OPC XML/DA Client Communication Driver

This document has the specific information related to the driver configuration. For a generic explanation on Devices, Channels, Nodes and Points configuration, please refer to the reference guide.

Contents

Section 1 – Summary Information

Communication Driver Name: OPC XML/DA Client

Implementation DLL: T.ProtocolDriver.OPCXmlDA.dll

Protocol: OPC proprietary

Interface: OPC proprietary

Description: OPC Xml/DA Client implements communication with local and remote OPC servers. The communications blocks are dynamically created according the pooling cycle defined on the Access Type for each Device Point.

OPC servers supported: Any OPC server compatible with OPC Xml/DA v2.05 or v3.0 specifications

Protocol Options: None

Max number of nodes: user defined

PC Hardware requirements: none

PC Software requirements: OPC Core components

> ✍Note:
> You can find the OPC Core components in the OPC Foundation web site.
> http://www.opcfoundation.org/

Section 2 – Channel Configuration

There is no channel configuration for OPC Xml/DA Client channels.

Section 3 – Node Configuration

Station Configuration

Service URL: Defines the location of the OPC Server. Example: OPCDAServer.2, \\192.168.1.201\OPCDAServer.2, http://192.168.1.2:4200

Refresh Rate: Server update rate.

AllItemsSameGroup: Flag indicating whether driver should add all items at the same OPC group and only one connection is created with OPC Server.

EnableReadPolling: Flag indicating whether reading is by polling.

ReadFromDevice: Force all reads made from device.

UseTimestampFromComputer: Use timestamp from computer instead of device.

Section 4 – Point Configuration

Choose the OPCServer item that will communicate with the tag.

You can type the OPC Server item name into the textbox, or you can browse the OPC Server items with the cell editor.

OPC Arrays: You should configure the Array field in Modifiers column.

Section 5 – Troubleshoot

The status of the driver execution can be observed through the diagnostic tools, which are:

- Trace window
- Property Watch
- Module Information

The above tools indicate if the operations have succeeded or have failed, where the status 0 (zero) means success. Negative values are internal error codes and positive values are protocol error codes.

Please, consult your OPC Server documentation for the protocol specific error codes.

Revision History

Revision	Description	Date
A	Initial Revision	January, 2012
B	Created new option "UseTimestampFromComputer"	November, 2014
C	Added DCOM configuration procedure	February, 2021

Append – How to Configure DCOM

1.1 What is DCOM

Distributed Component Object Model (DCOM) is an extension of Component Object Model (COM) that allows COM components to communicate among objects on different computers. DCOM uses Remote Procedure Call (RPC) to generate standard packets that can be shared across a network, which in turn allows COM to communicate beyond the boundaries of the local machine.

Because DCOM poses a security threat, care should be taken to not expose more than what is required for the application. Although multiple security layers exist, it is still possible that some part of the system will be compromised.

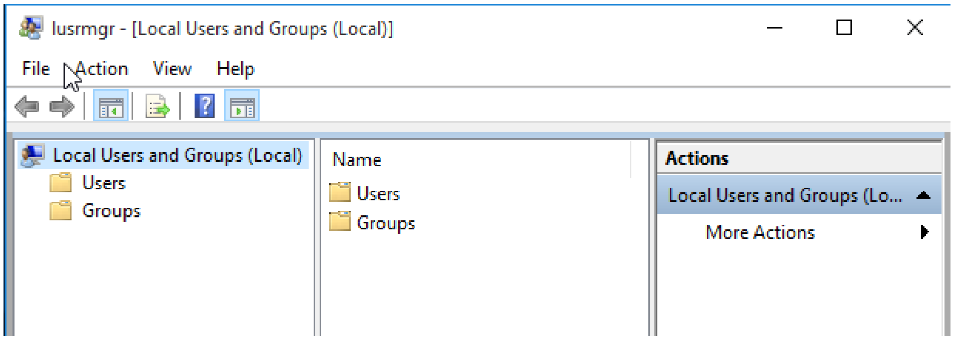
2 Users and Groups

To ensure that an OPC connection is secure, it is suggested the creation of users and groups that are exclusively for this use. These can be manually added by any user who has the proper credentials to do so.

Note: The procedure described below must be executed in both **Client** and **Server** sides. The User created in both computers must have the same name and password.

