# Integration Objects'
## DCOM Configuration Guidelines

Published November 2018



customerservice@integrationobjects.com

# TABLE OF CONTENTS

# 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 |
| **Type** | 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 → Manage

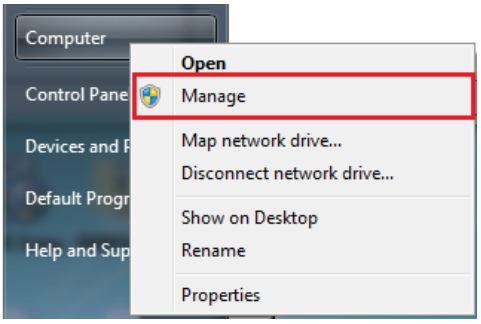



**Figure 1: Computer Management**

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

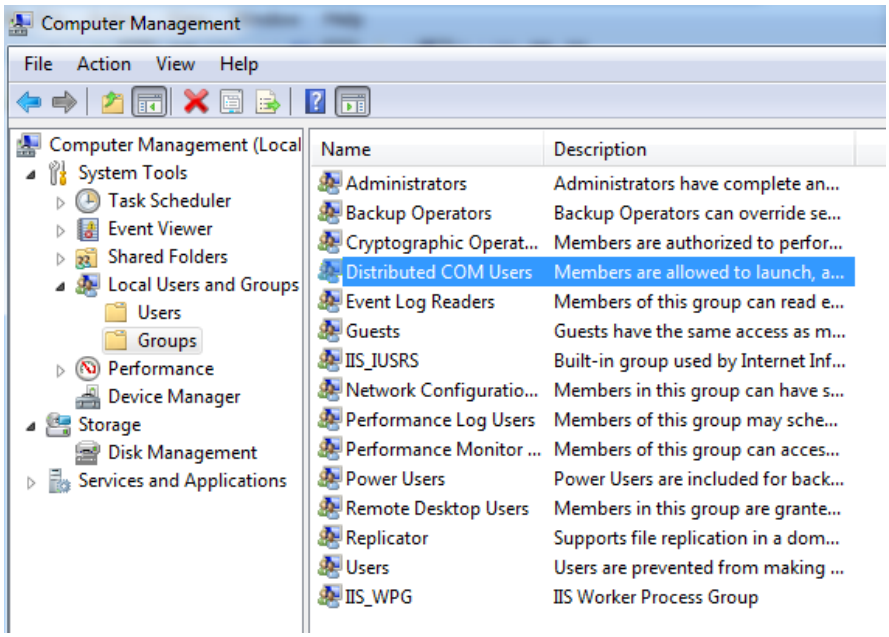



