Asset Graphics / inVISU PMS

Security setting for OPC

Windows 7, 8, 10, Server 2008, Server 2012, Server 2016

Introduction

OPC DA (data access) communication is based on COM and DCOM. COM is used to communicate other over the same machine.

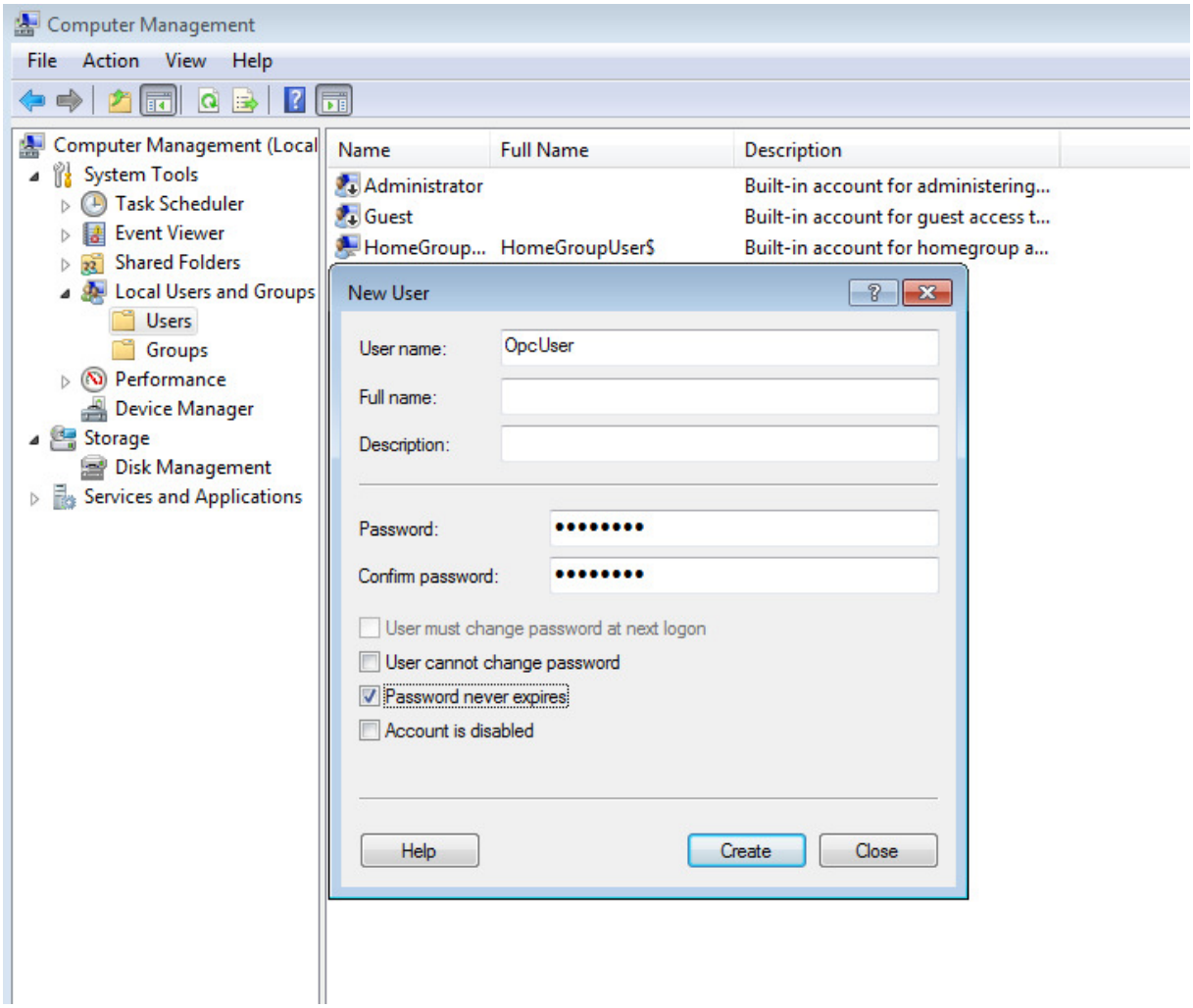
Several configuration steps are necessary to allow OPC clients to connect to OPC servers over network. This document describes these steps.

It is necessary to create users with the same name and password on the server and client computer. These users have to be enabled to launch and use DCOM applications. OPC clients have to run using one of these special users.

If it is not possible to launch the OPC Server and Client with the same user account, you have to use so called OPC tunneling or bridge software.

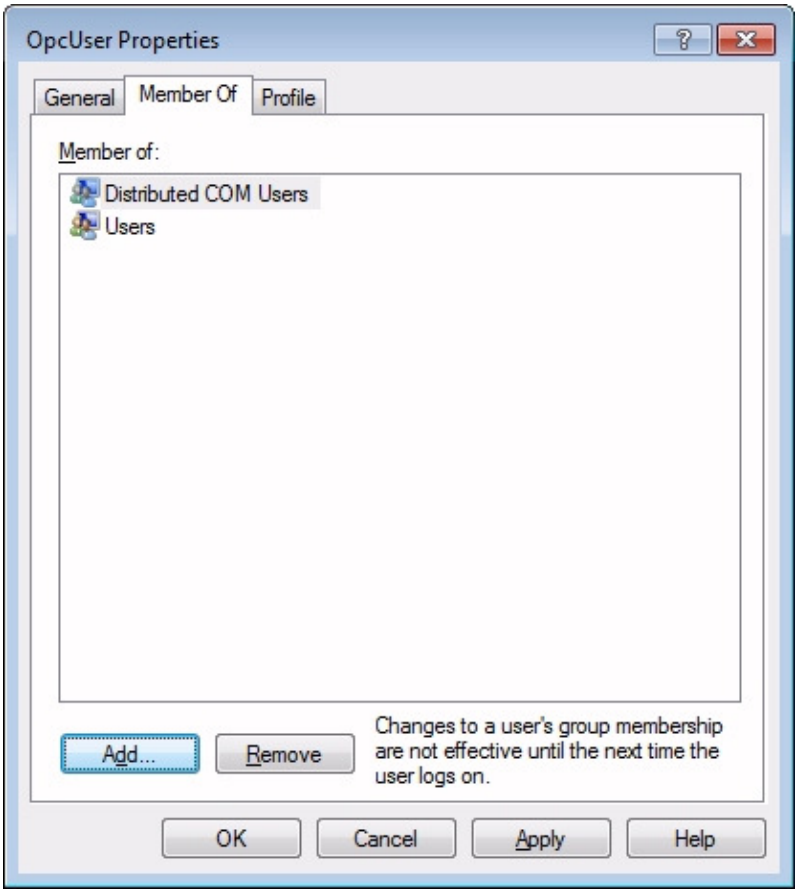
1. User Settings

In this tutorial we create a new user, called **OpcUser**.



Note An empty password is not allowed.