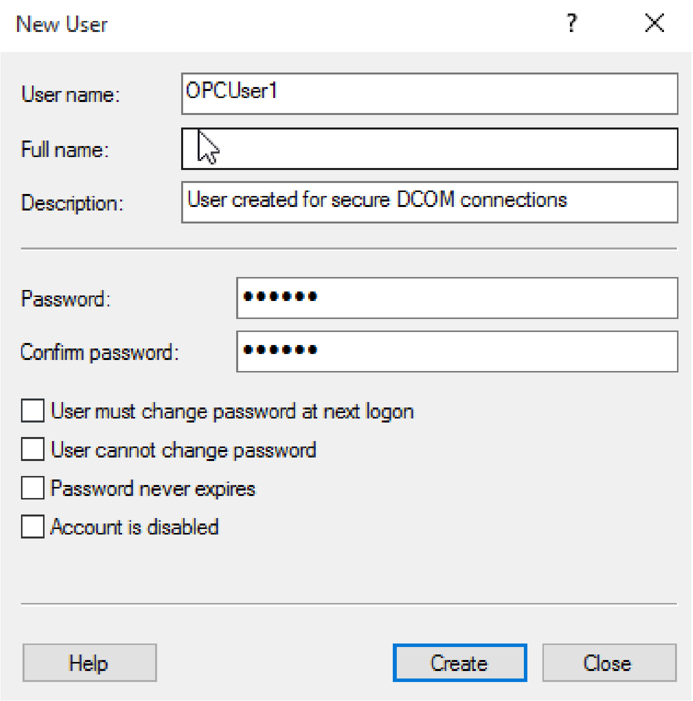
2.1 Adding a Local User

- Launch the **Local User and Groups** snap-in, which is part of the Microsoft Management Console. It can be viewed directly by selecting **WindowsKey + R** and typing '**lusrmgr.msc**'.


lusrmgr - [Local Users and Groups (Local)]
File
Action
View
Help
Local Users and Groups (Local)
Users
Groups
Name
Users
Groups
Actions
Local Users and Groups (Lo...
More Actions

Adding Local User.

- Next, click **Users**. Then, select **Action** > **New User**.



User name: OPCUser1

Full name:

Description: User created for secure DCOM connections

Password: ••••••

Confirm password: ••••••

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

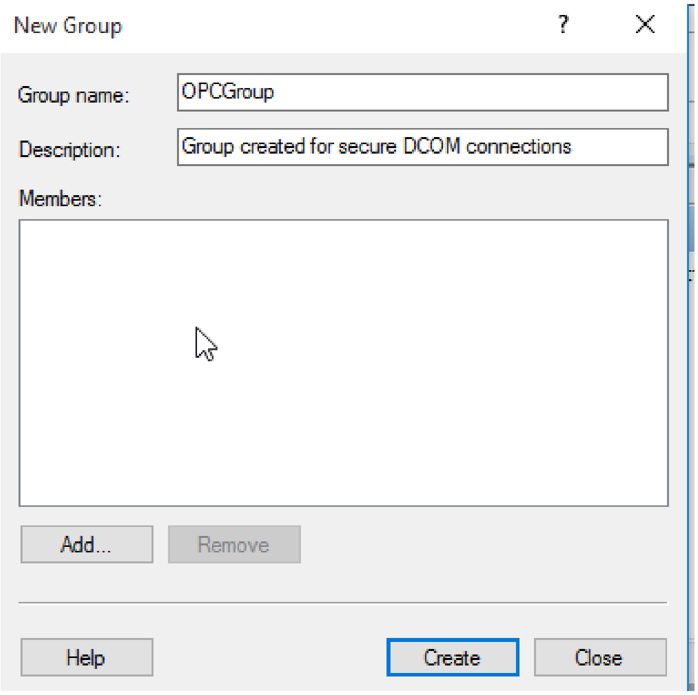
Adding Local User.

- Type the appropriate information in the dialog box.
- Change the following options as required:
  - User must change password at next logon;
  - User cannot change password;
  - Password never expires;
  - Account is disabled.
- Click **Create**. Then, click **Close**.

2.2 Adding a Local Group

- Launch the **Local User and Groups** snap-in, which is part of the Microsoft Management Console. It can be viewed directly by selecting **WindowsKey+R** and typing ‘**lusrmgr.msc**’.

  Click **Groups** and then select **Action** > **NewGroup**.



New Group

Group name: OPCGroup

Description: Group created for secure DCOM connections

Members:

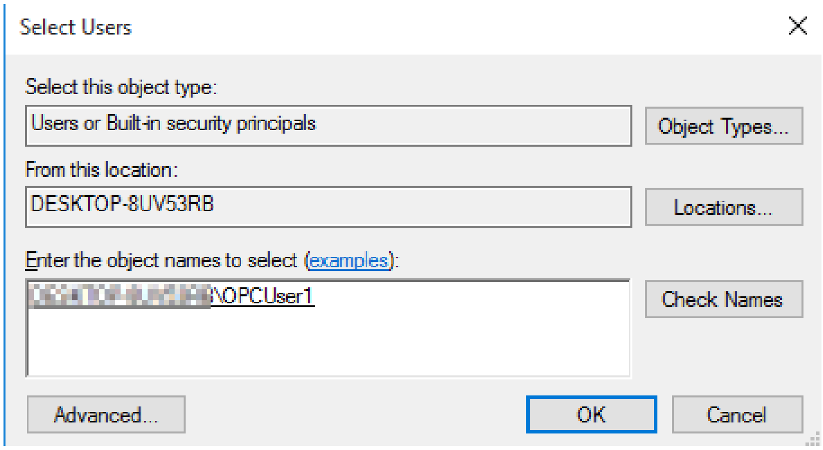
Adding Local Group.

