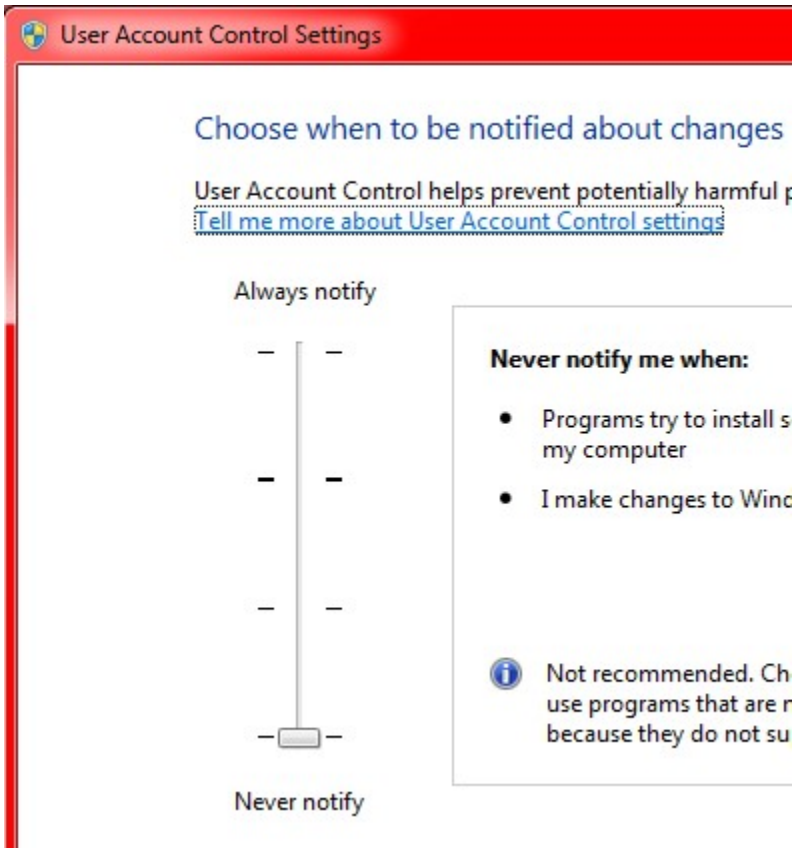
CTCOpc Server Installation As Service & Remote Access

Note: Below Assumes CTCOpc server is installed, licensed and operational locally before proceeding. The desired project should be the last loaded as that will be the one the service will start with. The service will have to be restarted whenever a change occurs to the project file (.cop).

Windows 7/10

Disable User Access Control (UAL) and reboot. This is under Control Panel->User Accounts

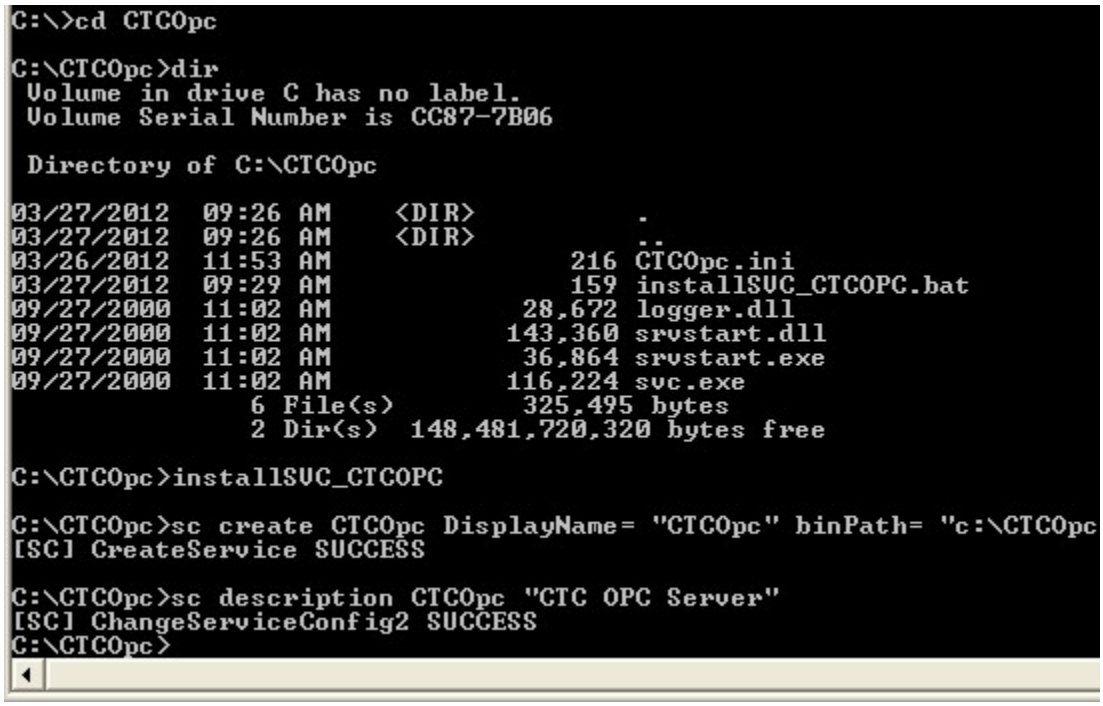


Windows 7/10 & Windows XP Service Pack 3

1. Create a C:\CTCOpc directory. Unzip the CTCOpcServices.zip file to this directory. It contains the utility programs and dll's needed for running CTCOpc as a service. The batch file you will run in the next step will only run properly with this exact directly name and placement.
2. Copy and paste the dll files within this directory (logger.dll and srvstart.dll) to the Windows\System32 subdirectory. Make sure msvcrt.dll is present in the directory

and if not obtain from Microsoft or another Windows installation. This dll may be missing on Windows XP but has always been present thus far on Windows 7/10.

