European Laboratory for Particle Physics
Laboratoire Européen pour la Physique des Particules
CH-1211 Genève 23 – Suisse

OPC Support

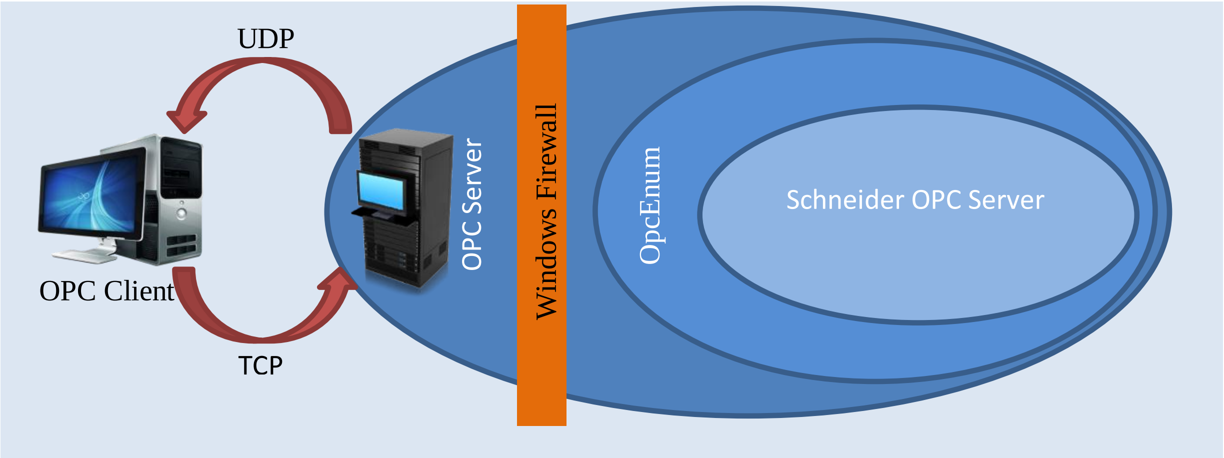
Setting DCOM for OPC under Windows 7 (32/64 bit)

Document Version:	0.1
Document Issue:	0
Document Date	20 July 2012
Document Status	Beta 3
Document Author:	Benjamin Farnham, Marco Pimentel

Contents

1. Windows 7 (32/64 bit) configuration overview

This tutorial walks through the DCOM configuration and security settings under Windows 7 to configure an OPC server



🟦 User access authorization control
🟧 Windows firewall

The steps to securely configure the OPC Server are: first of all, setting the wide DCOM protocol security authorizations for the computer access (MyComputer**)** then create some exceptions on the firewall so the OPC client can access the OpcEnum which gives the list of the OPC servers running on the machine, and last, configure the DCOM access permissions for OpcEnum and the OPC server.

The steps described in this tutorial will not follow this order to make it shorter