- In **Group Name**, type a name for the new group.
- In **Description**, type a description of the new group.
- Click **Create** and then **Close**.

2.3 Adding Users to a Group

- Launch the **Local User and Groups** snap-in.

  Next, select **Groups** and right-click on the group in which a member will be added and select **All Tasks**. Click **Add to Group** > **Add**.



Select this object type:
Users or Built-in security principals

From this location:
DESKTOP-8UV53RB

Enter the object names to select (examples):
[redacted]\OPCUser1

Adding Users to Group.

- In **Object Types**, select the types of objects to find.
- In **Locations**, click the domain or the computer that contains the users to add. Then, click **OK**.
- Type the name of the user or group that will be added to the group and then click **OK**. To validate the user or group names being added, click **Check Names**.

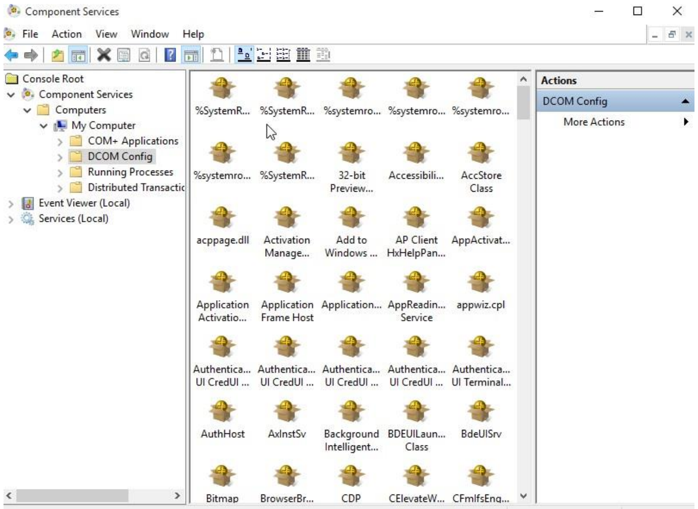
3 DCOM Configuration

The computer running the OPC server must make changes to the application and system levels to setup DCOM correctly.

3.1 Configuring the Application

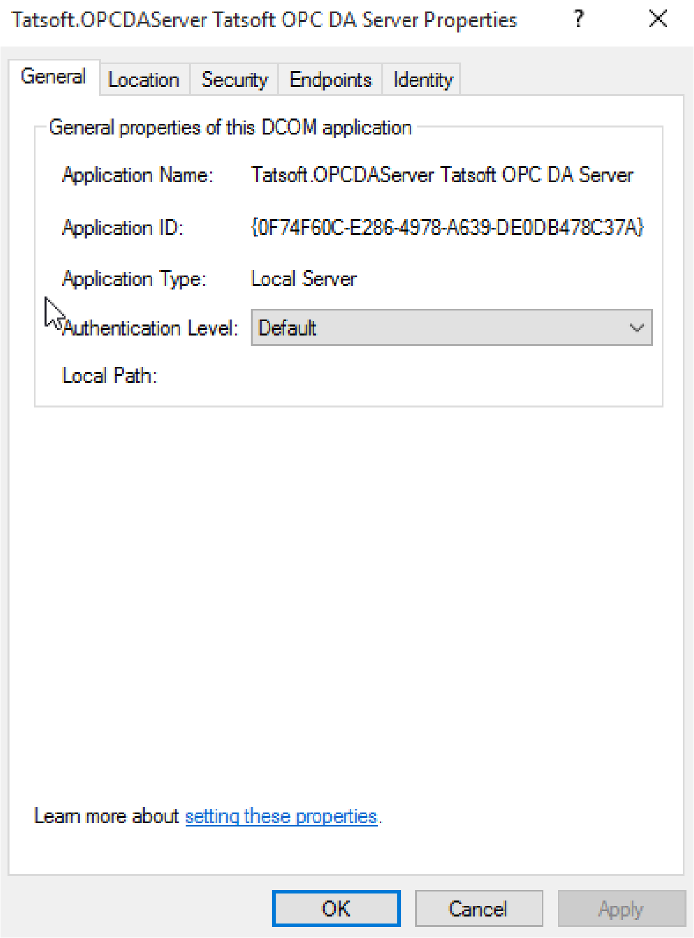
- Launch the **Component Services** snap-in, which is part of the Microsoft Management Con- sole. It can be viewed directly by selecting **Windows Key + R** and then typing '**dcomcnfg**'.

  Under **Console Root**, go to **Component Servers** > **Computers** > **My Computer** > **DCOM Config**.



DCOM Configuration.