Make **OpcUser** a member of the group **Distributed COM Users**.

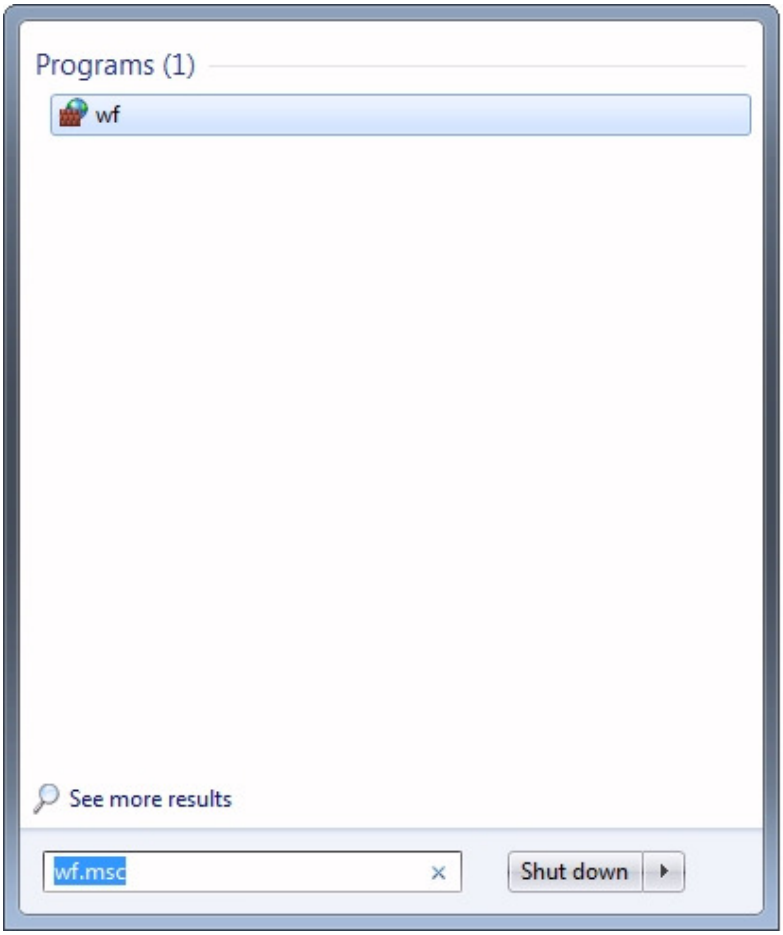


2. Firewall

The OPC technology is based on the DCOM technology which uses the system port 135 for its work. Only if OPC server and clients are running on different computers, you have to configure the Windows firewall.

1. Start the firewall configuration

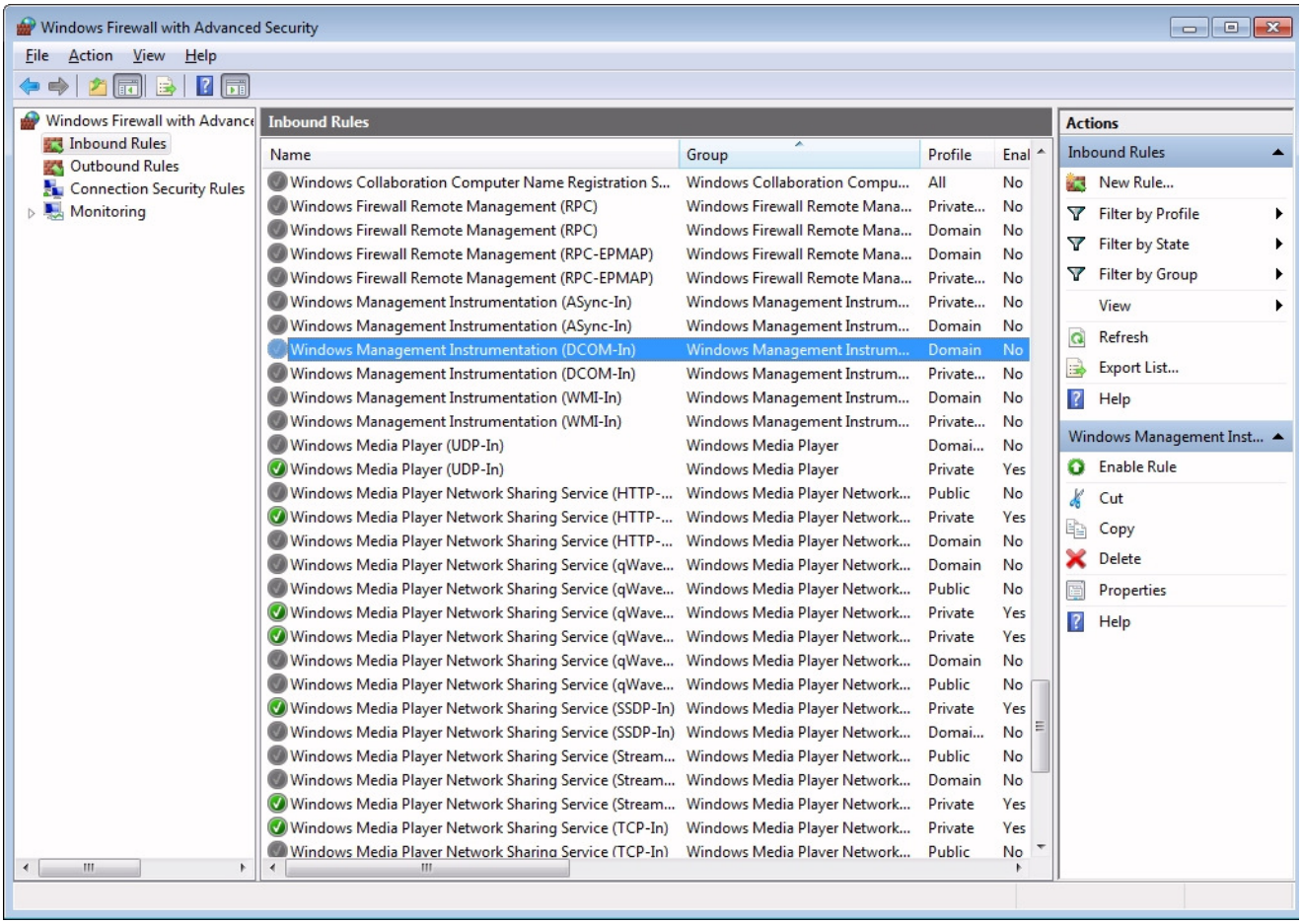
Enter **wf.msc** in the command prompt to open the firewall configuration.