**Figure 2: DCOM Group**

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

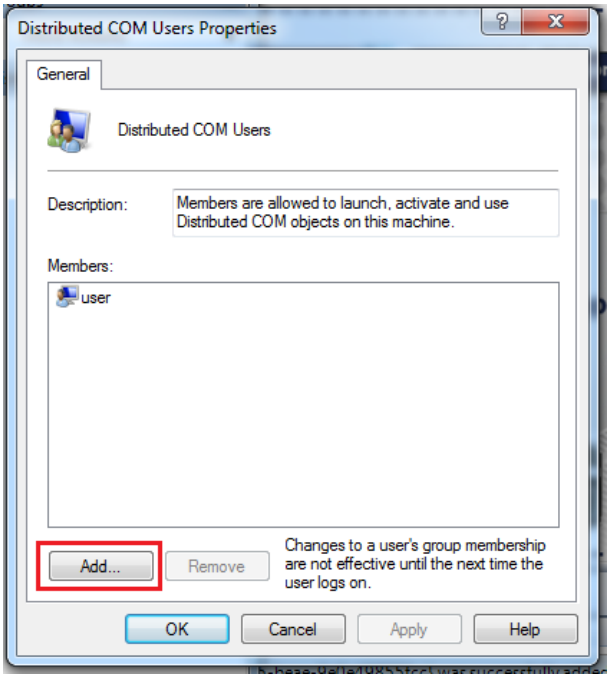



**Figure 3: Add User to DCOM Group**

## 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”

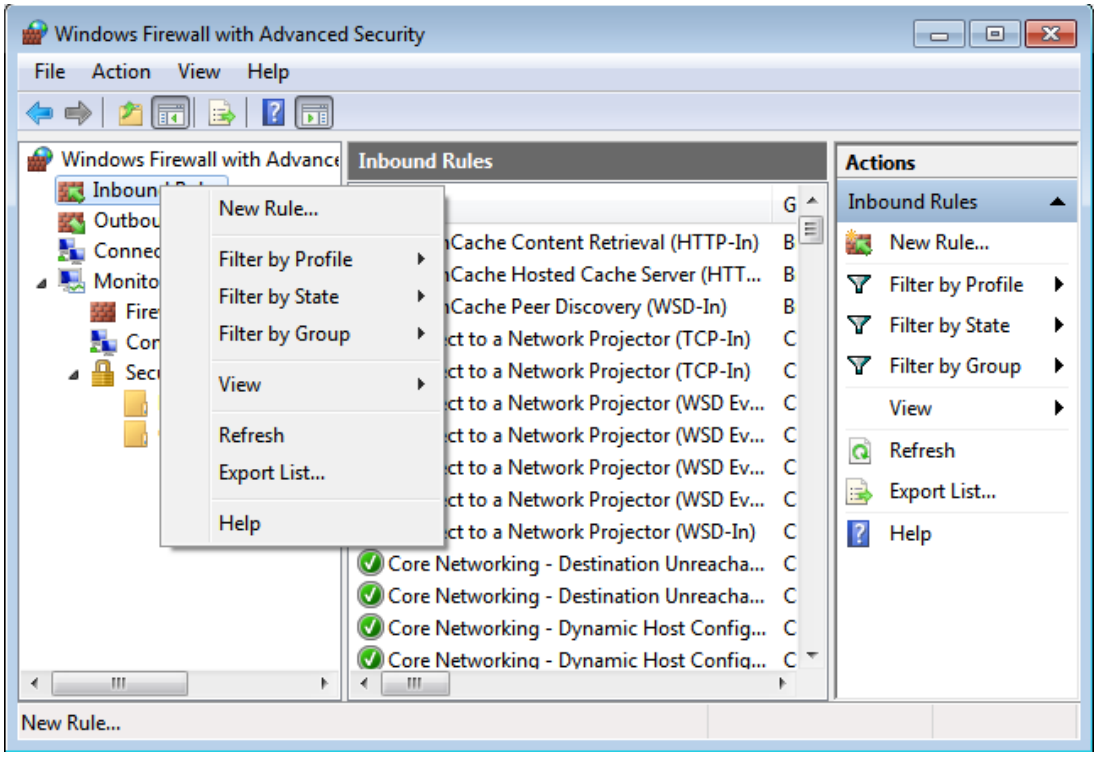



**Figure 4: New Rule**

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

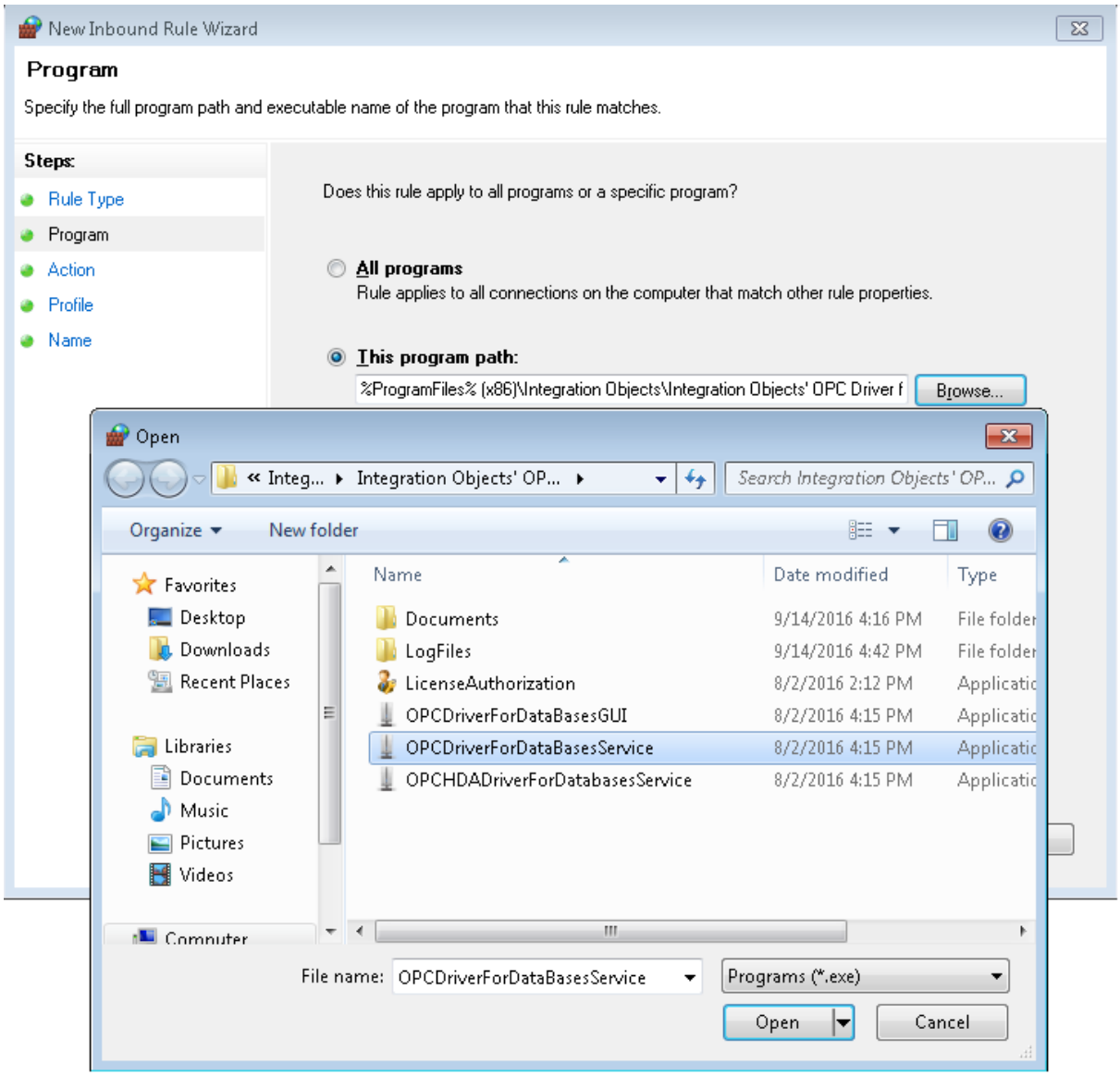
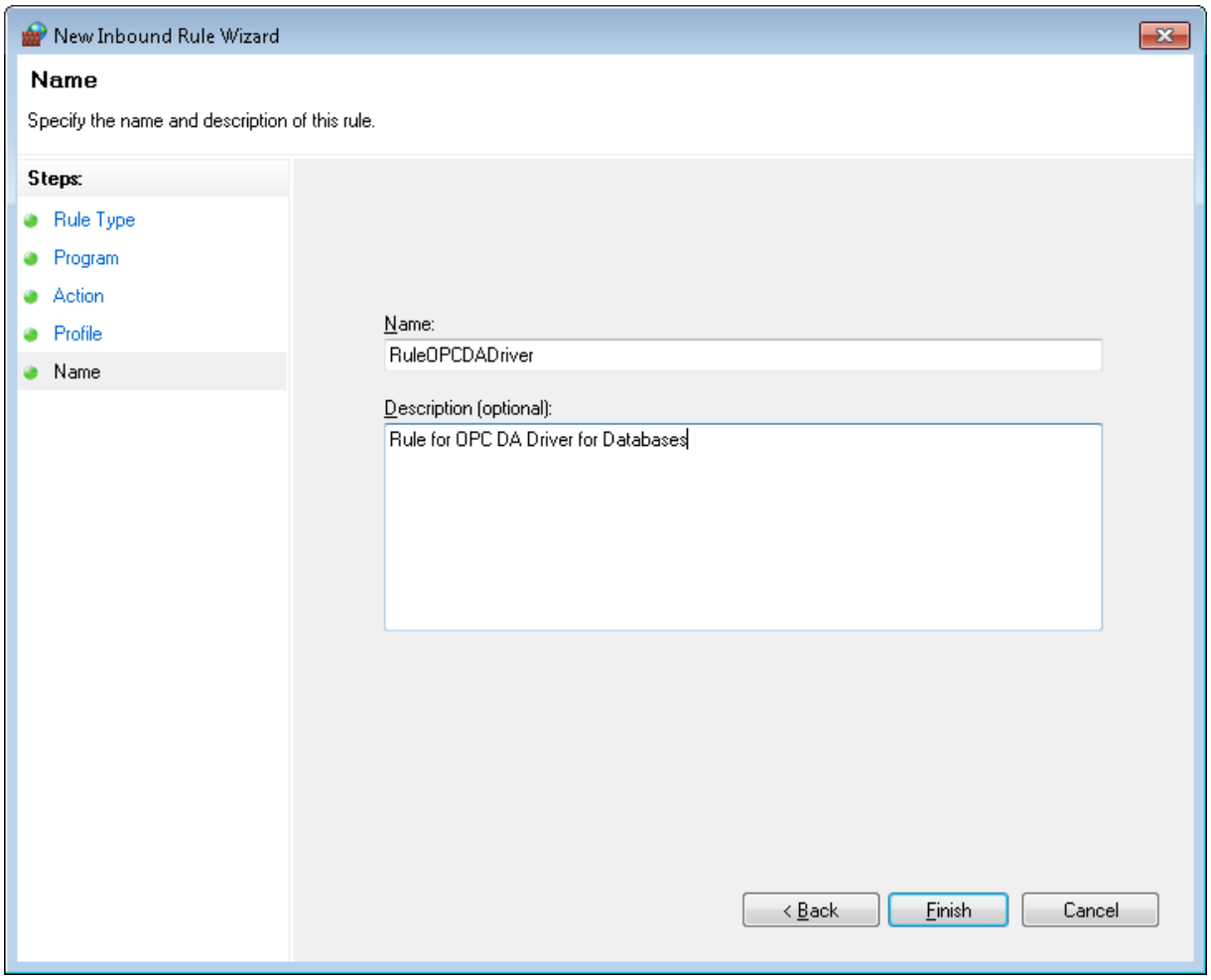