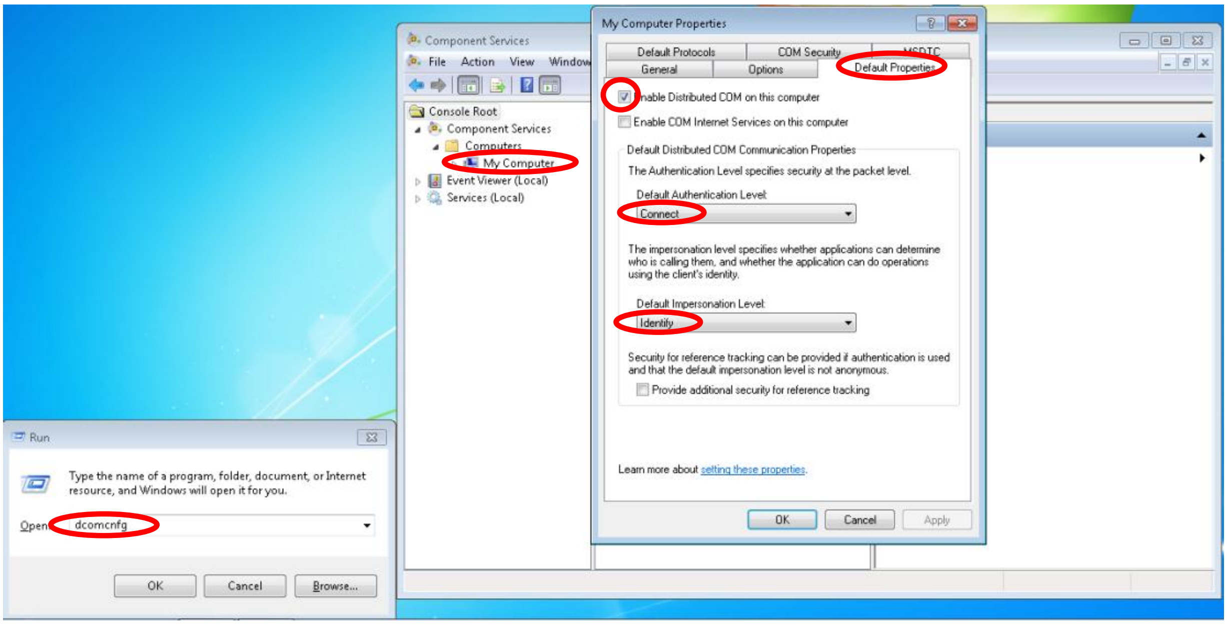
2. OPC Server Settings

A. Wide security “MyComputer” settings

Managing the settings for the general computer access, users and permissions

- Press ⊞ **+ R** to open the Run menu type "**DCOMCNFG**" on the text area and press **ENTER** to open the Component Services window
- Under: **Component Services→Computers**, Right-click on "**My Computer**" and Choose the "**Properties**" from the menu.
- Click the "**Default Properties**" Tab and configure as follow:

  Enable Distributed COM on this computer checked.
  Default Authentication Level **Connect**
  Default Impersonation Level **Identify**



☑ 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.

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: dcomcnfg

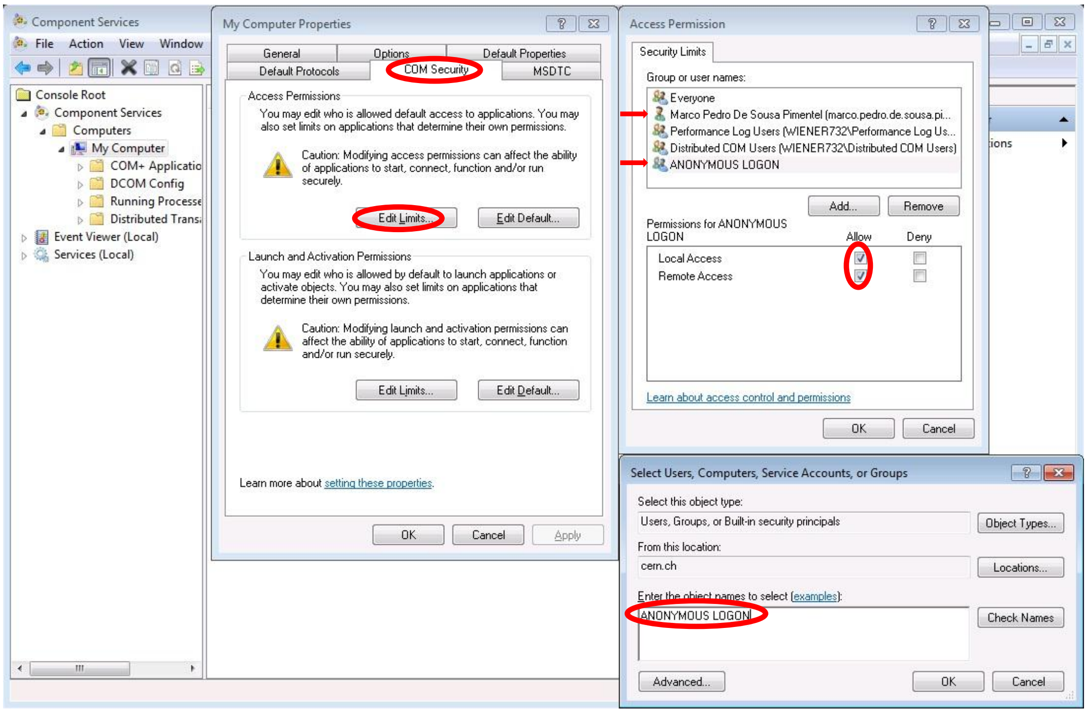
- Click on the "**COM Security**" tab

First we need to add “**ANONYMOUS LOGON”** to Access Permissions Limits and give it local and remote access, it is necessary to request user account information[1], also add the users accounts and/or groups who should be able to access the COM service in this machine.