2. Enable network access to DCOM.

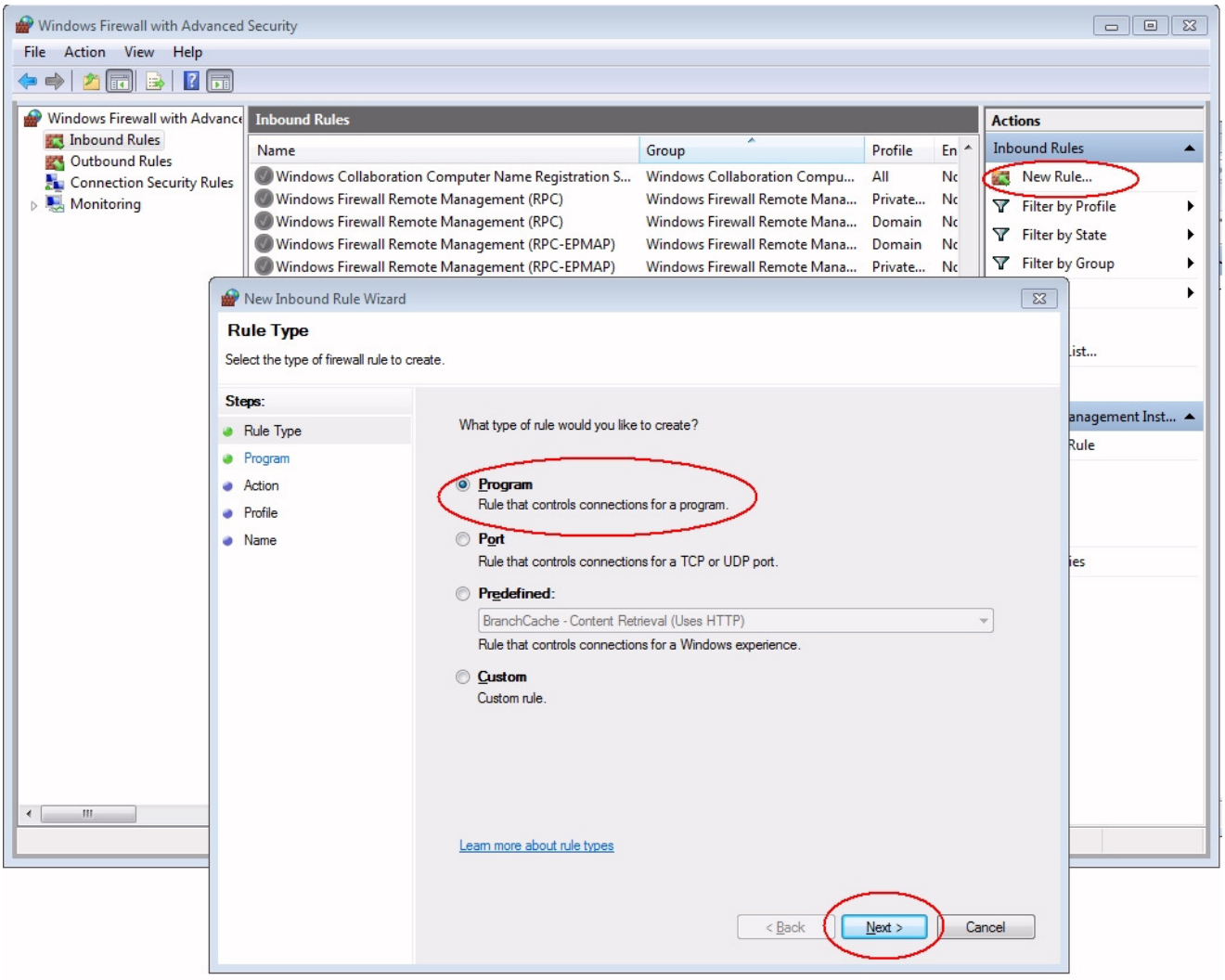
By default DCOM network traffic is blocked.

Right-click on the pre-defined inbound rule **Windows Management Instrumentation (DCOM-In)** and enable it.


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Inbound Rules
Name
Group
Profile
Enal
Windows Collaboration Computer Name Registration S... Windows Collaboration Compu... All No
Windows Firewall Remote Management (RPC) Windows Firewall Remote Mana... Private... No
Windows Firewall Remote Management (RPC) Windows Firewall Remote Mana... Domain No
Windows Firewall Remote Management (RPC-EPMAP) Windows Firewall Remote Mana... Domain No
Windows Firewall Remote Management (RPC-EPMAP) Windows Firewall Remote Mana... Private... No
Windows Management Instrumentation (ASync-In) Windows Management Instrum... Private... No
Windows Management Instrumentation (ASync-In) Windows Management Instrum... Domain No
Windows Management Instrumentation (DCOM-In) Windows Management Instrum... Domain No
Windows Management Instrumentation (DCOM-In) Windows Management Instrum... Private... No
Windows Management Instrumentation (WMI-In) Windows Management Instrum... Domain No
Windows Management Instrumentation (WMI-In) Windows Management Instrum... Private... No
Windows Media Player (UDP-In) Windows Media Player Domai... No
Windows Media Player (UDP-In) Windows Media Player Private Yes
Windows Media Player Network Sharing Service (HTTP-... Windows Media Player Network... Public No
Windows Media Player Network Sharing Service (HTTP-... Windows Media Player Network... Private Yes
Windows Media Player Network Sharing Service (HTTP-... Windows Media Player Network... Domain No
Windows Media Player Network Sharing Service (qWave... Windows Media Player Network... Domain No
Windows Media Player Network Sharing Service (qWave... Windows Media Player Network... Public No
Windows Media Player Network Sharing Service (qWave... Windows Media Player Network... Private Yes
Windows Media Player Network Sharing Service (qWave... Windows Media Player Network... Private Yes
Windows Media Player Network Sharing Service (qWave... Windows Media Player Network... Domain No
Windows Media Player Network Sharing Service (qWave... Windows Media Player Network... Public No
Windows Media Player Network Sharing Service (SSDP-In) Windows Media Player Network... Private Yes
Windows Media Player Network Sharing Service (SSDP-In) Windows Media Player Network... Domai... No
Windows Media Player Network Sharing Service (Stream... Windows Media Player Network... Public No
Windows Media Player Network Sharing Service (Stream... Windows Media Player Network... Domain No
Windows Media Player Network Sharing Service (Stream... Windows Media Player Network... Private Yes
Windows Media Player Network Sharing Service (TCP-In) Windows Media Player Network... Private Yes
Windows Media Player Network Sharing Service (TCP-In) Windows Media Player Network... Public No
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
Windows Management Inst...
Enable Rule
Cut
Copy
Delete
Properties
Help