**Figure 5: Add Program**

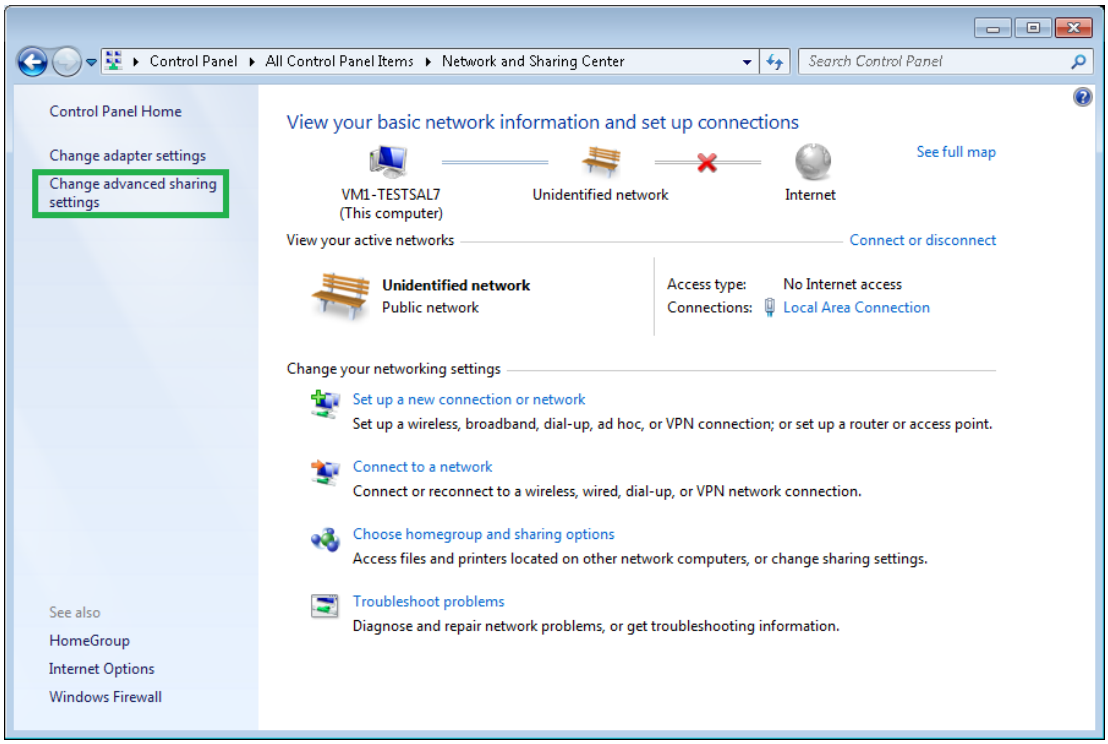
7. Select “Allow the connection” and then click Next
8. Click next then name your rule to “RuleOPCDADriver”