- Click **"Edit Limits"** button within the **"Access Permissions"**

  Hit **Add** enter the object name **(ANONYMOUS LOGON)**
  Hit OK
  Check local access and remote access boxes
  Click OK
  Hit **Add** enter the users accounts and/or groups wanted (ex: **workgroup\user)**
  Repeat the operations until completed

[1] technet microsoft



Access Permissions

You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.

Launch and Activation Permissions

You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.

Learn more about setting these properties.

Group or user names:

- Everyone
- Marco Pedro De Sousa Pimentel (marco.pedro.de.sousa.pi...
- Performance Log Users (WIENER732\Performance Log Us...
- Distributed COM Users (WIENER732\Distributed COM Users)
- ANONYMOUS LOGON

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

Learn about access control and permissions

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

From this location: cern.ch

Enter the object names to select (examples): ANONYMOUS LOGON

For the “**Launch and Activation Permissions**” configure as needed, adding only permissions to the users and/or groups who should be able to access the COM service in this machine, setting the permissions. To assign permissions to a special group or user, add it and check the desired boxes.

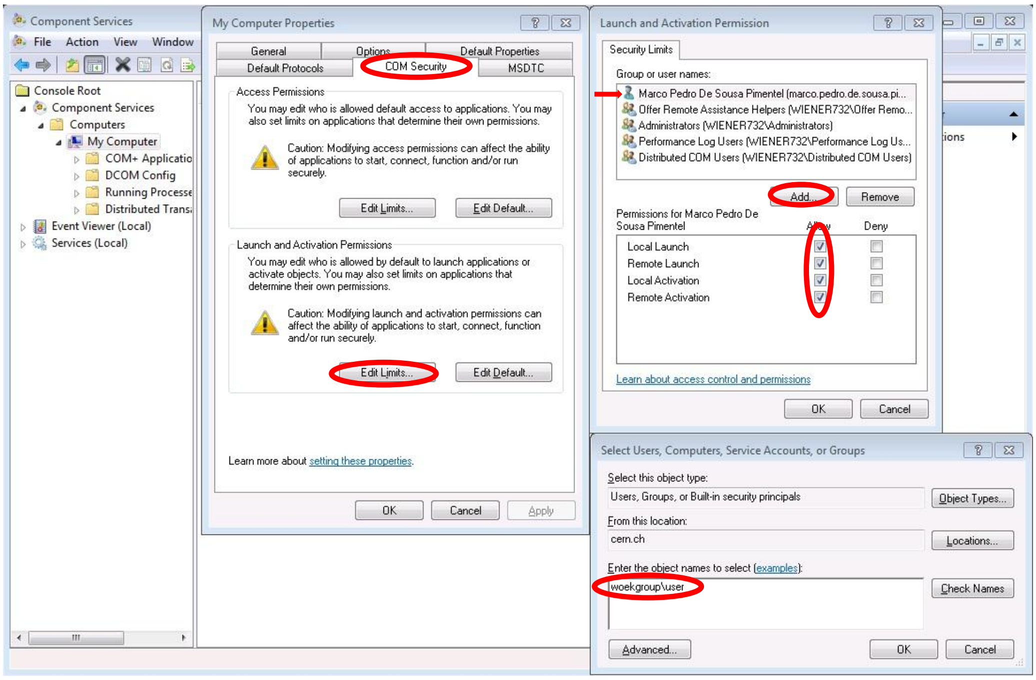
- click **"Edit Limits"** button within the **"Launch and activation Permissions"**

  hit **Add** enter users accounts and/or groups wanted (ex: **workgroup\user)**

  hit OK

  check the desired allow or deny boxes

  click OK



Access Permissions

You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.

Launch and Activation Permissions

You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.

Learn more about setting these properties.

Group or user names:

- Marco Pedro De Sousa Pimentel (marco.pedro.de.sousa.pi...
- Offer Remote Assistance Helpers (WIENER732\Offer Remo...
- Administrators (WIENER732\Administrators)
- Performance Log Users (WIENER732\Performance Log Us...
- Distributed COM Users (WIENER732\Distributed COM Users)

Permissions for Marco Pedro De Sousa Pimentel	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