3. Open a command window as administrator (right click and select 'run as administrator' on the cmd selection). Execute the batch file: installSVC_CTCOPC for a 32 bit operating system or installSVC_CTCOPC64 for 64 bit, and ensure SUCCESS status as shown below:



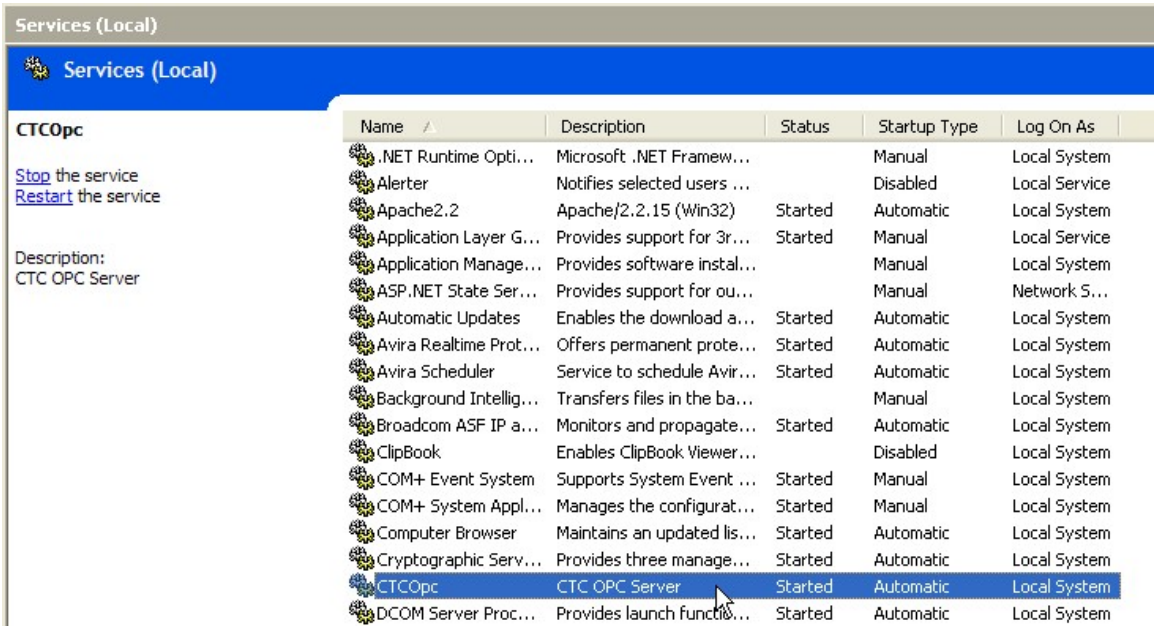
Note: Documentation for the batch file can be obtained from:

http://www.nick.rozanski.org.uk/services

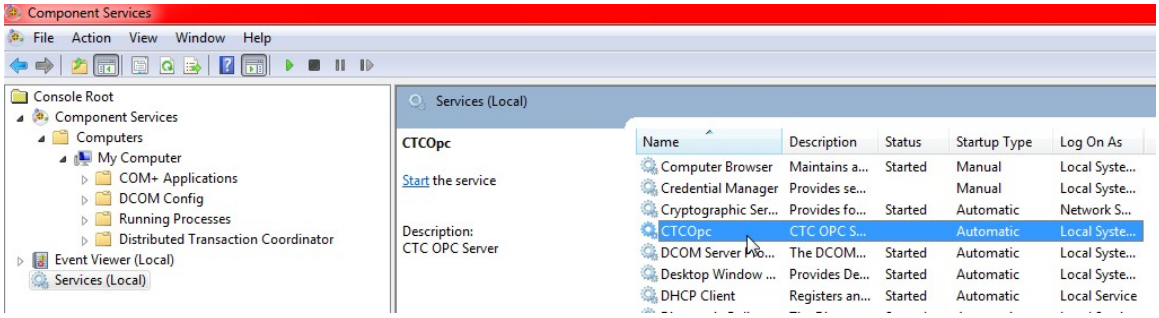
http://www.howtogeek.com/50786/using-srvstart-to-run-any-application-as-a-windows-service/

Reboot the computer or start the service as shown below (Control Panel->Administrative Tools):

Windows XP:



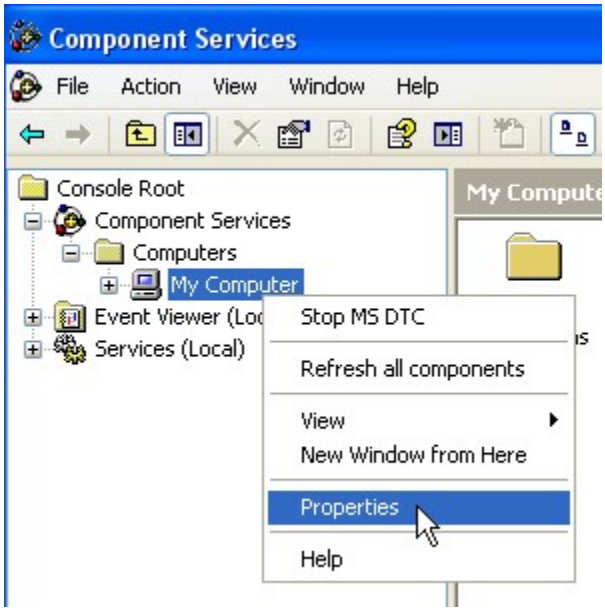
Windows 7:

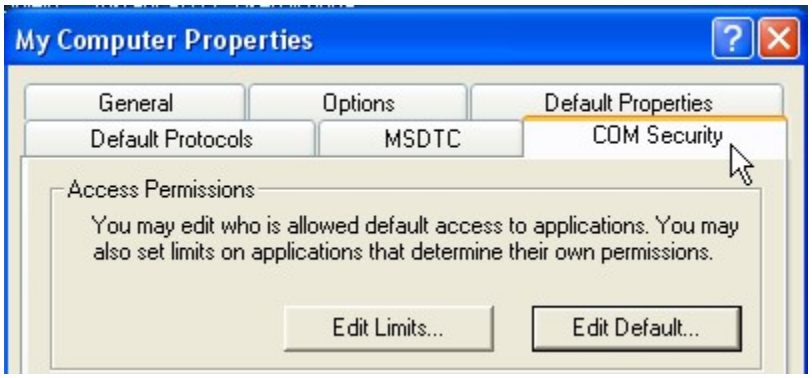


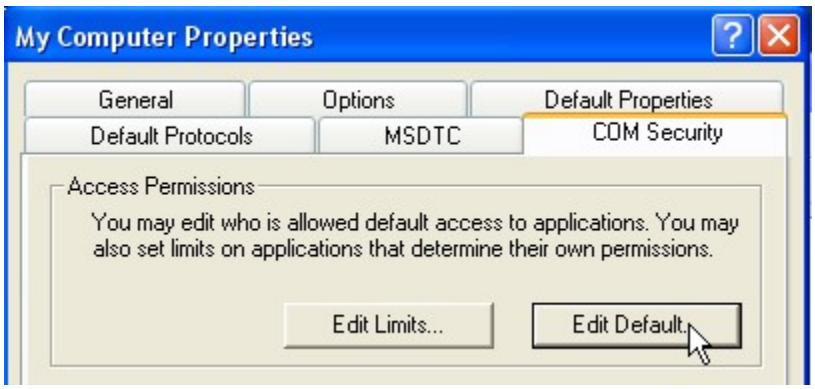
Local access only is now enabled.

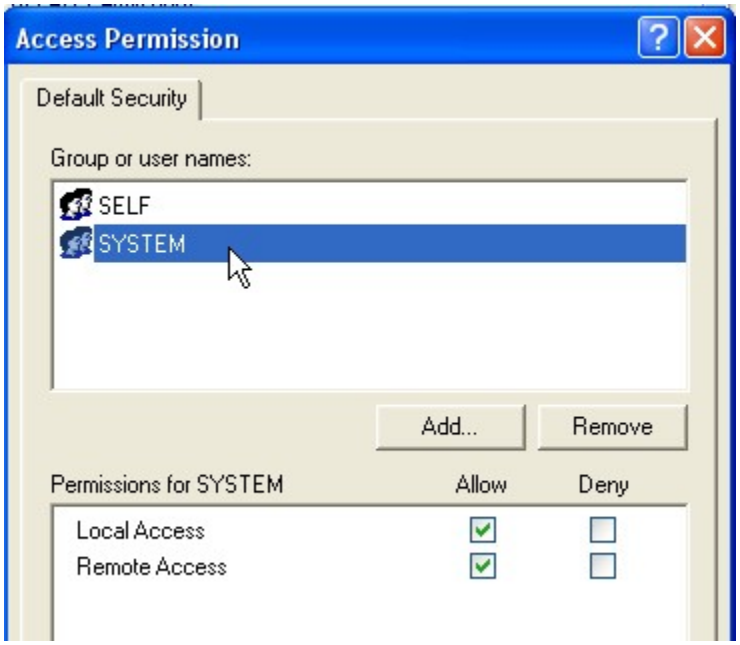
Windows XP - Remote Access of CTCOpc Server

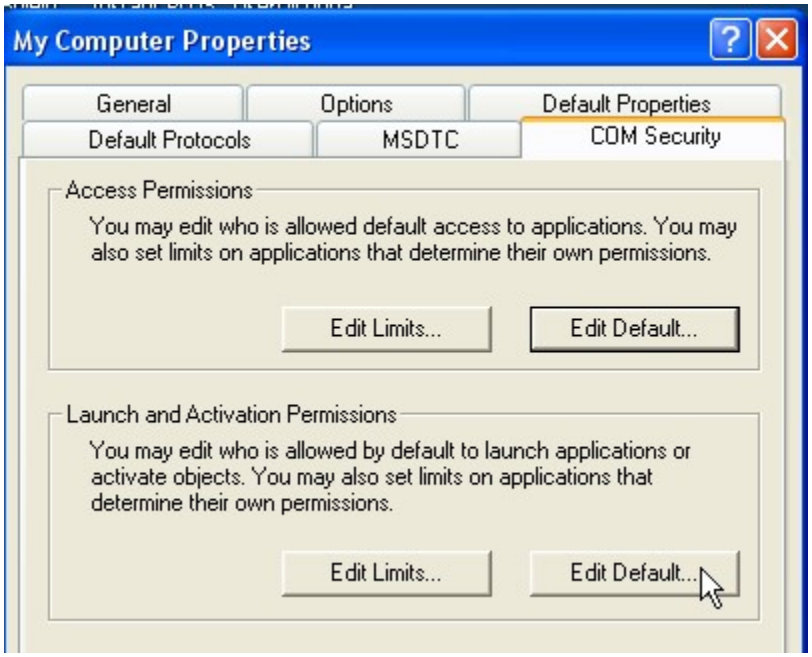
For Remote Access COM Security must be modified:

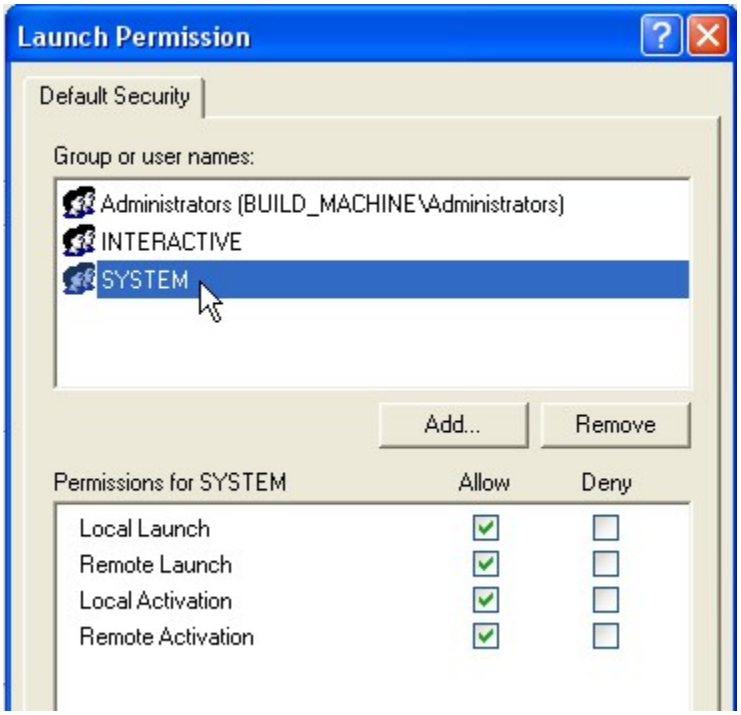


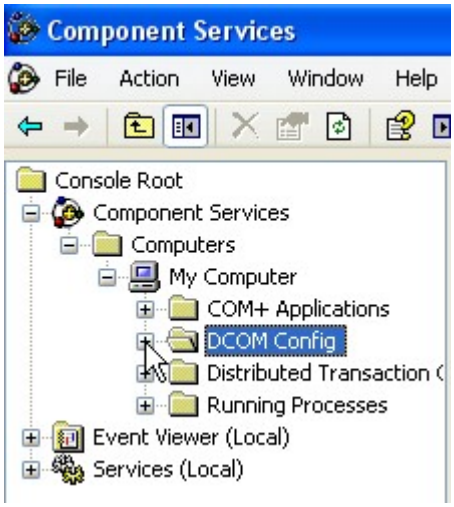


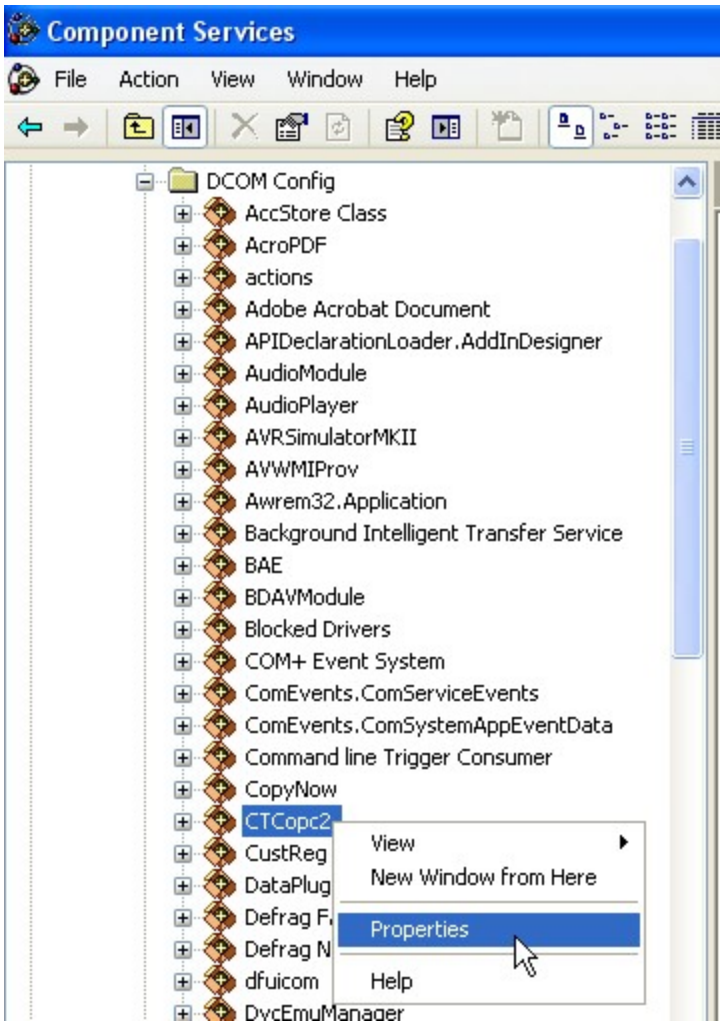


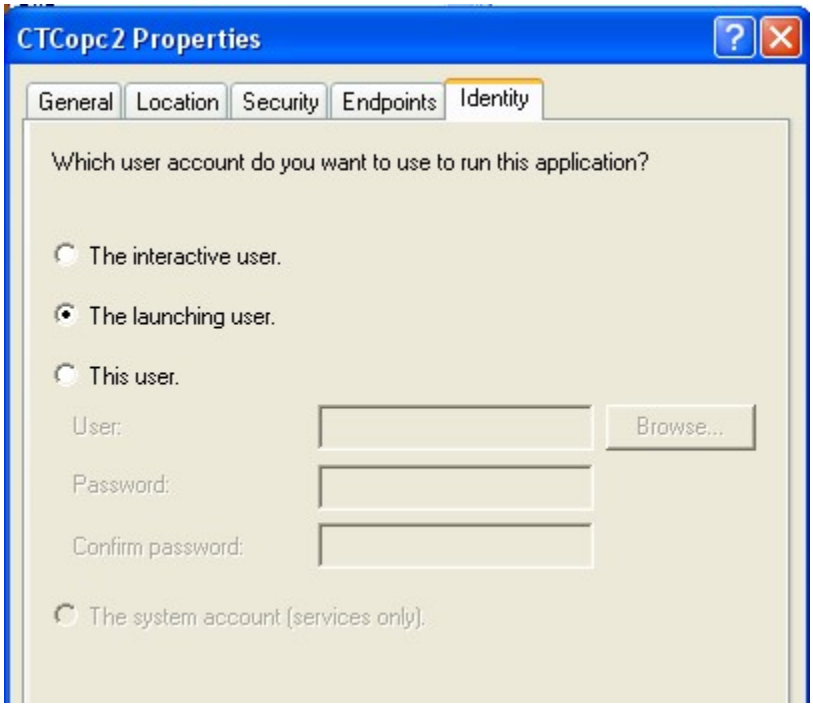

Access Permission
Default Security
Group or user names:
SELF
SYSTEM
Add...
Remove
Permissions for SYSTEM
Allow
Deny
Local Access
Remote Access


My Computer Properties
General
Options
Default Properties
Default Protocols
MSDTC
COM Security
Access Permissions
You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.
Edit Limits...
Edit Default...
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.
Edit Limits...
Edit Default...