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**




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

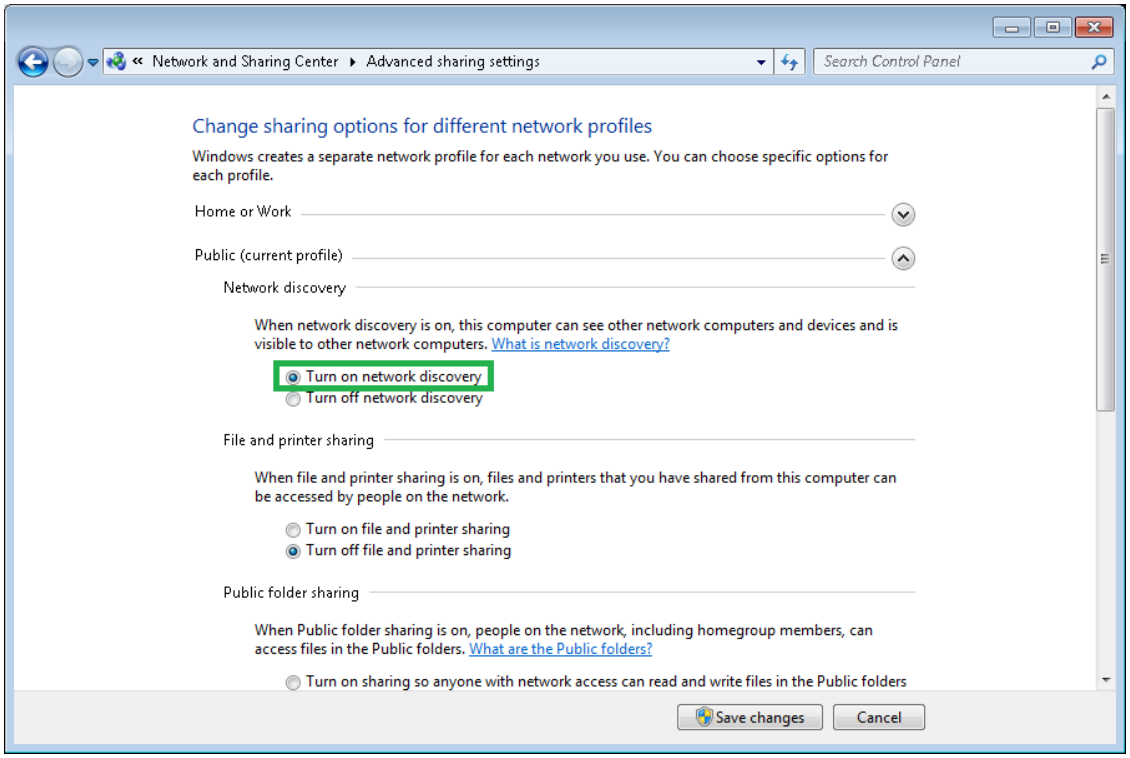



**Figure 6: Turn on the network discovery**

**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.

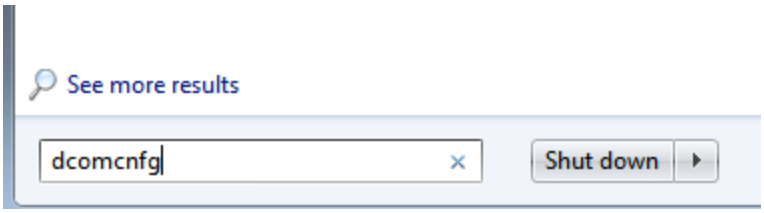



**Figure 7: Run dcomcnfg Command**

- 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 → Properties →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’

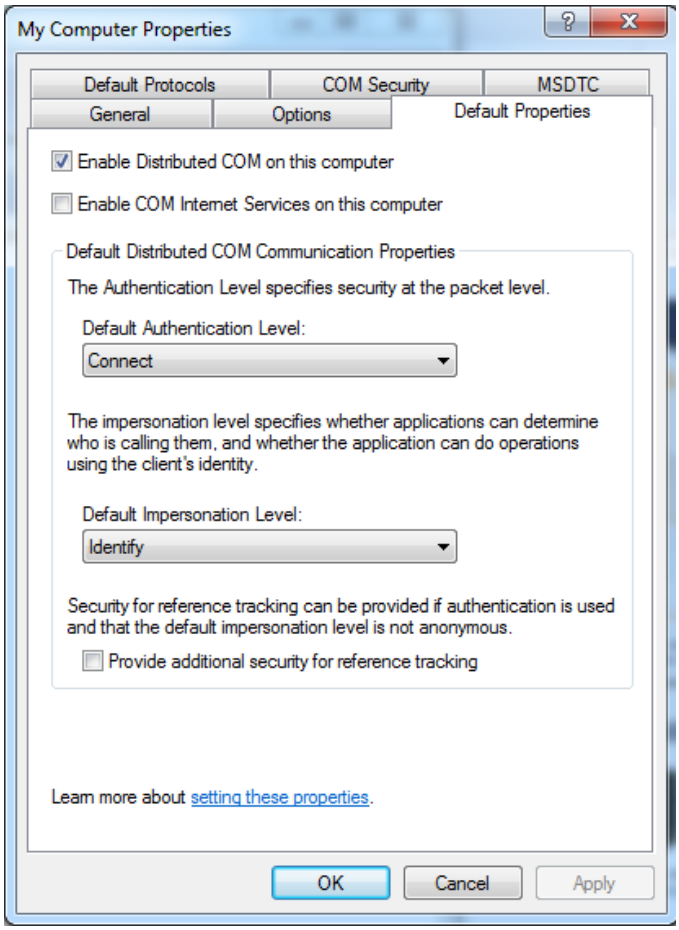



**Figure 8: My Computer Default Properties**

- 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:

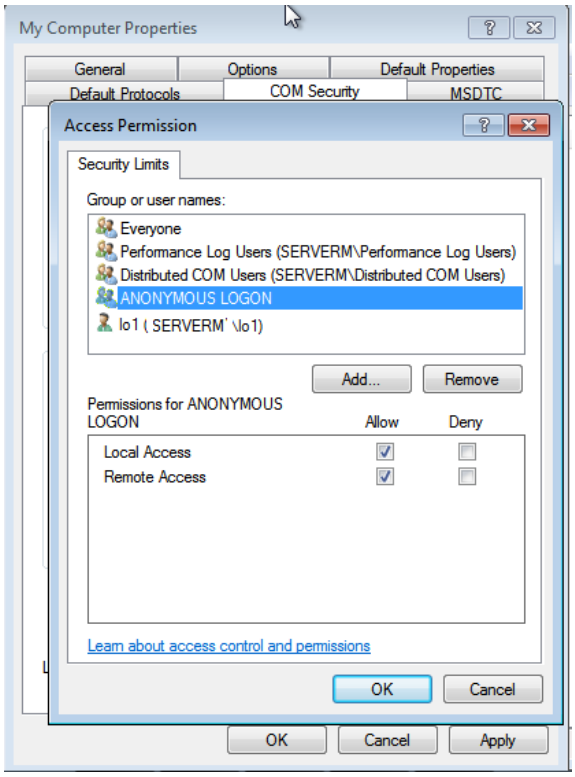



**Figure 9: Access Permission**

Under the 'Launch and activation permissions' tab:

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

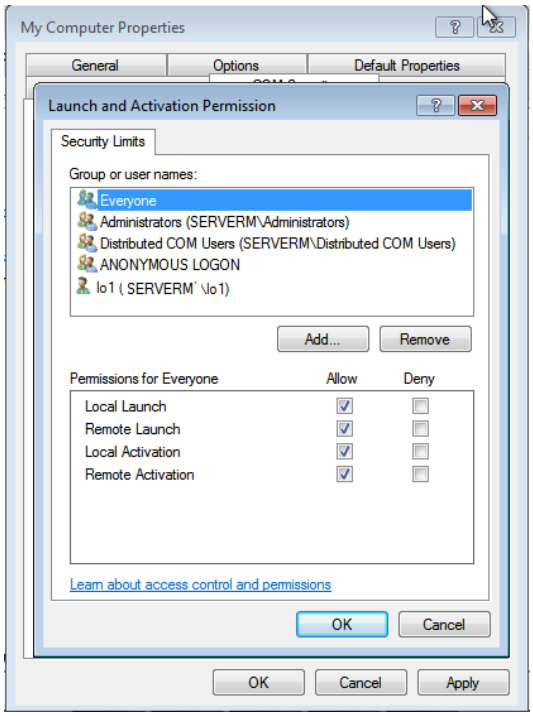



**Figure 10: Launch and Activation Permission**

### 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:

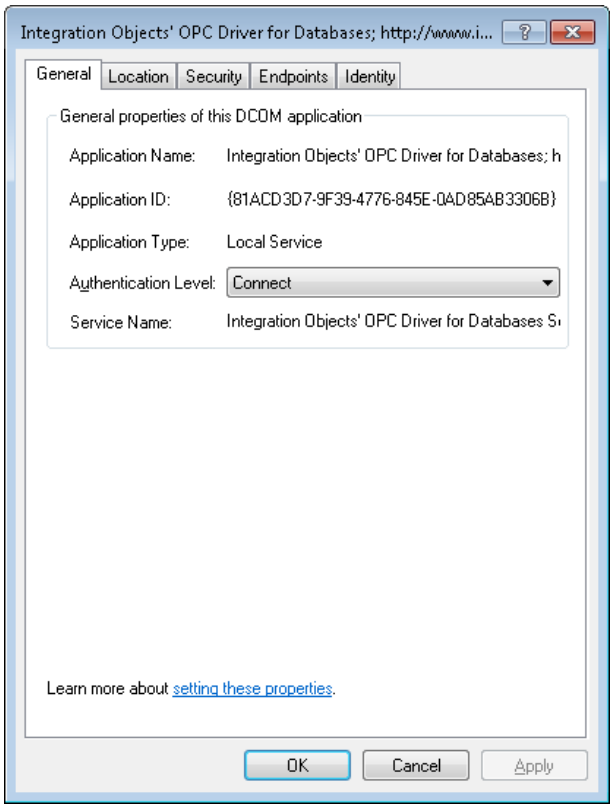



**Figure 11: General Tab**

➔ Go to the “Security” tab. For each permission type, choose the ‘Customize’ radio button and then click on the “Edit” button

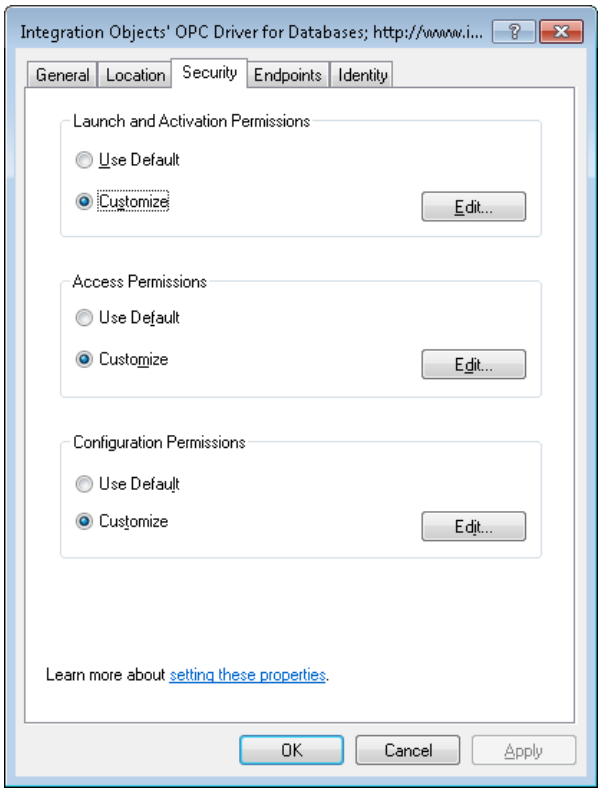



**Figure 12: Security Tab**

#### 5.1.2.1. Launch and Activation Permissions

Click on the "add" button → 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:

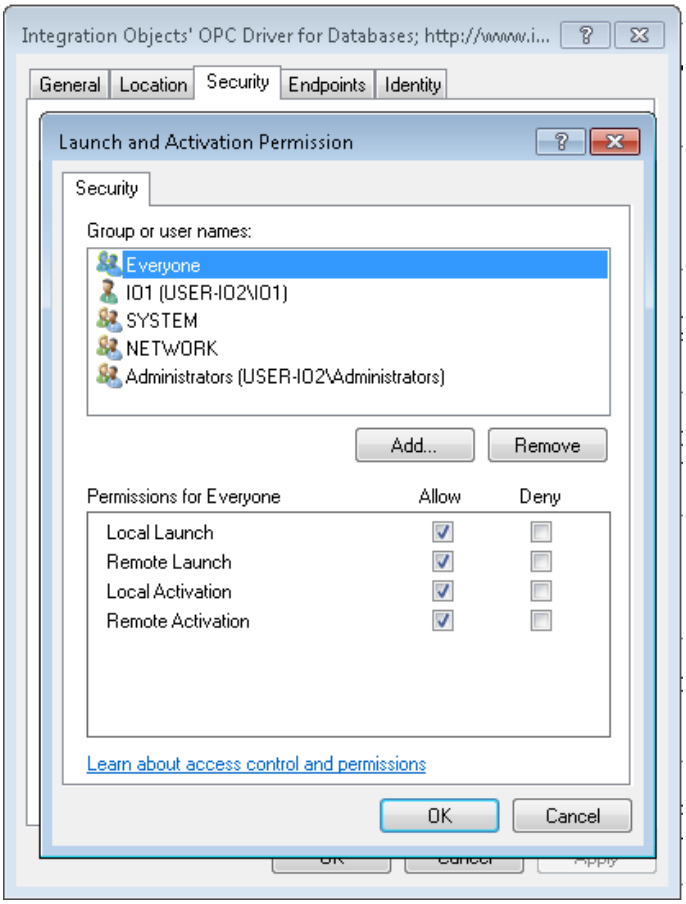



**Figure 13: Launch and Activation permission**

#### 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



customerservice@integrationobjects.com

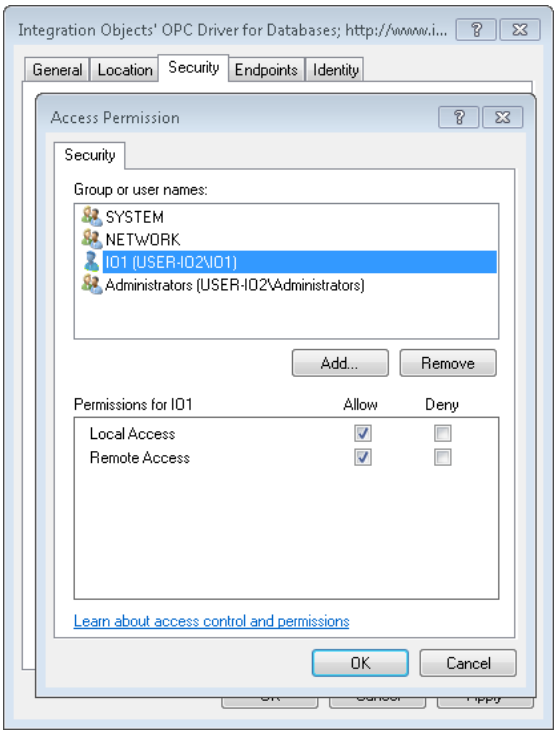



**Figure 14: Access Permission**

#### 5.1.2.3. Configuration Permissions

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

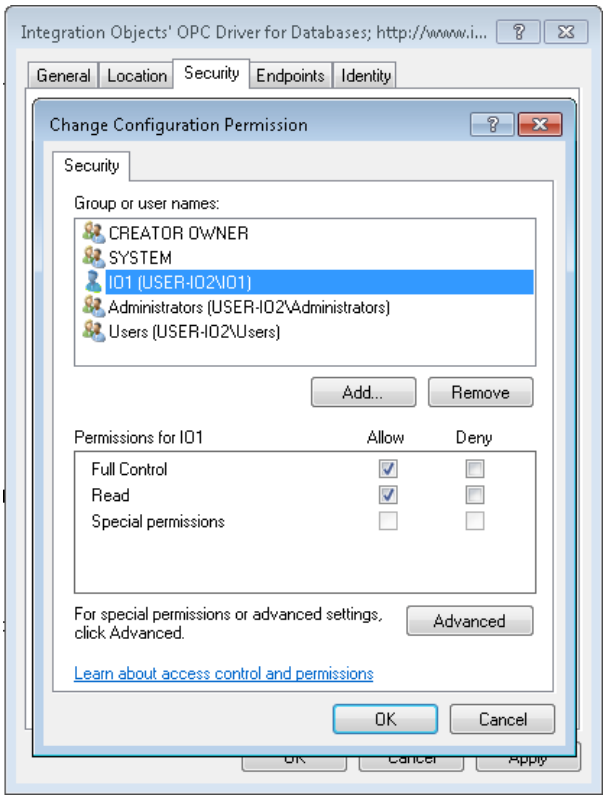



**Figure 15: Change Configuration Permission**

➔ 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.