Learn about access control and permissions

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

From this location: cern.ch

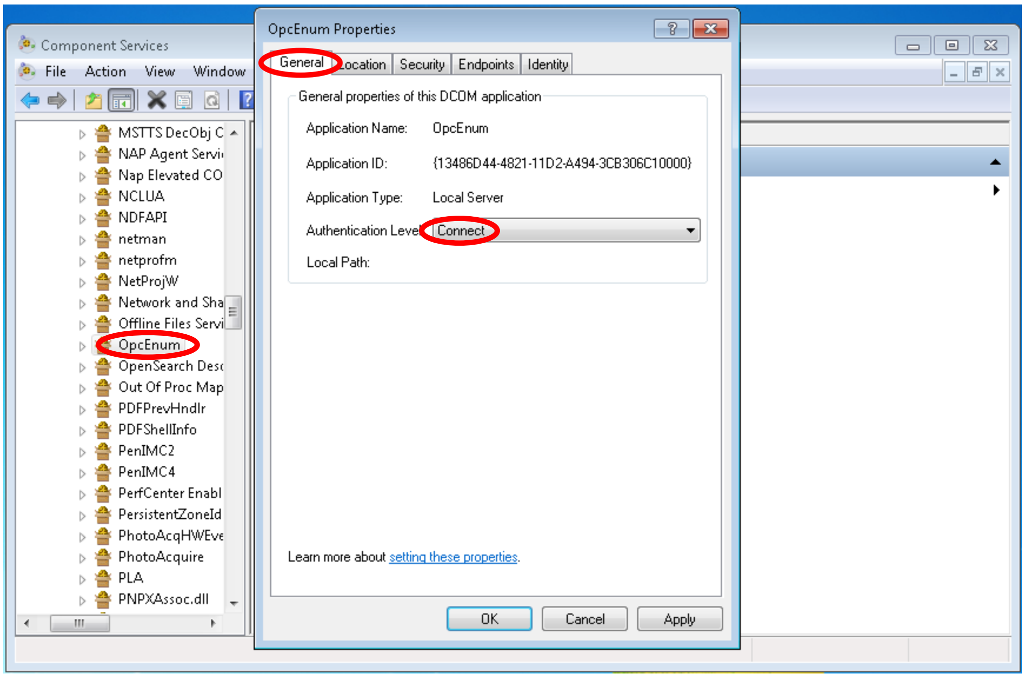
Enter the object names to select (examples): woekgroup\user

- Press OK at end to save settings.

B. “OpcEnum” Settings

Manage the users/groups that should be able to see the existing OPC servers running on the machine (It is possible to give authorisation to many users/groups to see the existing OPC servers running but authorise different users/groups to access to different servers. See: 4. Permissions settings)

- Under: **Component Services→Computers→My Computer→DCOM Config,** find **“OpcEnum**” on the list **right click** on it and Choose "**Properties**" from the menu.
- On the tab “General” Certify that the combo box have the value “connect” if not choose it.



General properties of this DCOM application

Application Name: OpcEnum

Application ID: {13486D44-4821-11D2-A494-3CB306C10000}

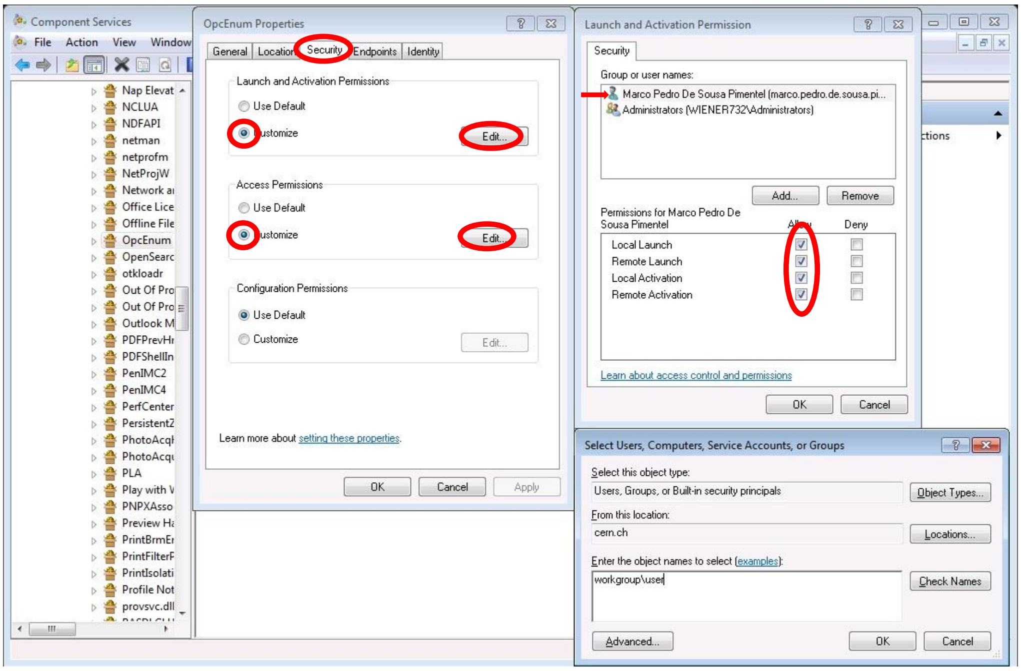
Application Type: Local Server

Authentication Level: Connect

Local Path:

Learn more about setting these properties.