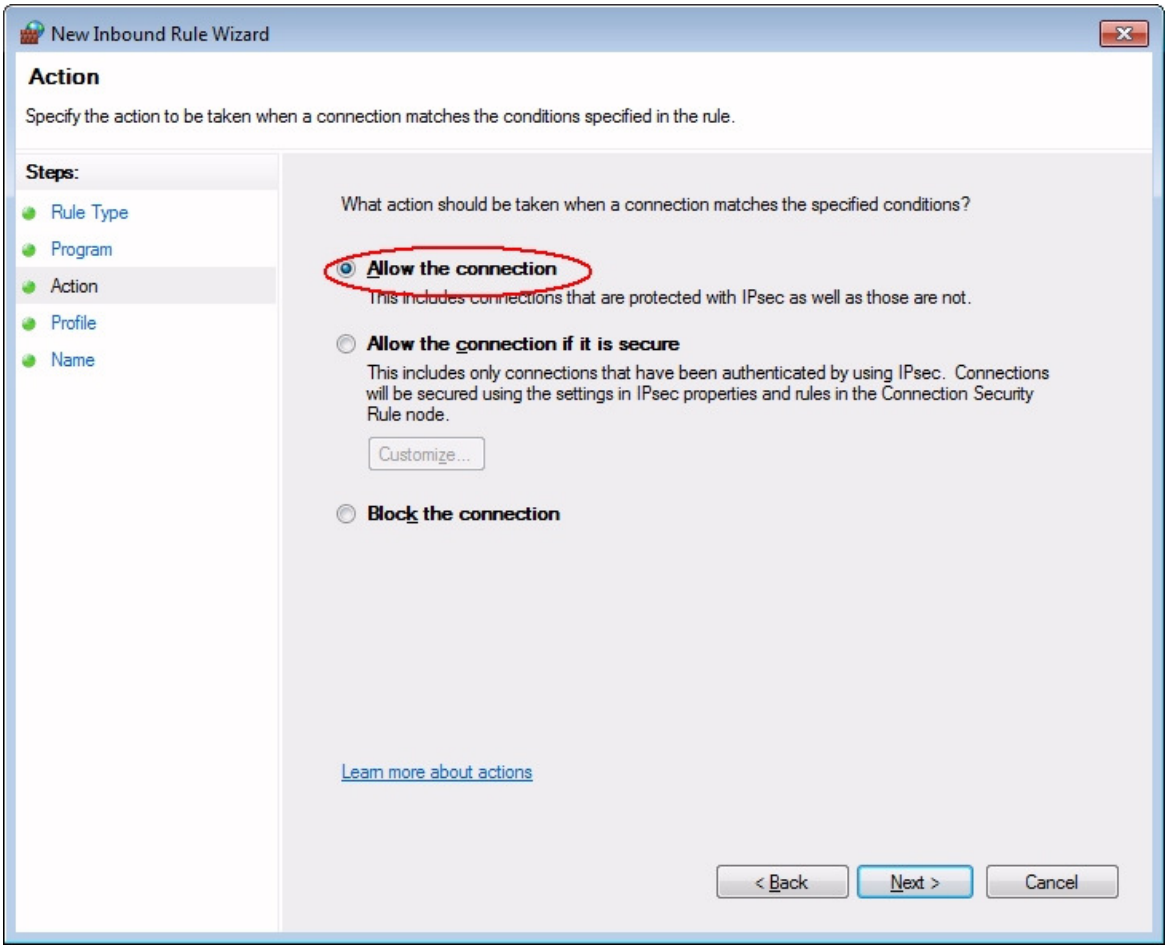
3. Enable **OpcEnum**

Press **New Rule…**, select **Program** and click **Next**.

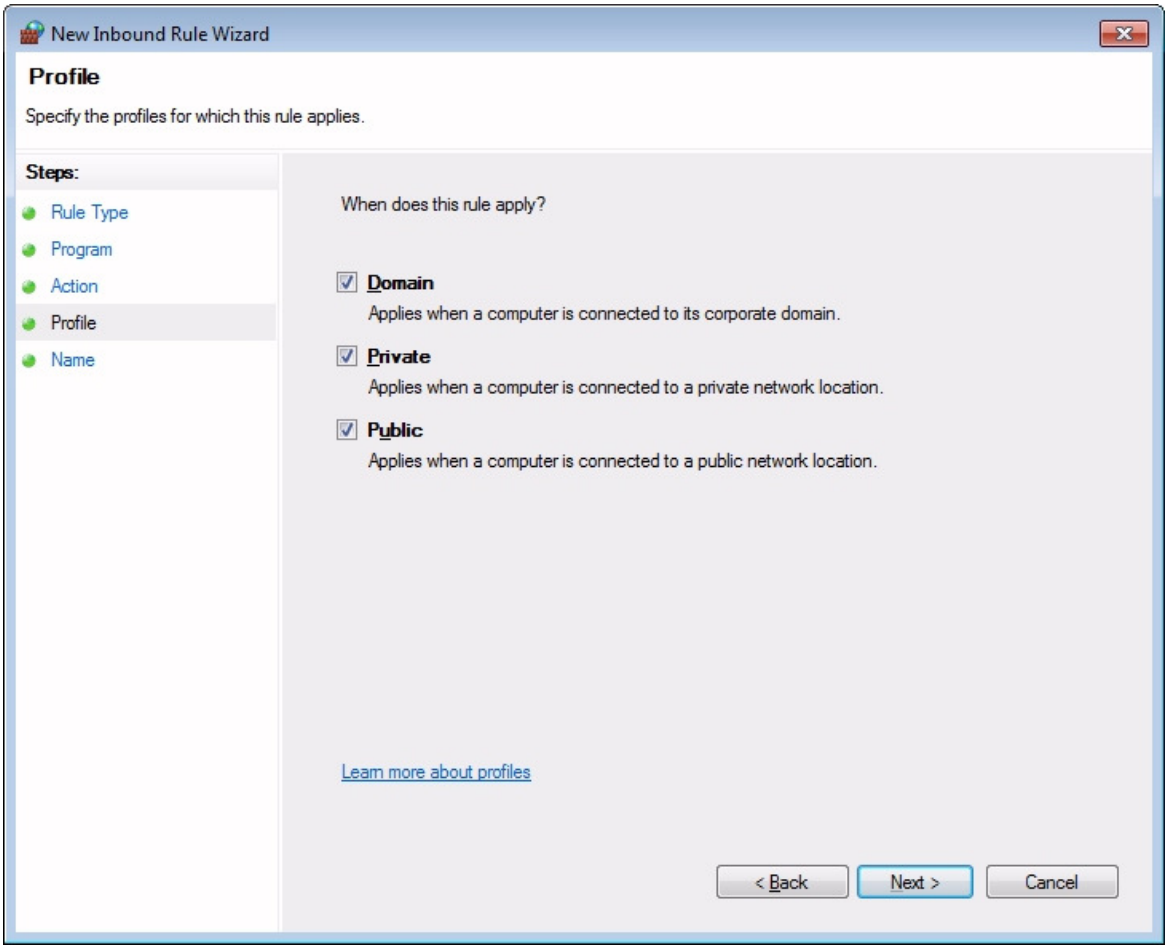


In the next dialog browse for **OpcEnum.exe.** It is located in the **Windows\System32** directory or on a 64bit OS in the directory **Windows\SysWOW64**.

Allow the connection.


