| | Example: c:\path\program.exe %ProgramFiles%\browser\browser.exe | |
| | | |
| | Learn more about specifying programs | |
| | <u> </u> | |

Figure 21: Add Program (Client side)

- 7. Select "Allow the connection" and then click Next
- 8. Click next then name your rule to "RuleOPCClient"
- 9. Click Finish



6. System Restart

Restart both Client and Server Machines and test your DCOM communications.

7. Troubleshooting

In some cases, the client cannot connect to the remote OPC Server because it does not have access to browse the remote registry. It is recommended to prepare and apply a customized .reg file on the client computer in order to export Implemented categories and CLSID from the server machine registry database and add them to the client machine registry. To do so, proceed to the following steps:

1st Step:

- On the server machine, click on the Windows Start button, and select Run, and then type "regedit" to open the registry Editor Dialog box.
- Search for your server CLSID under "HKEY_CLASSES_ROOT" → "CLSID".
- Right click on your Server CLSID and click on "Export.
- Save the Exported CLSID.



Figure 22: Export the Server CLSID

• Copy the .reg file in your client machine and double click on it.

2nd Step:

- Search for your server ProgID under "HKEY_CLASSES_ROOT" → "Server ProgID".
- Right click on your Server ProgID and click on "Export".
- Copy the Exported ProgID and execute it on the client machine.

• 3rd Step:

• Go to HKEY_CLASSES_ROOT \rightarrow AppID and search for your server CLSID.



- Right click on it and Click on "Export".
- \checkmark Copy the Exported file and execute it on the client machine.



Make sure that there are no other firewall or antivirus blocking the communication between the server and client machines.

Now you will be able to connect to the server located on the server machine (User-IO2) from the client machine (User-IO1).



For additional information on this guide, questions or problems to report, please contact:

Offices

- Americas: +1 713 609 9208
- Europe-Africa-Middle East: +216 71 195 360

Email

- Support Services: customerservice@integrationobjects.com
- Sales: sales@integrationobjects.com

To find out how you can benefit from other Integration Objects products and custom-designed solutions, please visit us on the Internet:

Online

- www.integrationobjects.com