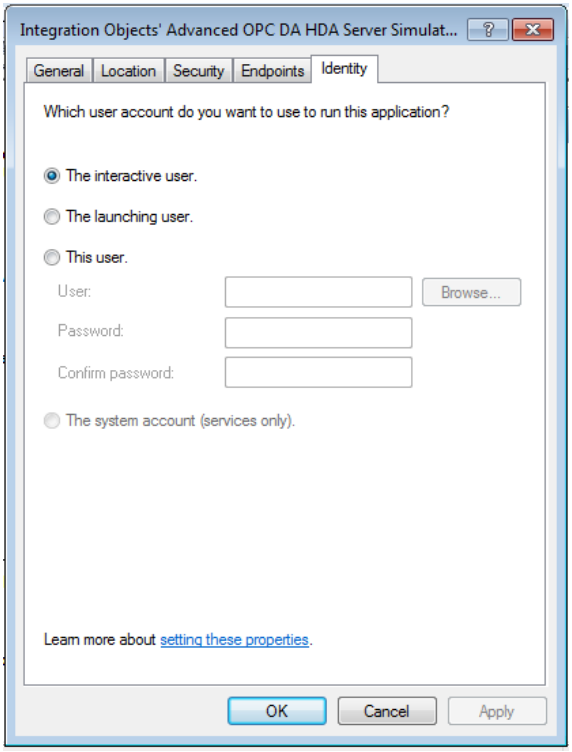



**Figure 16: Identity Rab**

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

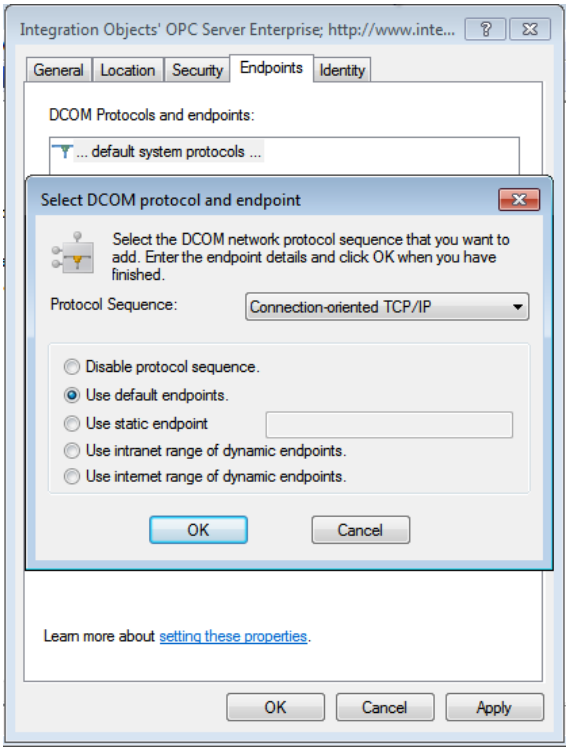



**Figure 17: Endpoints Tab**

### 5.1.3. OPCEnum Configuration

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

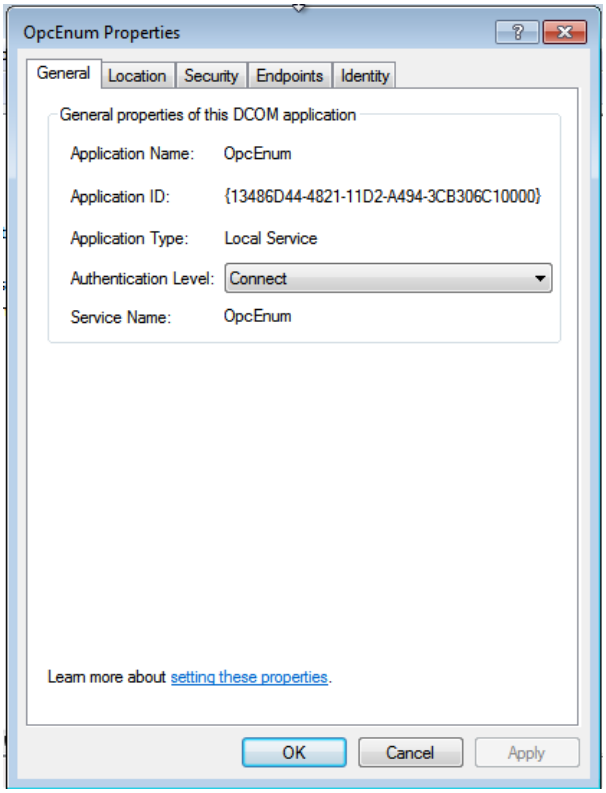



**Figure 18: DCOM OPC Enum - General**

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

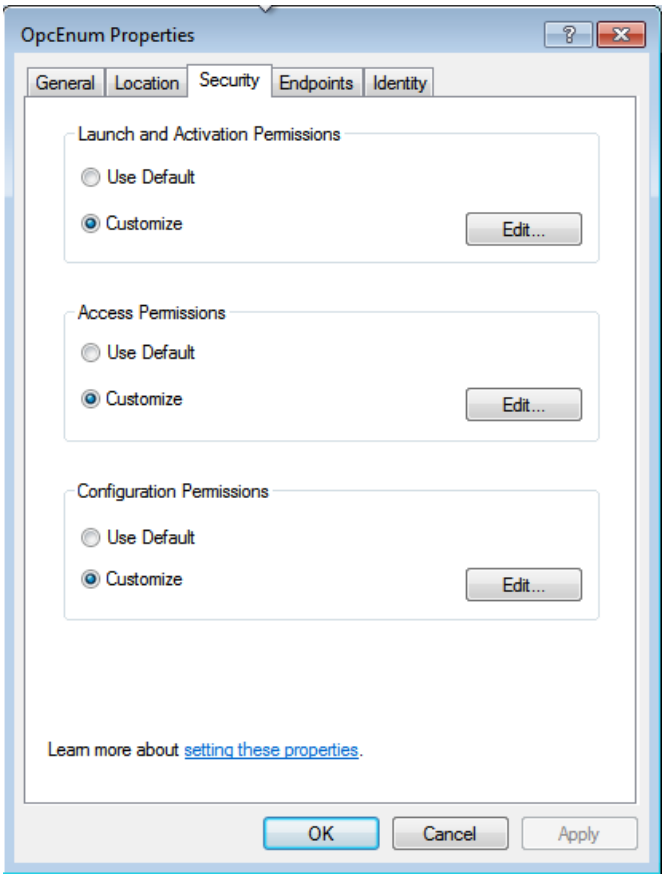



**Figure 19: OPCEnum Security**

#### 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”

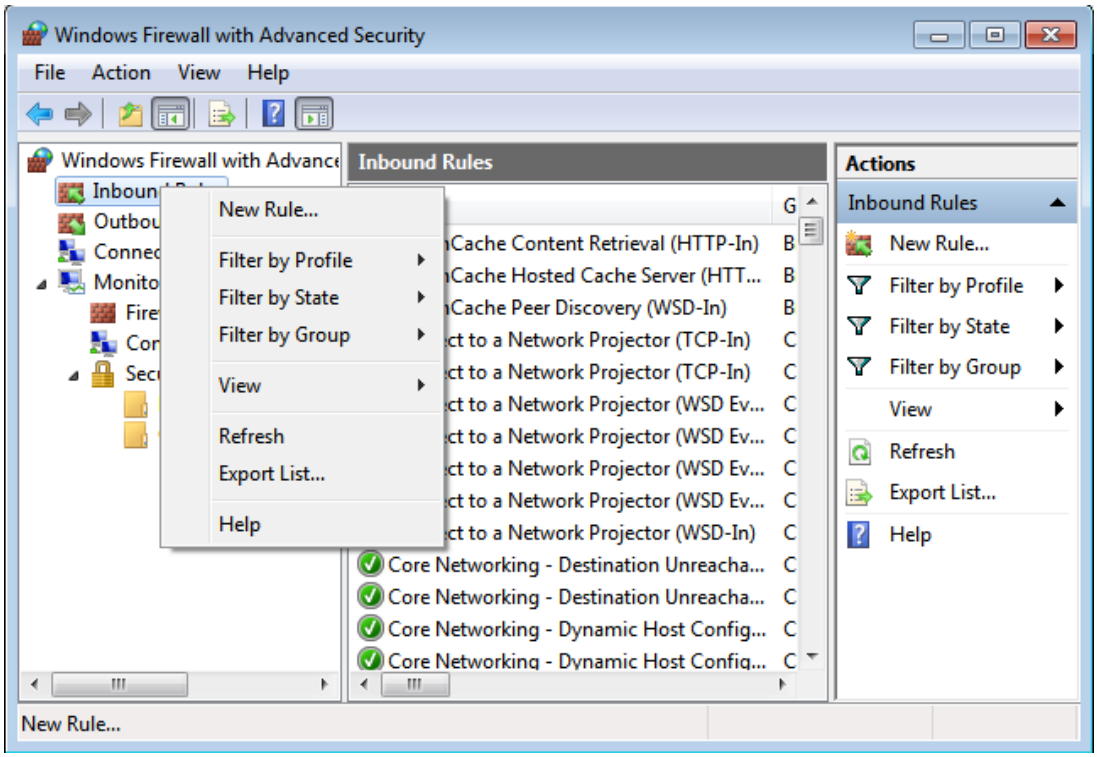