New Inbound Rule Wizard
Action
Specify the action to be taken when a connection matches the conditions specified in the rule.
Steps:
Rule Type
Program
Action
Profile
Name
What action should be taken when a connection matches the specified conditions?
Allow the connection
This includes connections that are protected with IPsec as well as those are not.
Allow the connection if it is secure
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
Customize...
Block the connection
Learn more about actions
< Back
Next >
Cancel

This rule applies to all profiles.



Enter a convenient name for the new rule.

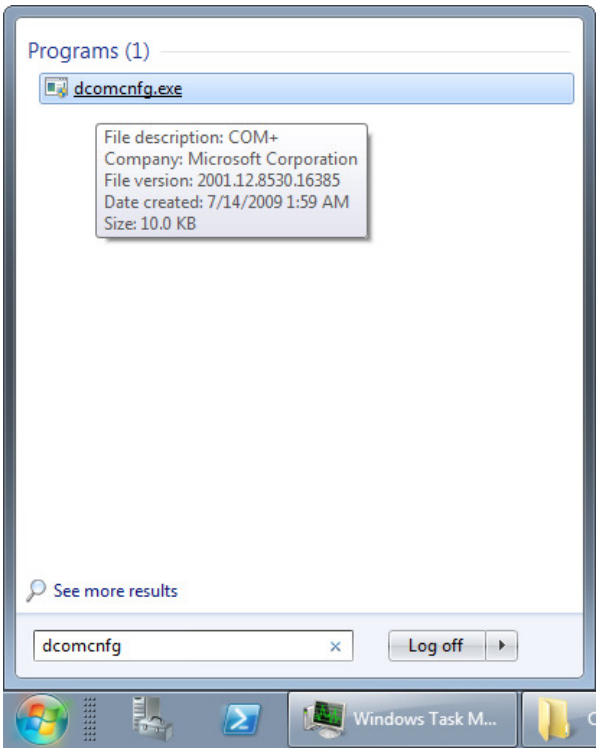
3. Enable the **inVISU OPC Server**.

Configure a new rule for the inVISU OPC Server similar to OpcEnum.

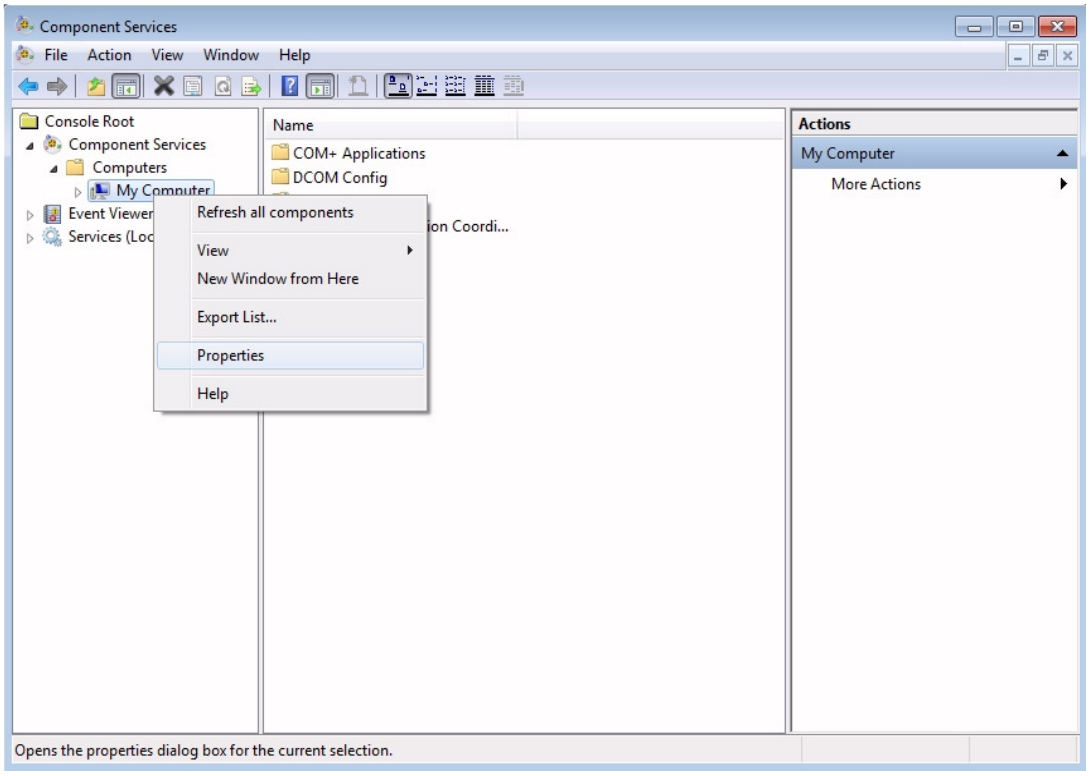
The executable name of the inVISU OPC Server is **OPCServer.exe** (located in the installation directory).

3. DCOM Settings

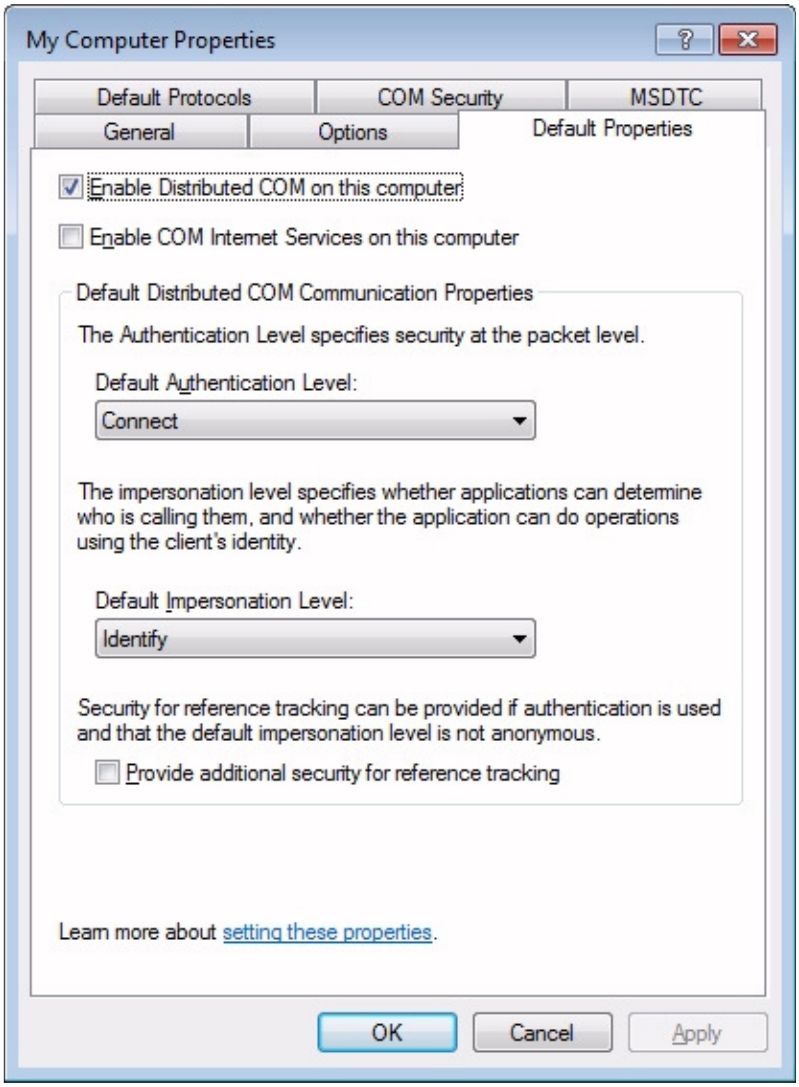
1 Open the DCOM configuration (**Start** -> **Run…** -> **dcomcnfg**)