- Select the “**security**” tab, on the Launch and Activation Permissions area hit the “**Customize**” button then the “**Edit**” button.



Launch and Activation Permissions

○ Use Default

● Customize

Access Permissions

○ Use Default

● Customize

Configuration Permissions

● Use Default

○ Customize

Learn more about setting these properties.

Group or user names:

Marco Pedro De Sousa Pimentel (marco.pedro.de.sousa.pi...

Administrators (WIENER732\Administrators)

Permissions for Marco Pedro De Sousa Pimentel	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

Learn about access control and permissions

Select this object type:

Users, Groups, or Built-in security principals

From this location:

cern.ch

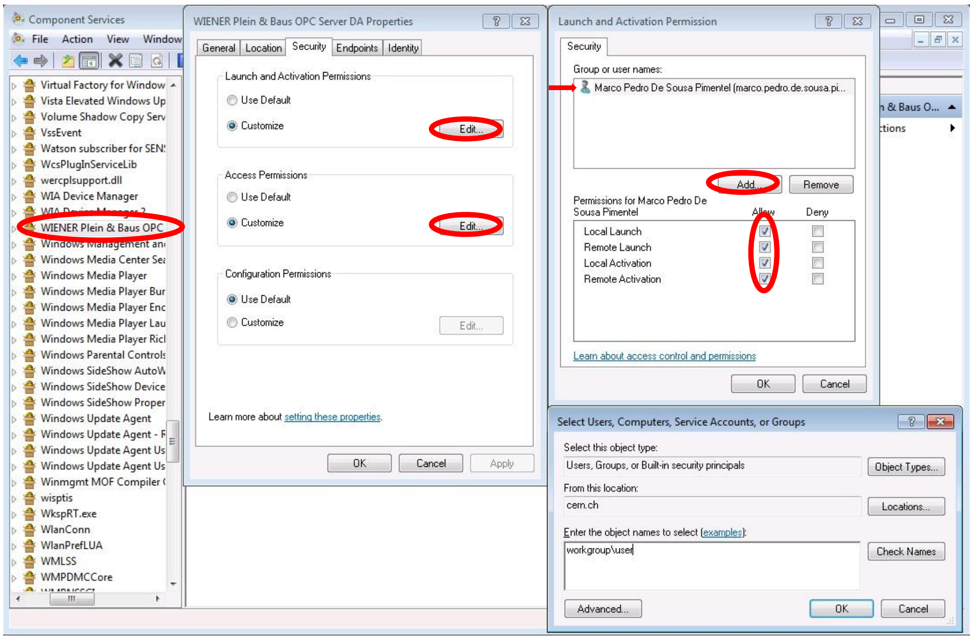
Enter the object names to select (examples):

workgroup\user

- On the “**Launch and activate permissions**” area hit the “**Customize”** button then the “**Edit**” button.
- Manage permissions. See: 4. Permissions settings click **OK** at end
- On the “**Access Permissions”** area hit the “**Customize”** button then the “**Edit**” button.
- Manage permissions. See: 4. Permissions settings click **OK** at end
- Leave the “**Configuration Permissions”** area as **Use Default**

C. OPC Server process Settings

- Find OPC process on the list for this example we install the WIENER OPC server, **right click** on it and Choose "**Properties**" from the menu.
- Repeat the steps in B knowing that the authorizations are now for this particular server



Launch and Activation Permissions
○ Use Default
● Customize Edit...

Access Permissions
○ Use Default
● Customize Edit...

Configuration Permissions
● Use Default
○ Customize Edit...

Learn more about setting these properties.

Group or user names:
Marco Pedro De Sousa Pimentel (marco.pedro.de.sousa.pi...