**Figure 20 : New Rule (Client side)**

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

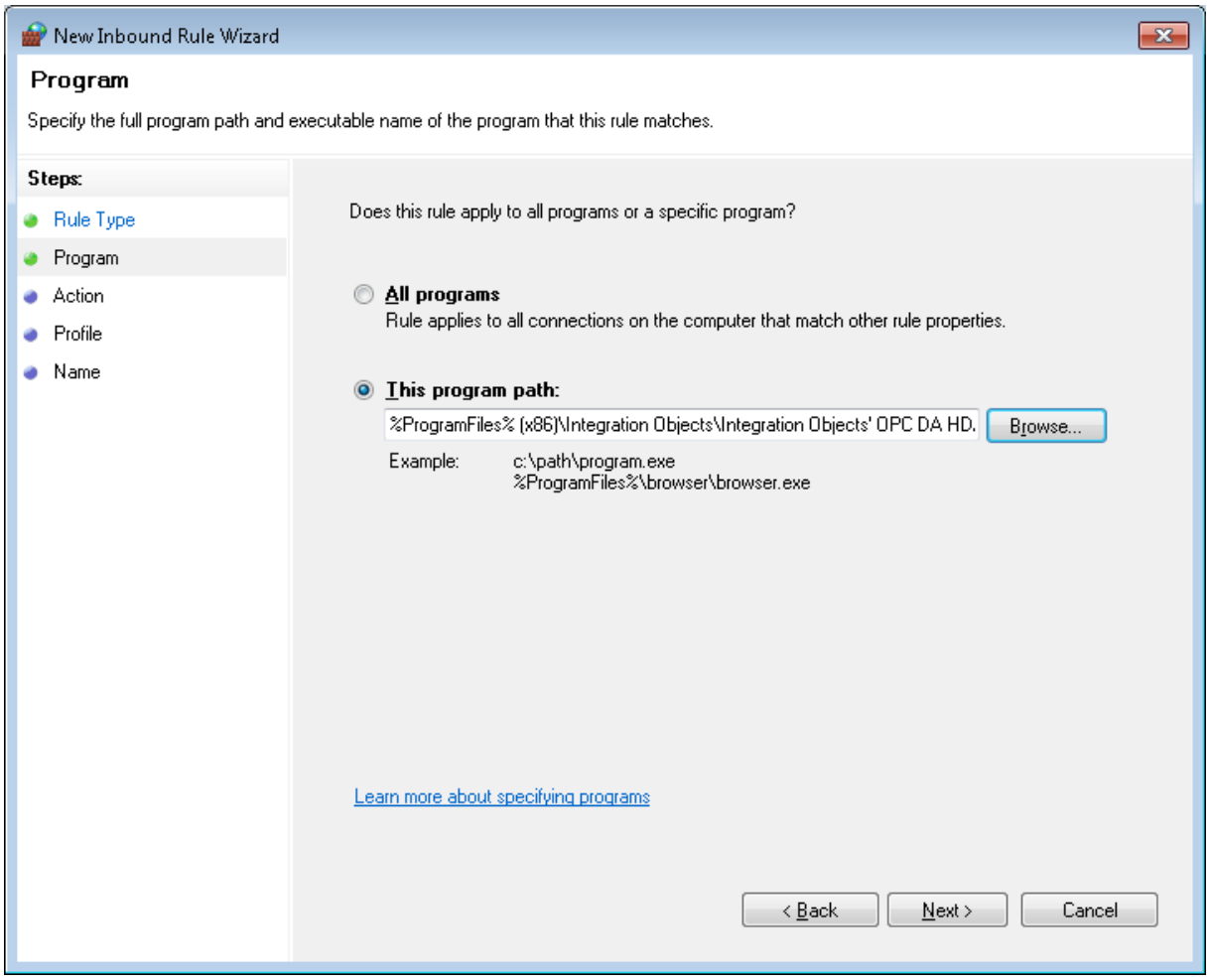



**Figure 21: Add Program (Client side)**

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.

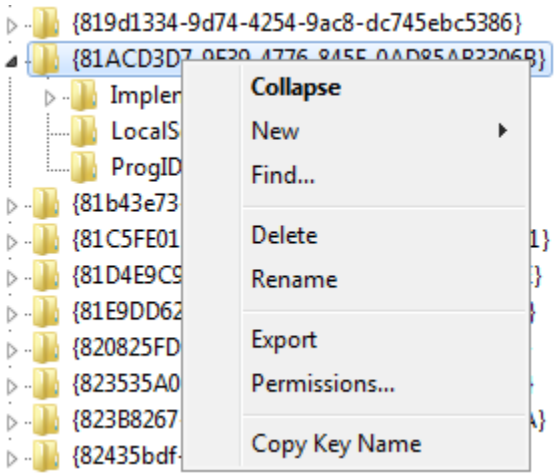



**Figure 22: Export the Server CLSID**

- 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 → AppID and search for your server CLSID.

- Right click on it and Click on “Export”.

✓ 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