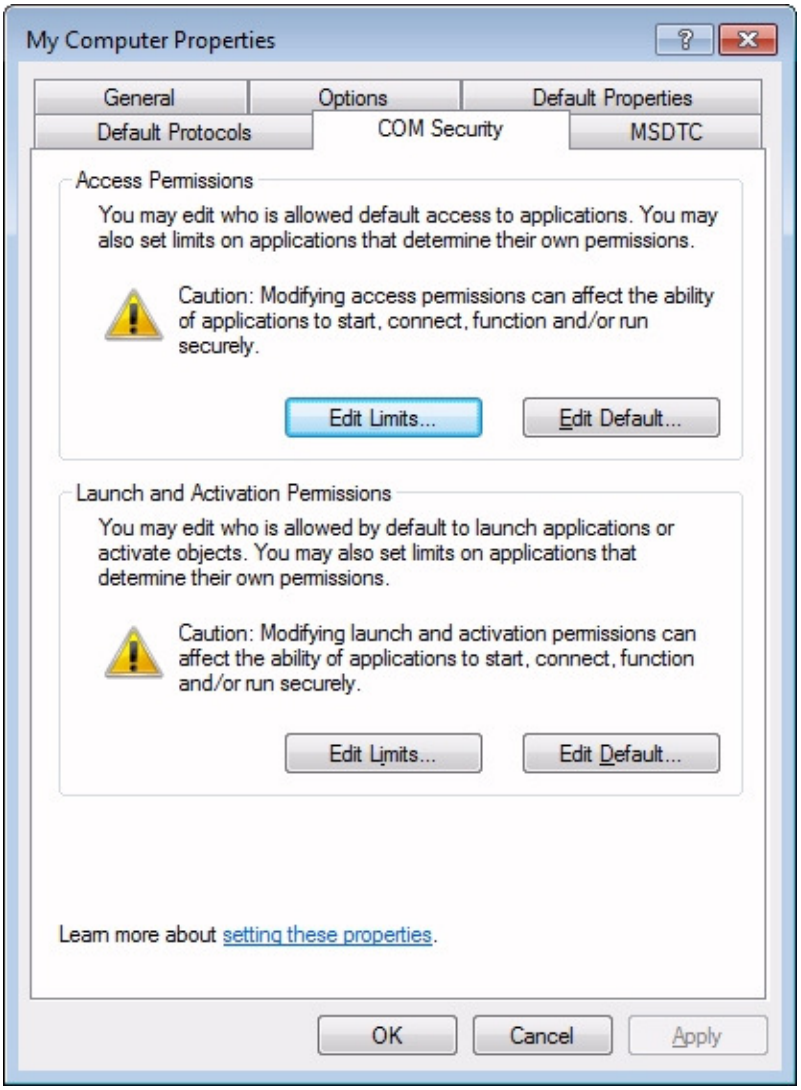
2. Choose **Console Root** -> **Component Services** -> **My Computer** -> **Properties**.



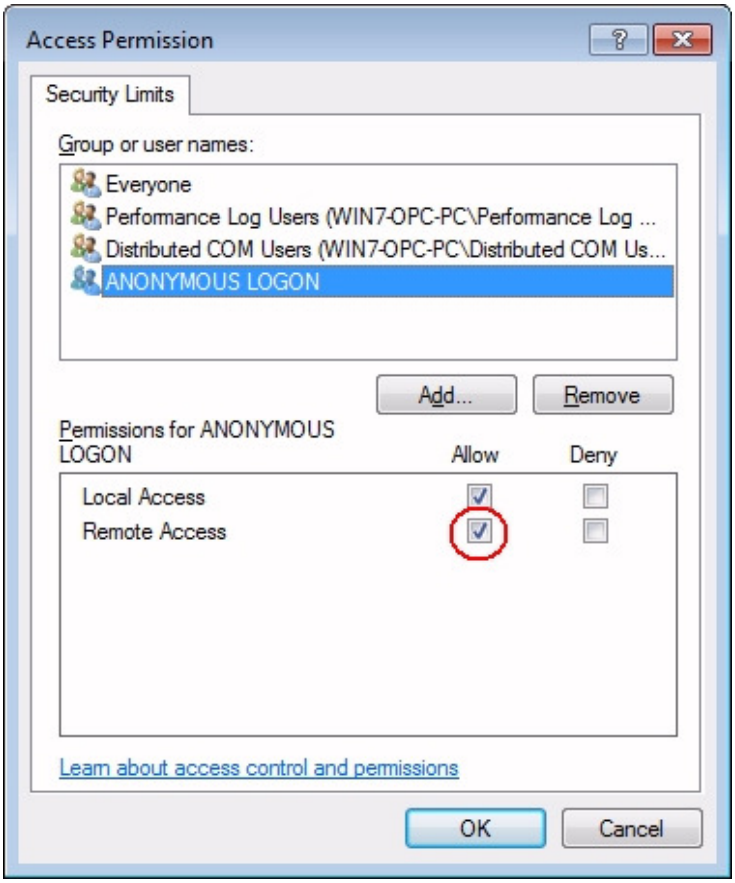
3. Verify the **Default Properties**.