- Browse the DCOM enabled objects until the OPC server application is located. In this example, '**Tatsoft OPC DA Server**' is displayed where the actual application name will appear.
- Right-click on the server application and select **Properties**.
- Open the **General** tab, then verify that the **Authentication Level** is set to **Default**.



Tatsoft.OPCDAServer Tatsoft OPC DA Server Properties

General properties of this DCOM application

Application Name: Tatsoft.OPCDAServer Tatsoft OPC DA Server

Application ID: {0F74F60C-E286-4978-A639-DE0DB478C37A}

Application Type: Local Server

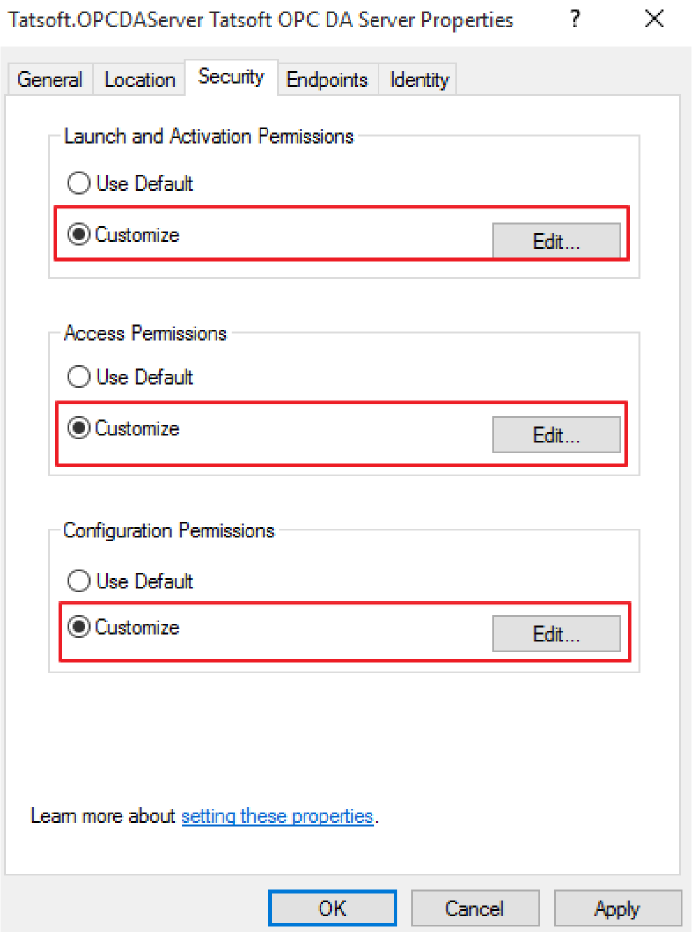
Authentication Level: Default

Local Path:

Learn more about setting these properties.

DCOM Configuration.

- Open the **Security** tab.



Tatsoft.OPCDAServer Tatsoft OPC DA Server Properties

Launch and Activation Permissions

○ Use Default

● Customize

Access Permissions

○ Use Default

● Customize

Configuration Permissions

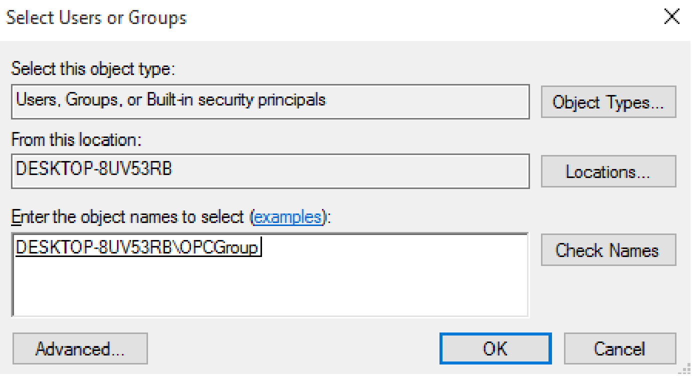
○ Use Default

● Customize

Learn more about setting these properties.

DCOM Configuration.

- In **Launch and Activation Permissions**, select **Customize**. Here, users and groups can be granted permission to start the OPC server if it is not already running.
- Click **Edit**.
- In **Launch and Activation Permissions**, select **Add**



Select Users or Groups

Select this object type:

Users, Groups, or Built-in security principals

From this location:

DESKTOP-8UV53RB

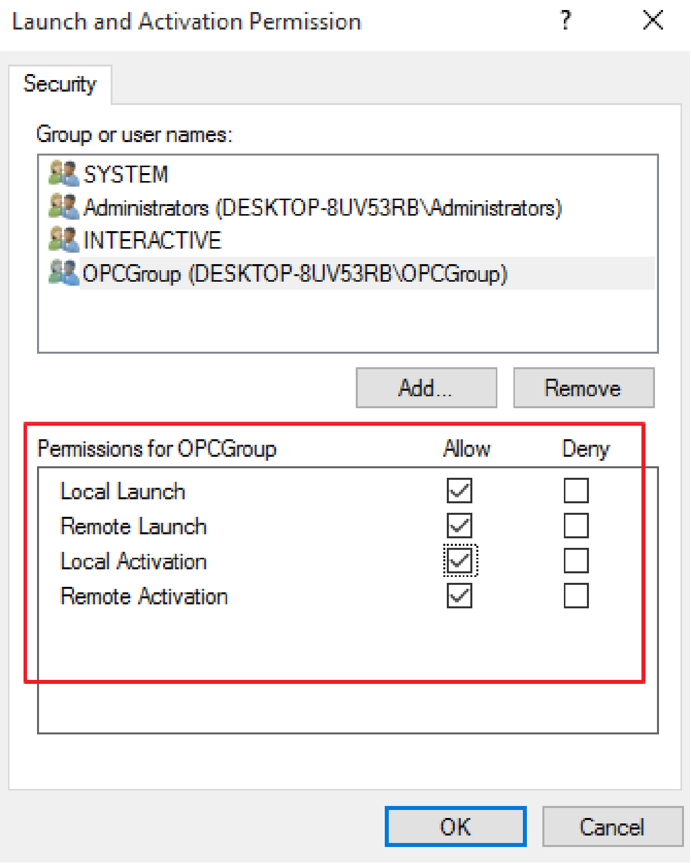
Enter the object names to select (examples):

DESKTOP-8UV53RB\OPCGroup

DCOM Configuration.

- In **Object Types**, select the desired object type.

- In **Locations**, click the domain or the computer that contains the users or groups that will be added. Then, click **OK**.
- Type the name of the user or group in the window. To validate the user or group names being added, click **Check Names**.
- After the account has been validated, click **OK**.
- Continue to add users and groups until all the desired accounts have been added. The new account or group should be visible in the G**roup or user names** list.
- Next, select the new user or group.



Group or user names:

- SYSTEM
- Administrators (DESKTOP-8UV53RB\Administrators)
- INTERACTIVE
- OPCGroup (DESKTOP-8UV53RB\OPCGroup)

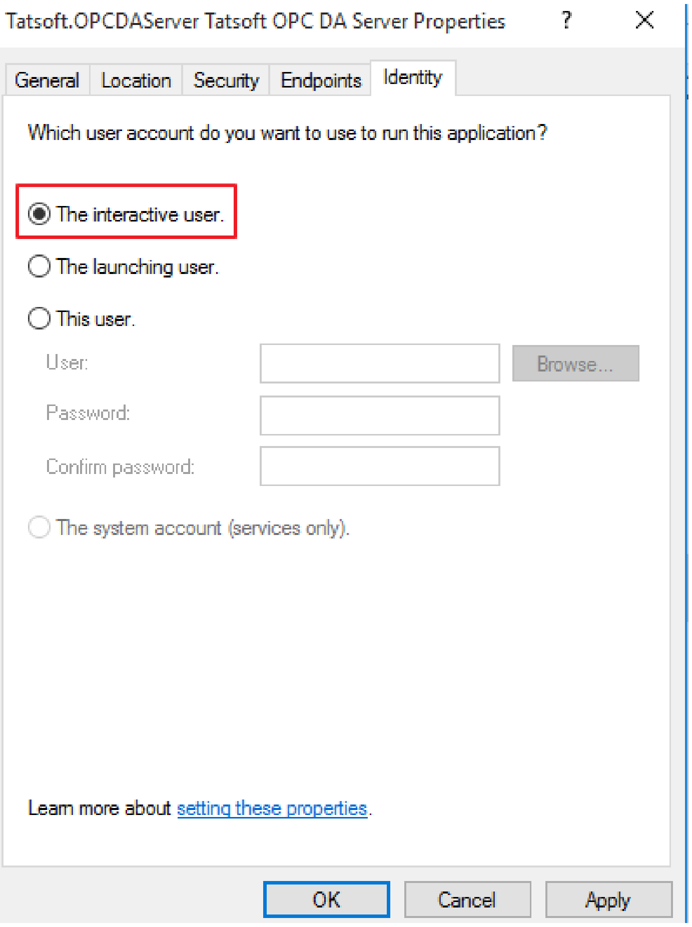
Permissions for OPCGroup	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

DCOM Configuration.

Note: To only allow local applications to connect, only enable the local permissions for the account. In this example, local and remote permissions are enabled.

- Repeat the process for all accounts that have been added. Click **OK**.
- Select **Customize** in the **Access Permissions** group. Here, users and groups can be granted permissions to make calls to the OPC server. These calls include browsing for items, adding groups and items, or any other standard OPC call. Click **Edit**.
- Repeat the same procedure for **Access Permissions** option.

- Browse to **Identity** tab and select **The interactive user** option.



Tatsoft.OPCDAServer Tatsoft OPC DA Server Properties

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:

Password:

Confirm password:

○ The system account (services only).