Permissions for Marco Pedro De Sousa Pimentel	Allow	Deny
Local Launch	☑	□
Remote Launch	☑	□
Local Activation	☑	□
Remote Activation	☑	□

Learn about access control and permissions

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

From this location:
cern.ch

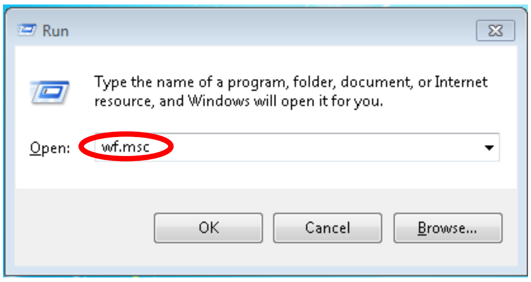
Enter the object names to select (examples):
workgroup\user

Exit the DCOMCNFG

3. Server Firewall Settings

Configure the firewall exceptions

- Press ⊞ **+ R** to open the Run menu type " **wf.msc**" on the text area and press **ENTER** to open the Component Services window

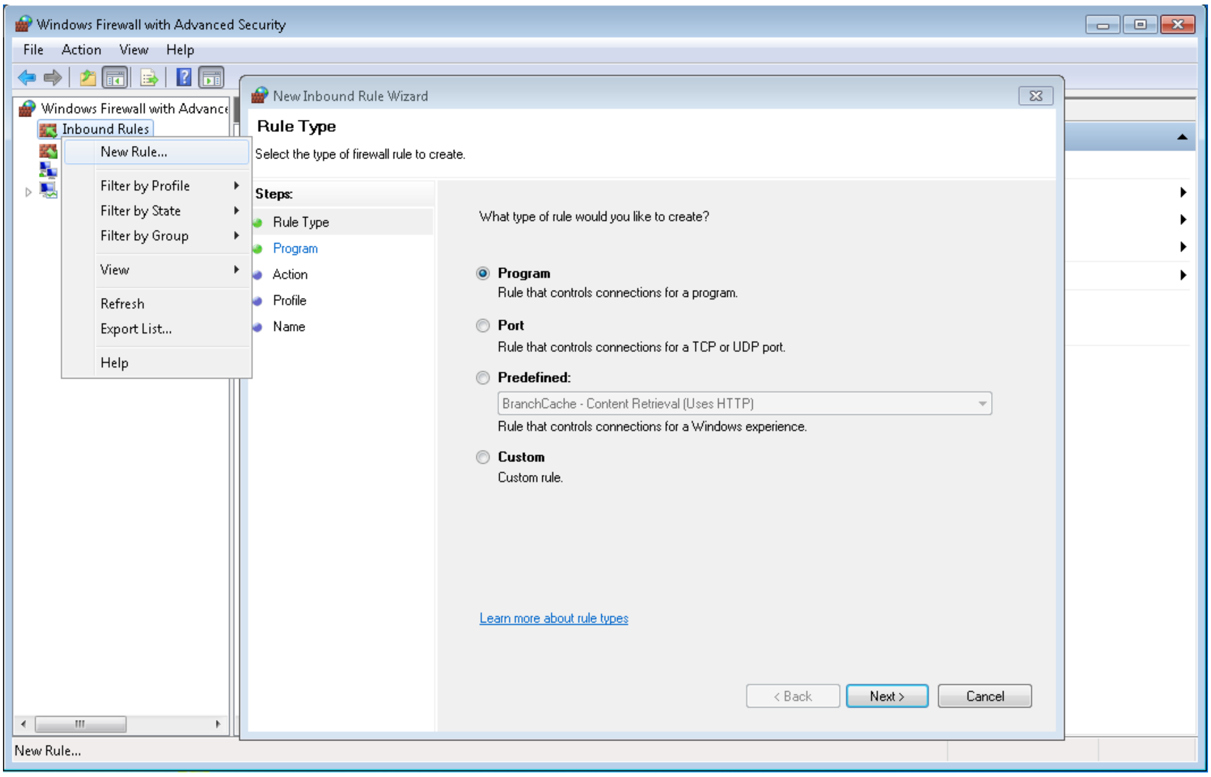


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: wf.msc

A. OPC Server Enumerator exception

- **Right click Inbound Rules** and choose **New Rule** from the drop down menu, the Inbound Rules wizard will appear



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.