4. Go to the tab **COM Security**.

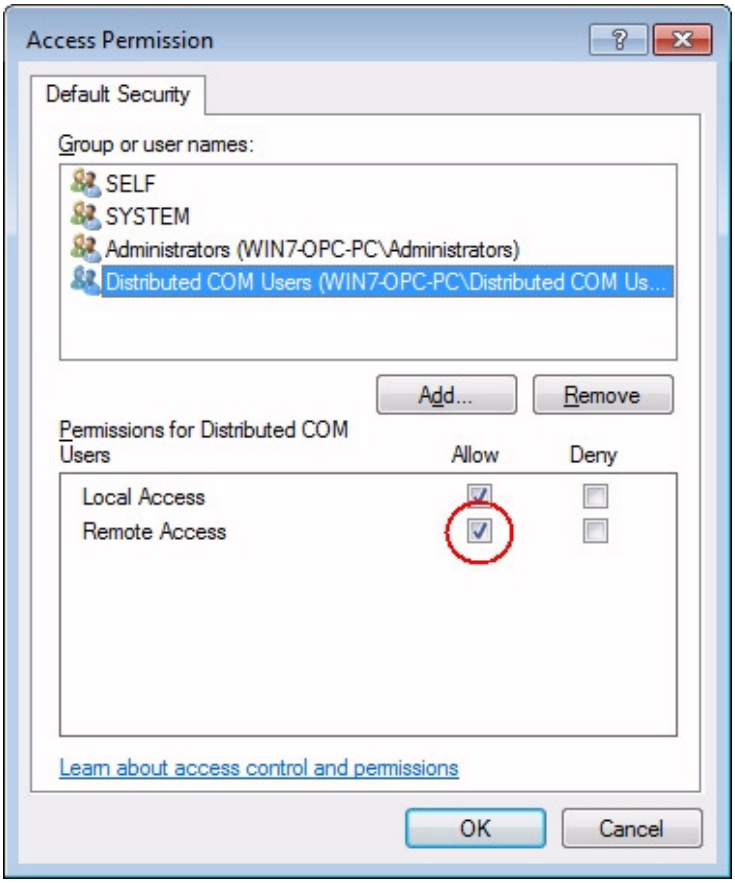


5. In group **Access Permissions** press **Edit Limits…**
Enable **Remote Access** for **ANONYMOUS LOGON**.

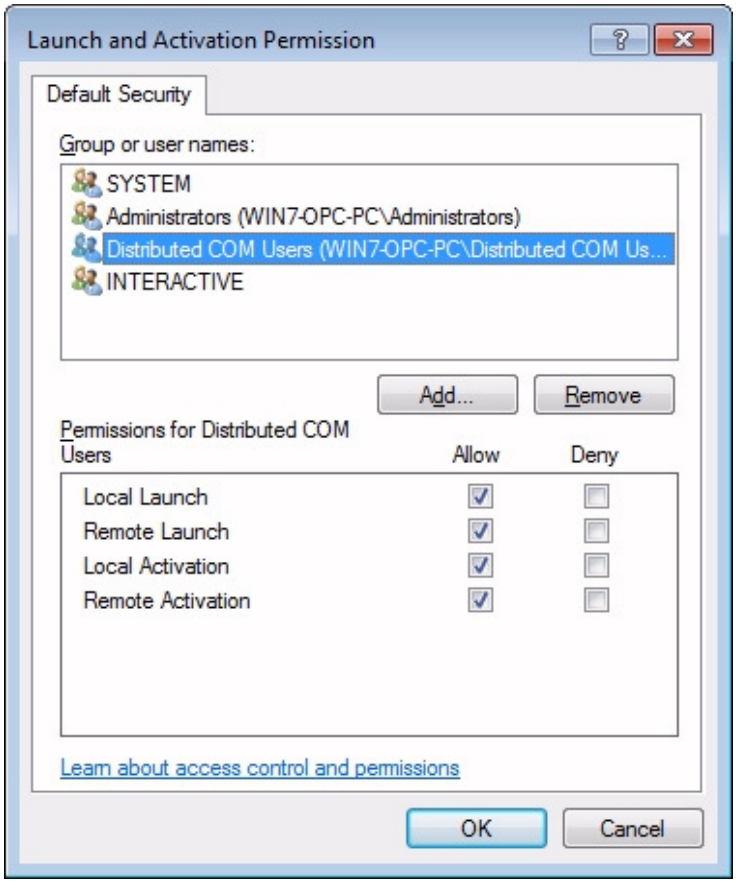


6. In group **Access Permissions** press **Edit Default…**

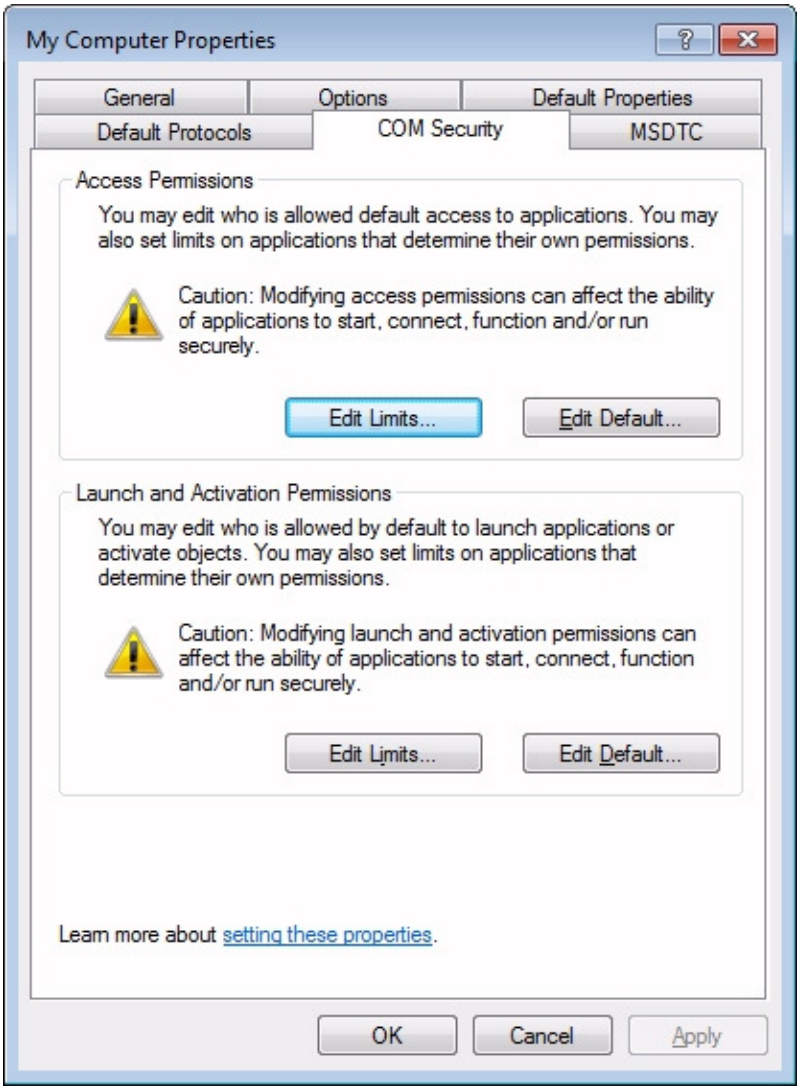
If not present add **Distributed COM Users** and enable **Remote Access**.