Launch Permission
Default Security
Group or user names:
Administrators (BUILD_MACHINE\Administrators)
INTERACTIVE
SYSTEM
Add...
Remove
Permissions for SYSTEM
Allow
Deny
Local Launch
Remote Launch
Local Activation
Remote Activation


Component Services
File
Action
View
Window
Help
Console Root
Component Services
Computers
My Computer
COM+ Applications
DCOM Config
Distributed Transaction
Running Processes
Event Viewer (Local)
Services (Local)


Component Services
File
Action
View
Window
Help
DCOM Config
AccStore Class
AcroPDF
actions
Adobe Acrobat Document
APIDeclarationLoader.AddInDesigner
AudioModule
AudioPlayer
AVRSimulatorMKII
AVWMIProv
Awrem32.Application
Background Intelligent Transfer Service
BAE
BDAVModule
Blocked Drivers
COM+ Event System
ComEvents.ComServiceEvents
ComEvents.ComSystemAppEventData
Command line Trigger Consumer
CopyNow
CTCopc2
CustReg
DataPlug
Defrag F
Defrag N
dfuicom
DvcEmuManager
View
New Window from Here
Properties
Help

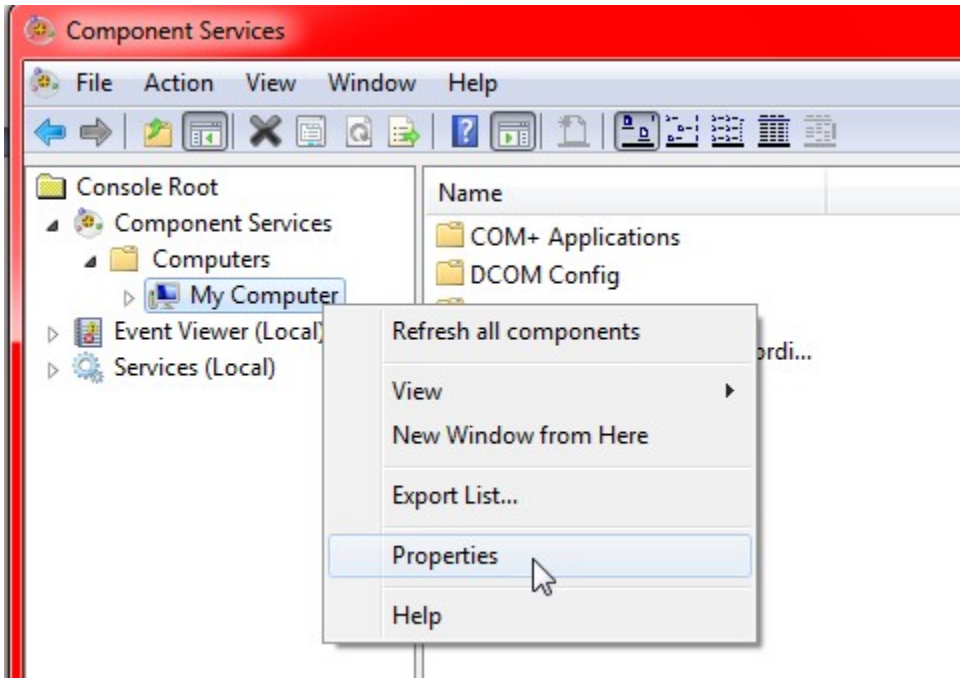


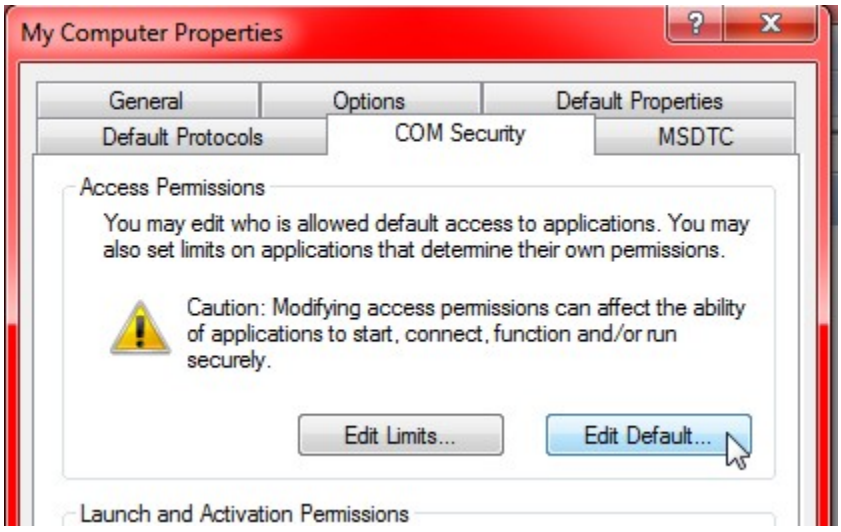
For remote access it may be preferred to select ‘This user’ and define an account to be used exclusively by OPC.

Note that above assumes Windows Firewall is disabled, if it must be turned on reference that section in Windows 7 for additional requirements, Page 14.

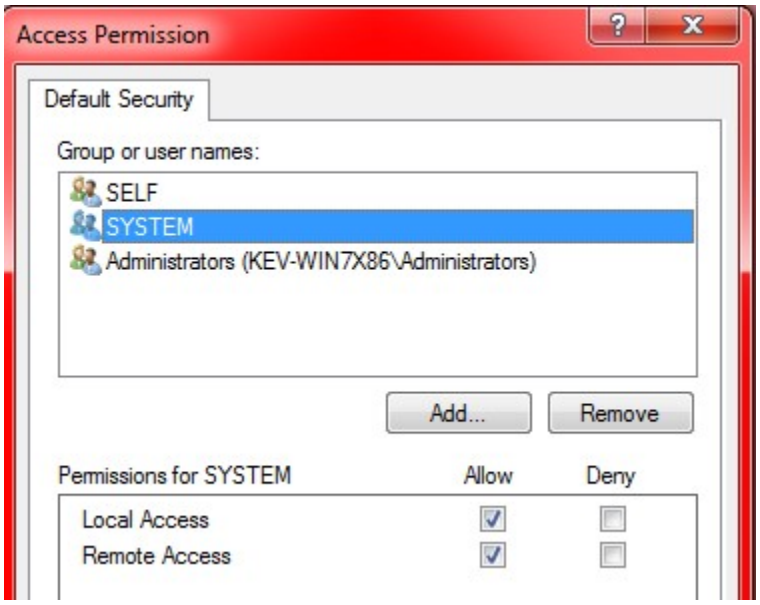
Windows 7 - Remote Access of CTCOpc Server