- Go to inbound rules and add to the exceptions list **Chose program** and **hit next>**
- chose **This program path**, hit **Brows** find **opcenum.exe double click** it and **hit next>**
  (the path should be:
  Windows7 32 bit machine → c:\windows\system32\opcenum.exe
  Windows7 64 bit machine and Windows Server 2008 R2 →C:\Windows\SysWOW64\opcenum.exe)
- Chose **Allow the connection** and hit **Next>**
- Check the desired boxes (in our example we only check Domain) hit **Next>**
- Give a name to the connection rule and a description if you desire to then **hit Finish.**

B. OPC Server exception

- **Right click Inbound Rules** and choose **New Rule** from the drop down menu, the Inbound Rules wizard will appear
- **Chose program** and **hit next>**
- chose **This program path**, hit **Brows** find **your OPC server executable double click** it and **hit next>** (the
- Chose **Allow the connection** and hit **Next>**
- Check the desired boxes hit **Next>**
- Give a name to the connection rule and a description if you desire to, then **hit Finish.**

Exit the firewall configuration window

Restart windows

4. Permissions settings

The server permissions can be managed according to the level of access we want to give, for example if we have a worckgroup (WG) how can access a server and we want user A (UA) to be able to access OPCserverA and user B (UB) to be able to access only OPCserverB, we should set. permissions as follow:

OpcEnum → WG
OPCserverA → WG\UA
OPCserverB → WG\UB

And allow remote and\or local operations for each one of them.

5. OPC Client Settings

A. Wide security “MyComputer” settings

In the client side the only permission we need to add is the “**Remote Access**” for the **ANONIMOUS LOGON** in the Access Permissions Limits as follow.

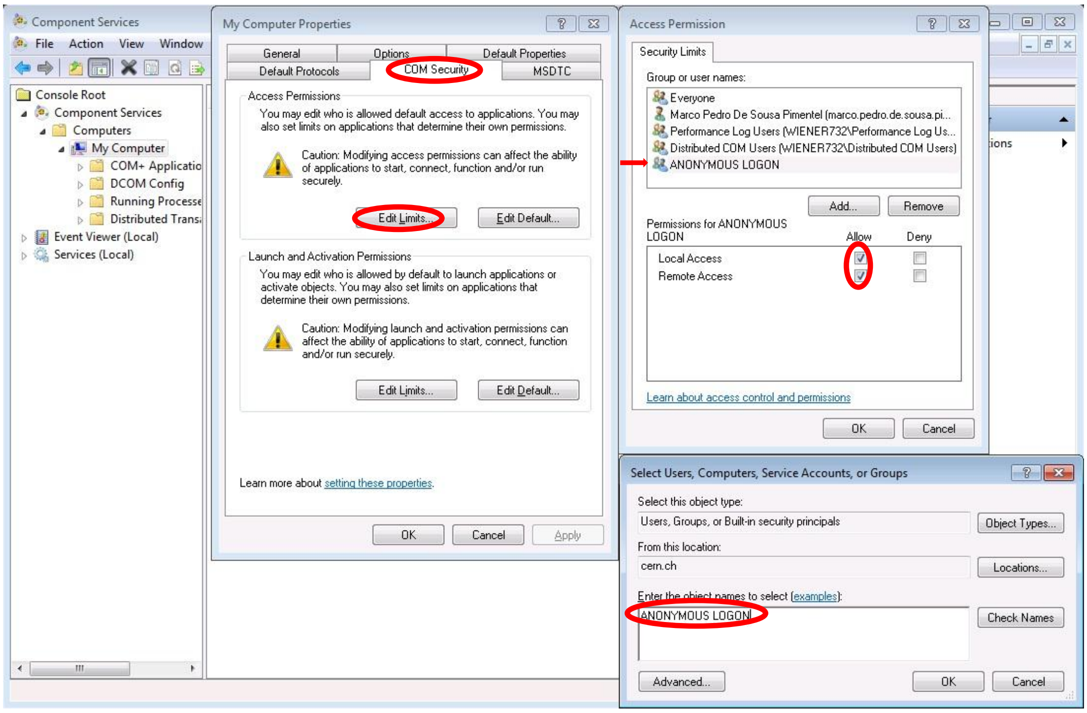
- Click **"Edit Limits"** button within the **"Access Permissions"**

  Hit **Add** enter the object name (**ANONYMOUS LOGON)**

  Hit OK

  Check local access and remote access boxes

  Click OK



My Computer Properties

Access Permissions

You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.

Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.

Launch and Activation Permissions

You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.

Learn more about setting these properties.