7. In group **Launch and Activation Permissions** press **Edit Default…**

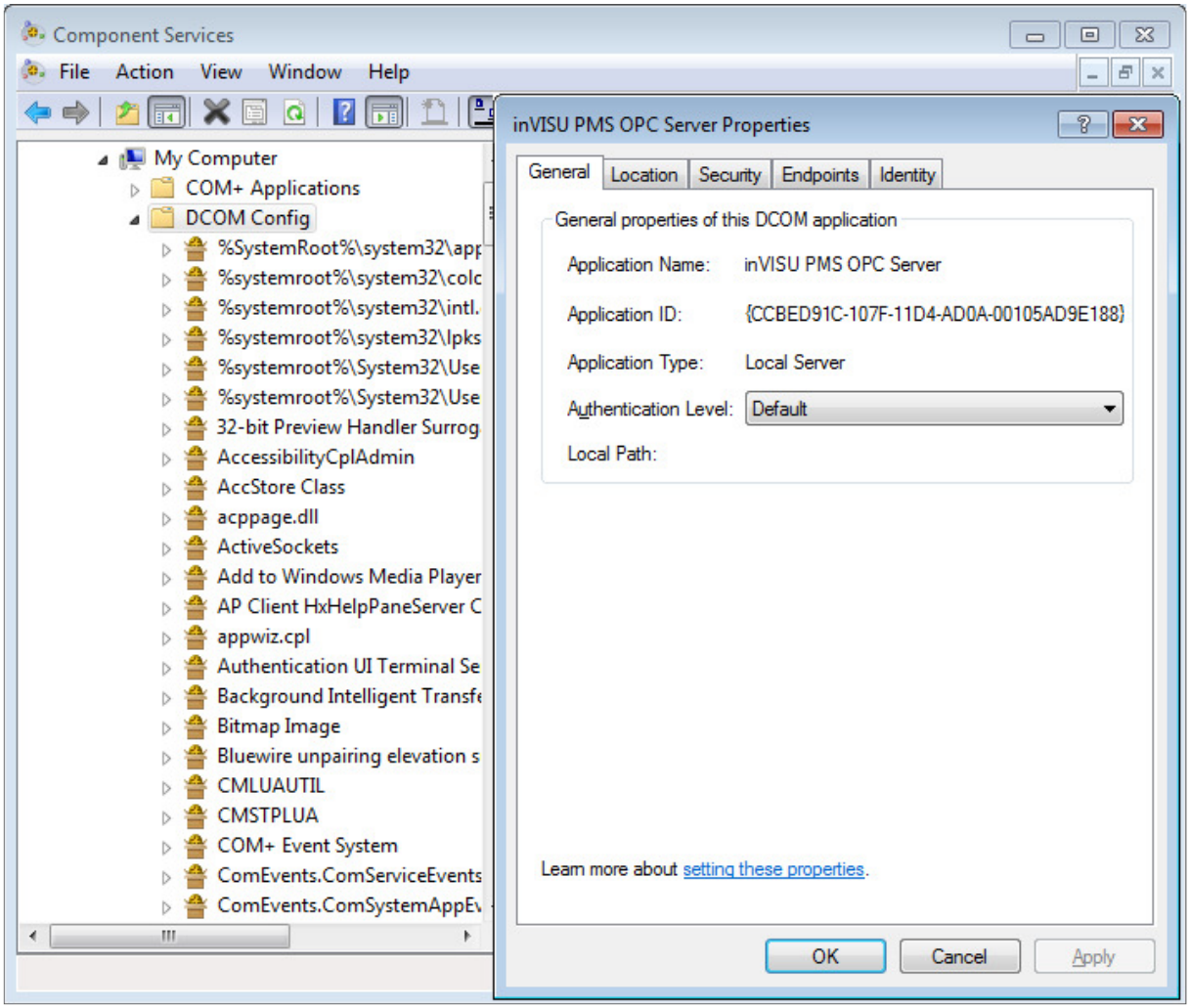


8. Press **OK** to close the DCOM settings for **My Computer**.

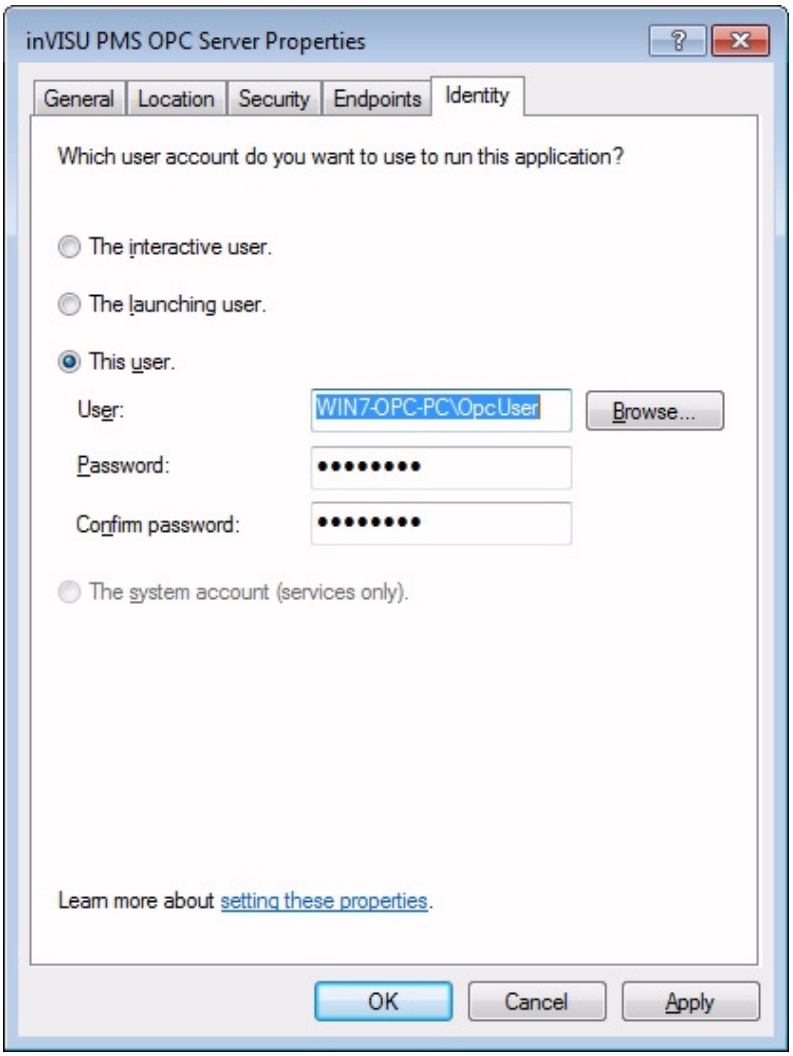


9. Edit the properties of the **inVISU PMS OPC Server**.

Open the folder **DCOM Config**, browse to the OPC Server, right-click on it and select **Properties**.



Go to tab **Identity** and configure **OpcUser** as user account.



4. Local Security Policy

It may be necessary to set the rule **Network access: Let Everyone permissions apply to anonymous users**.

Enter **Secpol.msc** in the Windows command line to start the Local Security Policy.

Go to **Local Policies** -> **Security Options** and set the rule **Network access: Let Everyone permissions apply to anonymous users** to **Enabled**.