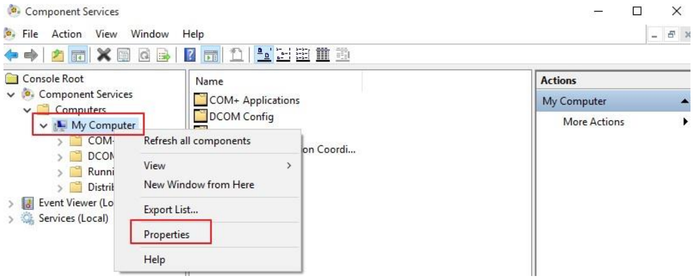
Learn more about setting these properties.

DCOM Configuration.

- Select **OK** to close the **Server Properties**.

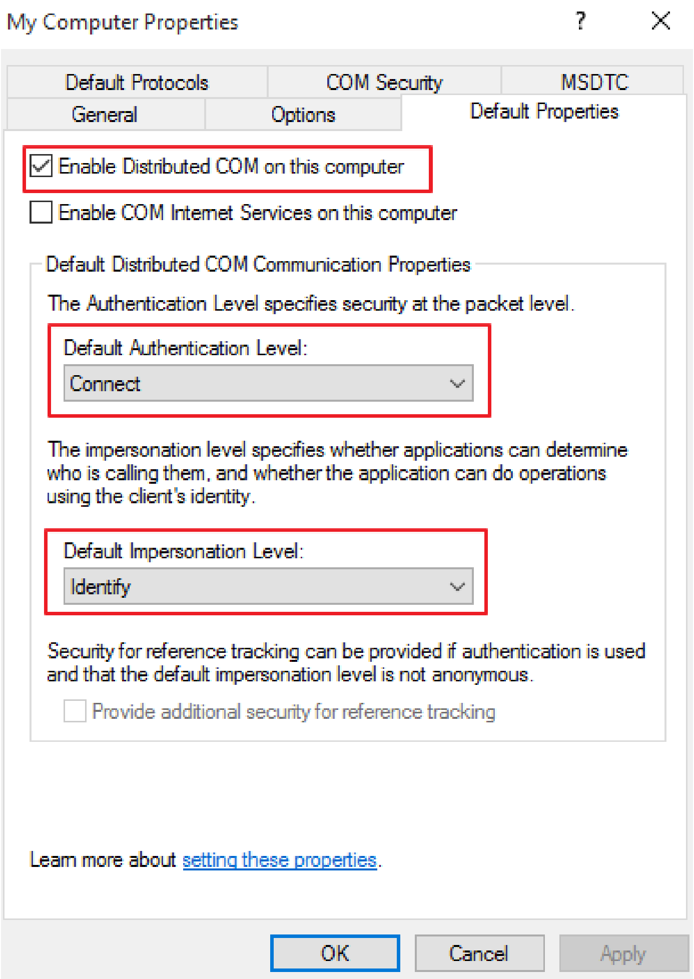
3.2 Configuring the System

- Under **Component Services** snap-in, go to **Console Root** > **Component Services** > **Computers**, right-click on **My Computer** and select **Properties**.



Configuring the System.

- Select the **Default Properties** tab and verify that the **Enable Distributed COM on this computer** option is enabled.
- Select **Connect** for the **Default Authentication Level**.
- Select **Identify** for the **Default Impersonation Level**.



☑ Enable Distributed COM on this computer

□ Enable COM Internet Services on this computer

Default Distributed COM Communication Properties

The Authentication Level specifies security at the packet level.

Default Authentication Level:
Connect

The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity.

Default Impersonation Level:
Identify

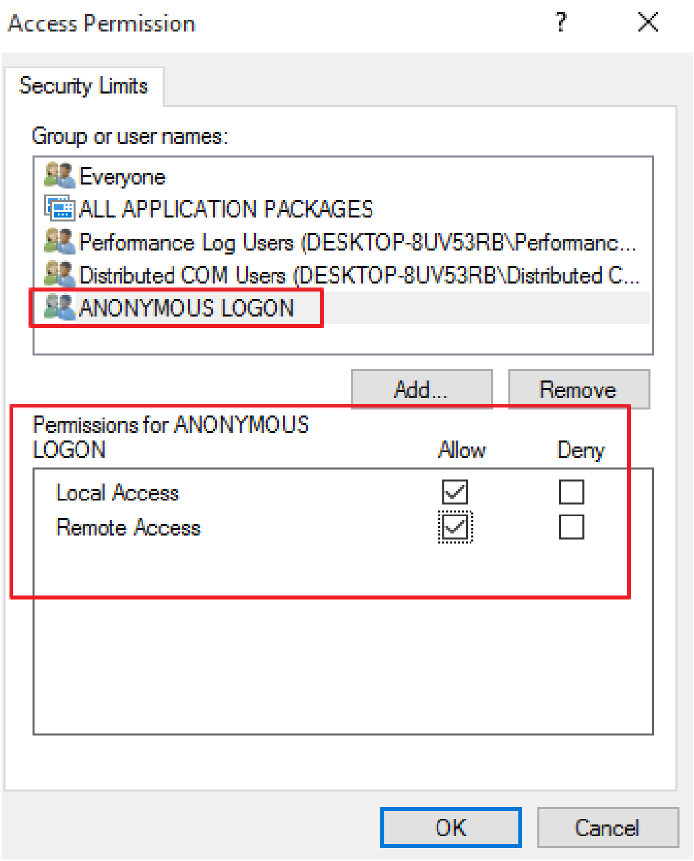
Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous.