For Remote Access COM Security must be modified. Access this from the Control Panel->System and Security->Administrative Tools->Component Services Screen:

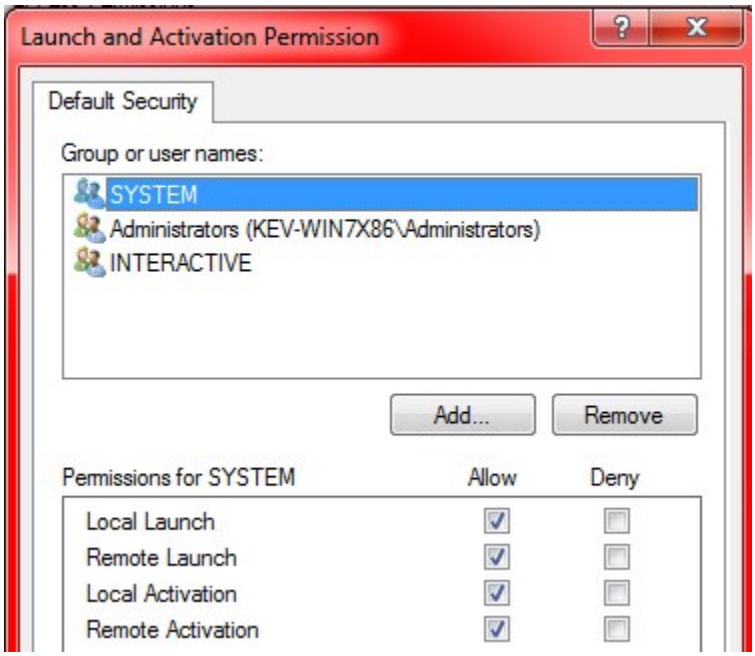


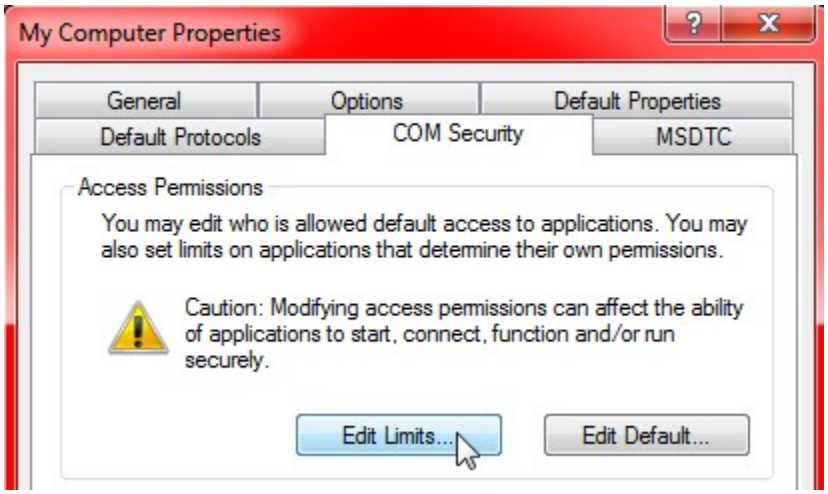


Under SYSTEM all should be checked:

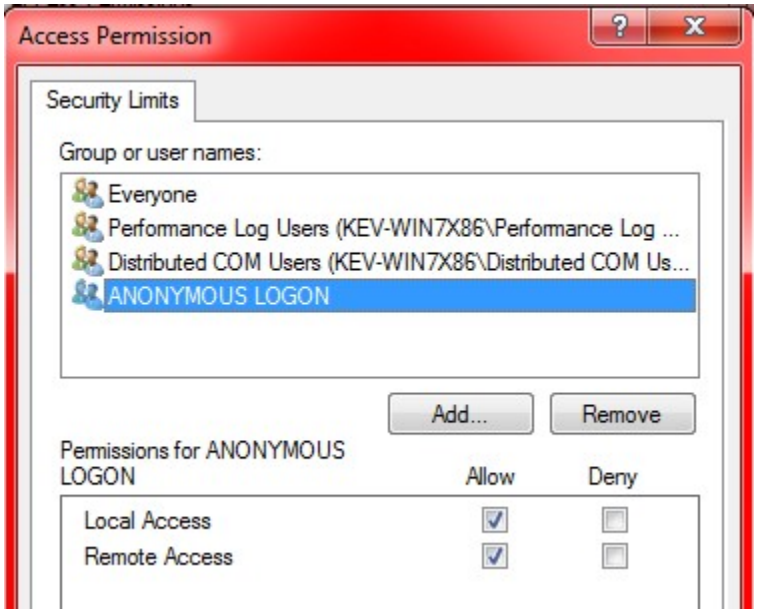


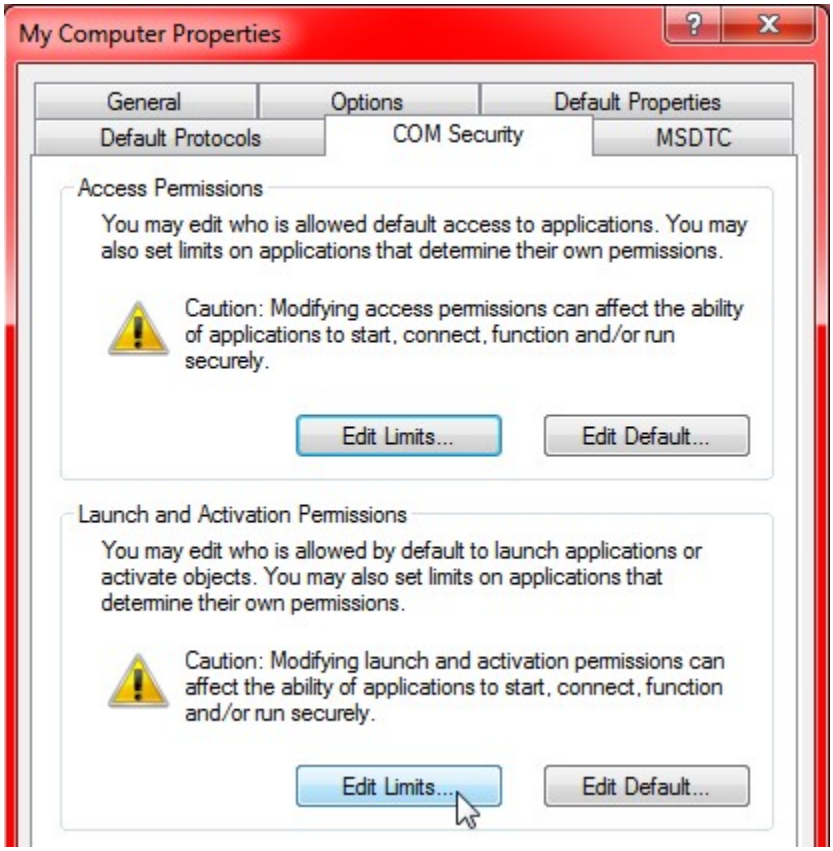
All should be selected for each below:



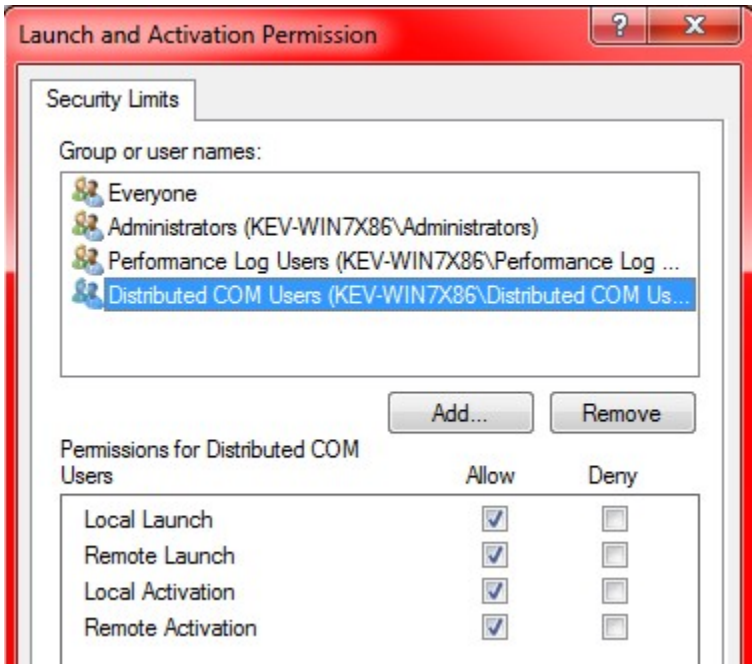


All should be checked for each below:


Access Permission
Security Limits
Group or user names:
Everyone
Performance Log Users (KEV-WIN7X86\Performance Log ...
Distributed COM Users (KEV-WIN7X86\Distributed COM Us...
ANONYMOUS LOGON
Add...
Remove
Permissions for ANONYMOUS LOGON
Allow
Deny
Local Access
Remote Access


My Computer Properties
General
Options
Default Properties
Default Protocols
COM Security
MSDTC
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.
Edit Limits...
Edit Default...
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.
Edit Limits...
Edit Default...

All should be selected for Distributed DCOM Users:



Below from following web site:
http://www.aggsoft.com/asdl-dcom-opc-config-3.htm

3.1 PERMITTING DCOM ACTIVITY

By default, Windows blocks inbound connections from other computer. For OPC clients to be able to connect to OPC servers on this computer, enable the corresponding rule.