Access Permission

Group or user names:

- Everyone
- Marco Pedro De Sousa Pimentel (marco.pedro.de.sousa.pi...
- Performance Log Users (WIENER732\Performance Log Us...
- Distributed COM Users (WIENER732\Distributed COM Users)
- ANONYMOUS LOGON

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

Learn about access control and permissions

Select Users, Computers, Service Accounts, or Groups

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

From this location:
cern.ch

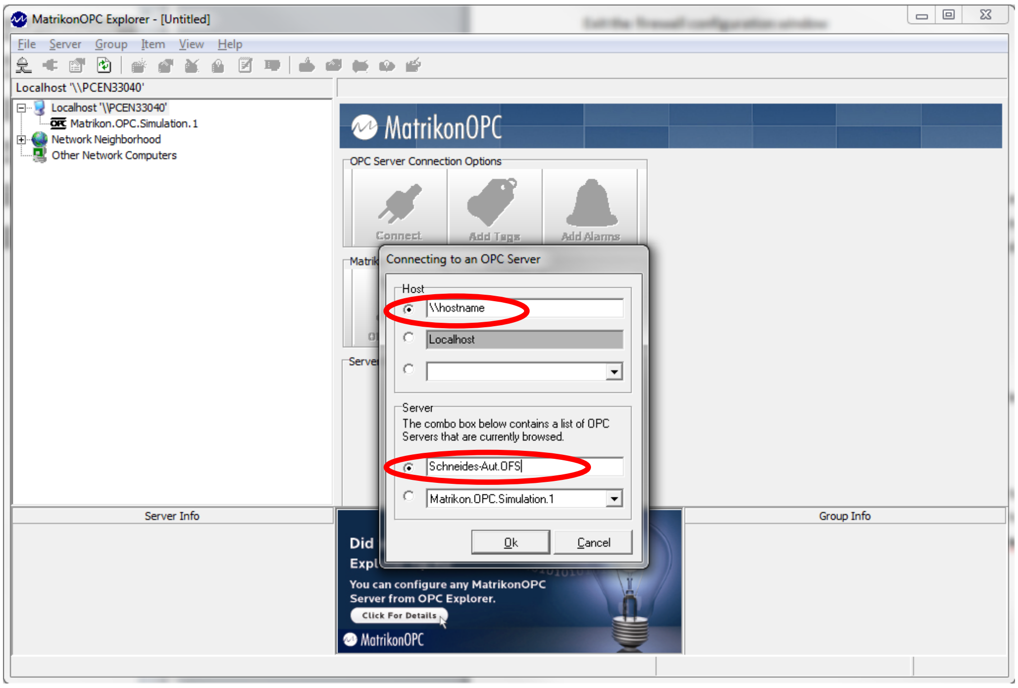
Enter the object names to select (examples):
ANONYMOUS LOGON

6. APENDIX

A. Testing the server

To test the connections use the free MatriconOPC Explorer running on a remote machine. In the Matrikon Explorer go to the menu Server→add/Connect server, on the connection dialogue fill the host name like this **\\hostname** and in the server write your OPC server name.

For WIENER: **WIENER.Plein.Baus.OPC.Server.DA**
For Schneider: **Schneider-Aut.OFS**



MatrikonOPC Explorer - [Untitled]

Localhost '\\PCEN33040'

Connecting to an OPC Server

Host
● \\hostname
○ Localhost
○

Server
The combo box below contains a list of OPC Servers that are currently browsed.
● Schneides-Aut.OFS
○ Matrikon.OPC.Simulation.1

Ok Cancel

You can configure any MatrikonOPC Server from OPC Explorer.

B. DCOM Logging

If you encounter problems during the connection I recommend activating the DCOM logging following these steps.

1. Click Start, click Run, type **regedit**, and then click **OK**.
2. Locate the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole registry subkey.
3. **Right-click** the Ole value, point to **New**, and then click **DWORD** Value.
4. Type **ActivationFailureLoggingLevel**, and then press **ENTER**.
   Double-click ActivationFailureLoggingLevel, type **1** in the Value data box, and then click **OK**.
5. **Right-click** the Ole value, point to **New**, and then click **DWORD** Value.
6. Type **CallFailureLoggingLevel**, and then press **ENTER**.
   Double-click CallFailureLoggingLevel, type **1** in the Value data box, and then click **OK**.
7. Restart the DCOM program, and then examine the System log and the Application log for DCOM errors (Event Viewer). The error messages in the Windows event log contain information that you can use to help resolve the permissions issue.

You can **turn off DCOM error logging** by changing the **ActivationFailureLoggingLevel** value and the **CallFailureLoggingLevel** value to **zero**.