□ Provide additional security for reference tracking

Learn more about setting these properties.

Configuring the System.

- Select the **COM Security** tab.
- Select **Edit Limits** in the **Access Permissions** group.
- Select the **ANONYMOUS LOGON** group account in the Group or user names list.



Access Permission

Security Limits

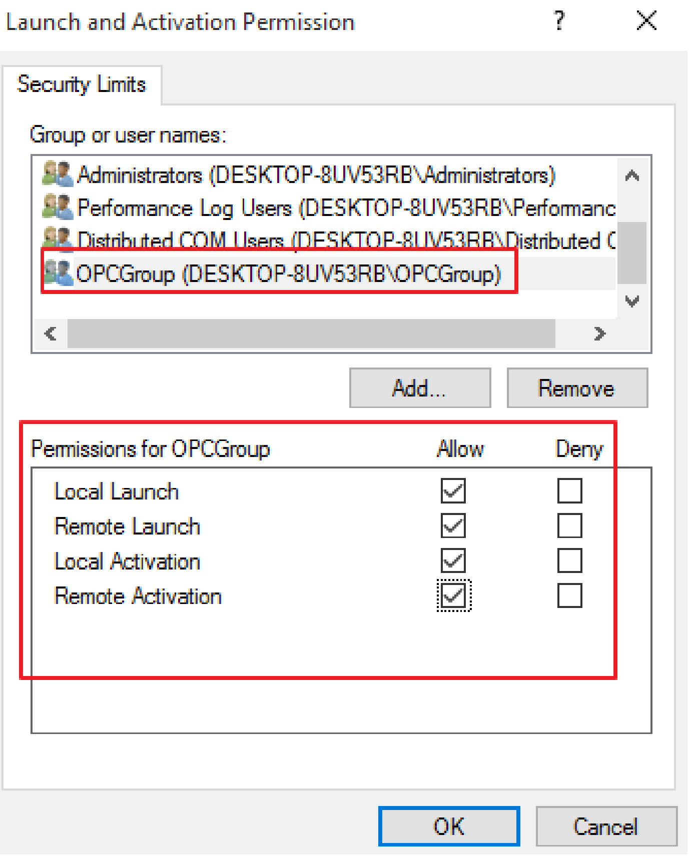
Group or user names:

- Everyone
- ALL APPLICATION PACKAGES
- Performance Log Users (DESKTOP-8UV53RB\Performanc...
- Distributed COM Users (DESKTOP-8UV53RB\Distributed C...
- ANONYMOUS LOGON

Permissions for ANONYMOUS LOGON	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

Configuring the System.

- In the **Launch and Activation Permissions** group, select **Edit Limits**.
- Add the created OPC Group to the Groups list.
- Next, select the new user or group and **allow** the permissions.



Group or user names:

- Administrators (DESKTOP-8UV53RB\Administrators)
- Performance Log Users (DESKTOP-8UV53RB\Performanc
- Distributed COM Users (DESKTOP-8UV53RB\Distributed C
- OPCGroup (DESKTOP-8UV53RB\OPCGroup)

Permissions for OPCGroup	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

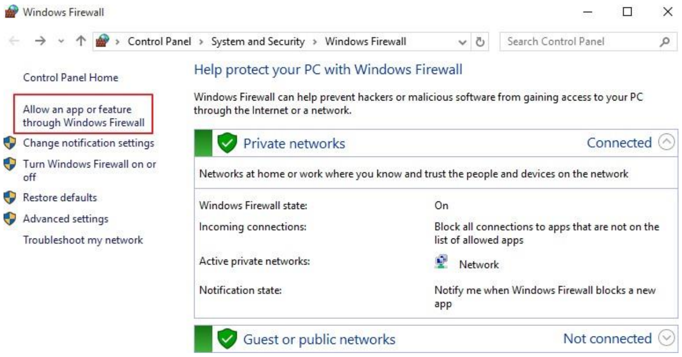
Configuring the System.

Note: Restart the computer to apply the changes.

4 Firewall Configuration

In some cases, it is easier to turn off any firewalls that may be running on both the client and server machine before DCOM is setup. Once a connection has been successfully created, it is recommended that the firewall security is restored and the correct exceptions are added.

- Launch the Windows Firewall by selecting **Windows Key + R** and then typing '**firewall.cpl**'.
- Browse to '**Allow an app or feature through Windows Firewall**'.



Windows Firewall
Control Panel › System and Security › Windows Firewall
Search Control Panel
Control Panel Home
Allow an app or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Connected

Networks at home or work where you know and trust the people and devices on the network

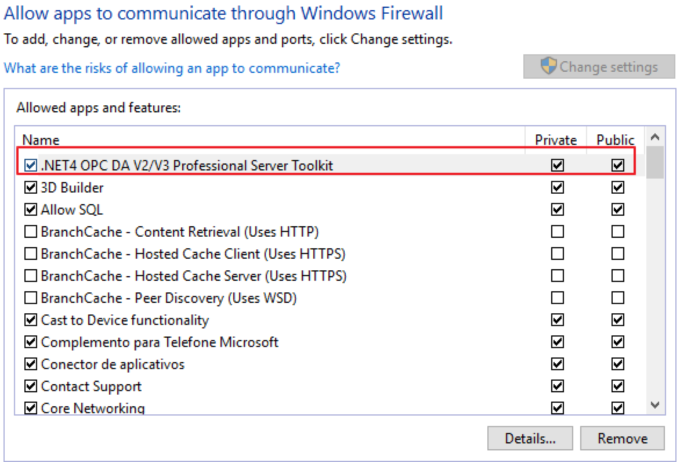
Windows Firewall state:	On
Incoming connections:	Block all connections to apps that are not on the list of allowed apps
Active private networks:	Network
Notification state:	Notify me when Windows Firewall blocks a new app

Guest or public networks — Not connected

Configuring the Firewall.

- Click on **Allow another app** and browse for the file named **DANSrvNet4.exe** that is usually located at:

$$C:\backslash ProgramFiles(x86)\backslash < CompanyName > \backslash < ProductName > \backslash < ProductVersion >$$



Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

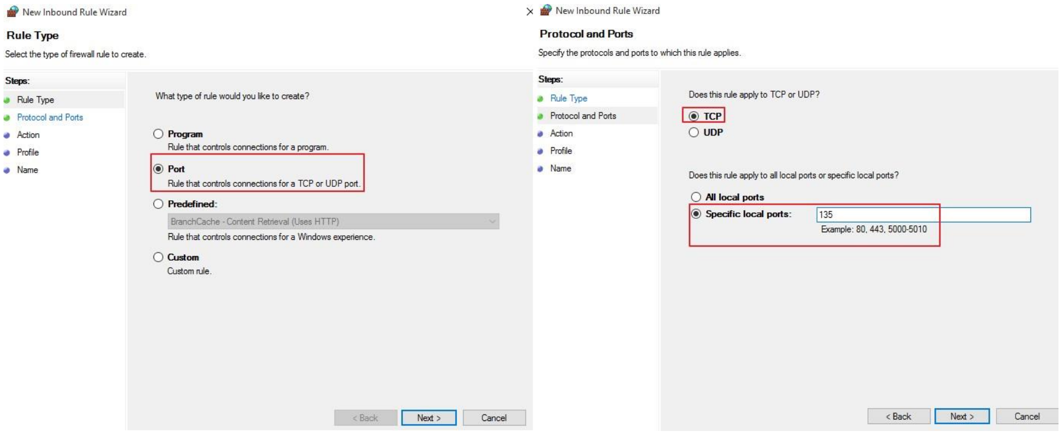
Allowed apps and features:

Name	Private	Public
☑ .NET4 OPC DA V2/V3 Professional Server Toolkit	☑	☑
☑ 3D Builder	☑	☑
☑ Allow SQL	☑	☑
□ BranchCache - Content Retrieval (Uses HTTP)	□	□
□ BranchCache - Hosted Cache Client (Uses HTTPS)	□	□
□ BranchCache - Hosted Cache Server (Uses HTTPS)	□	□
□ BranchCache - Peer Discovery (Uses WSD)	□	□
☑ Cast to Device functionality	☑	☑
☑ Complemento para Telefone Microsoft	☑	☑
☑ Conector de aplicativos	☑	☑
☑ Contact Support	☑	☑
☑ Core Networking	☑	☑

Configuring the Firewall.

The steps below must be executed on both **Client** and **Server** sides.

- Click on **Advanced Settings**, right-click on **Inbound Rules** and select **add new rule**.
- Select **Port** and click on Next.
- Apply the rule for **TCP** connections, and enter the port number 135.
- Select **Allow the connection** and click on next.
- Choose the domains that best suit your case.
- Enter a friendly name and description for the new rule.
- Repeat the procedure for **Outbound Rules** tab.



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:** 135
Example: 80, 443, 5000-5010

Configuring the Firewall.

Note: TCP Port 135 is commonly used for allowing clients to discover and utilize a DCOM service.