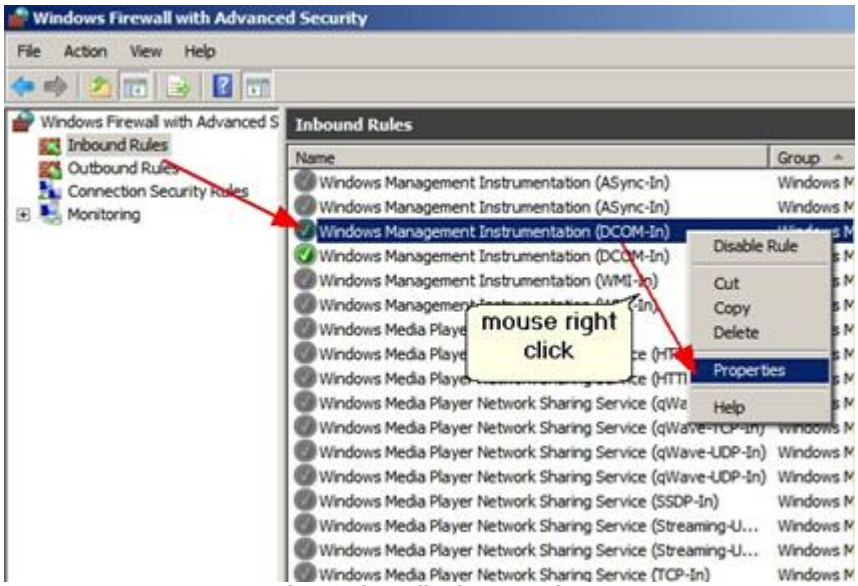


Fig. 12 Firewall rule properties

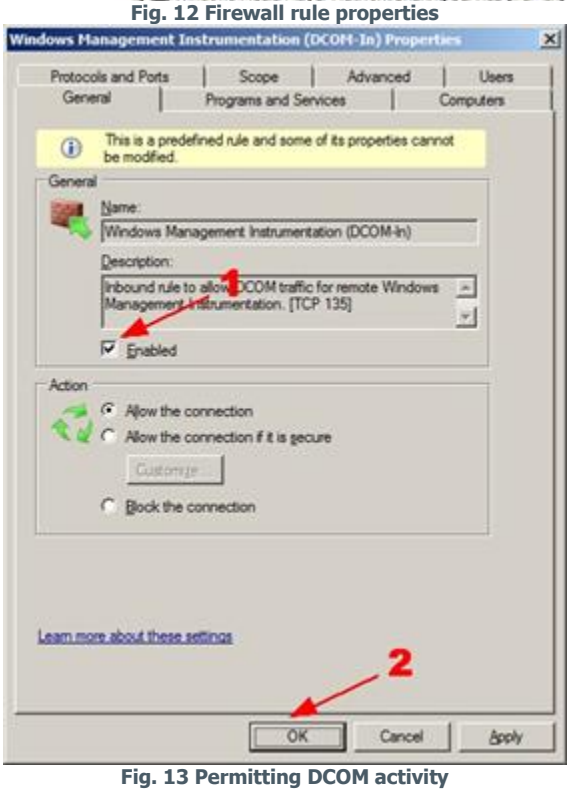


Fig. 13 Permitting DCOM activity

For Windows 7 users. If the "COM+ network access" or "DCOM" rule is not in the list, create two "Port" rules.

1. Port 135 rule for the TCP protocol;
2. Port 135 rule for the UDP protocol;

3.2 CREATING RULES FOR EVERY OPC SERVER

You need to permit activity for every OPC server running on this computer. Also, you should permit network activity for the OpcEnum system service that allows remote clients to receive the list of servers from this computer.

Below you can see an example of how to create a rule for OpcEnum. Rules for other applications are created in a similar way.

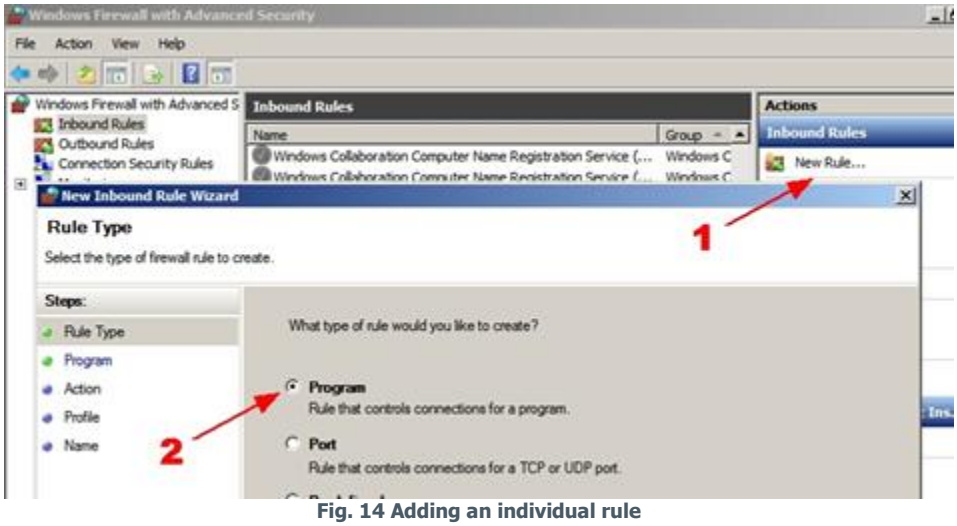


Fig. 14 Adding an individual rule

1. Select the "New Rule" action;
2. Select the "Program" rule type;
3. Click the "Next" button.

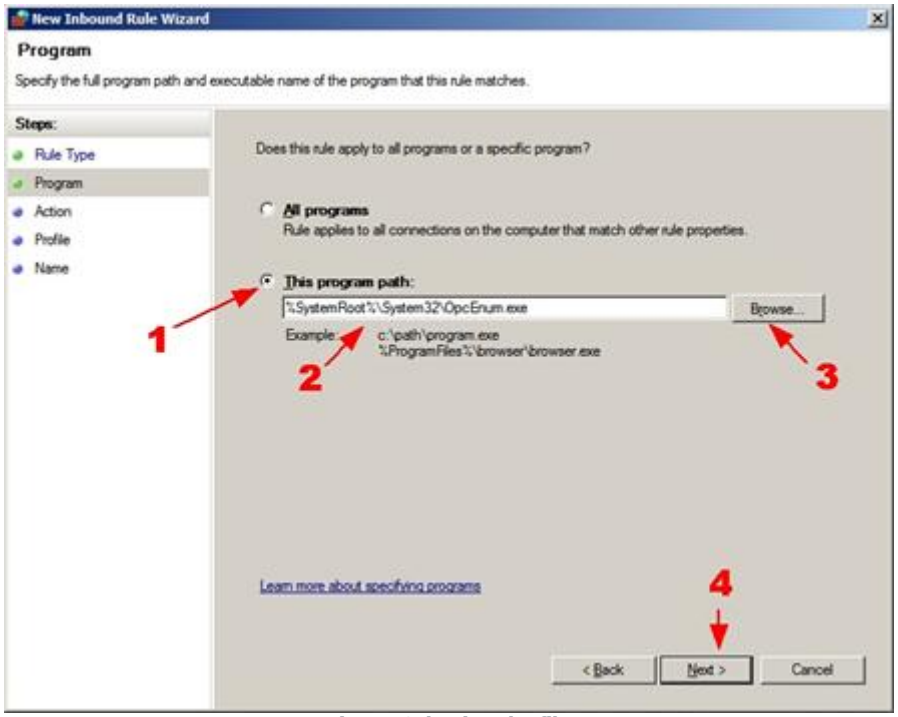


Fig. 15 Selecting the file

1. Select the "Program Path" option;
2. Specify the full path to the program and its file name;
3. You can select the program on the disk using the "Browse" button;
4. Click the "Next" button.

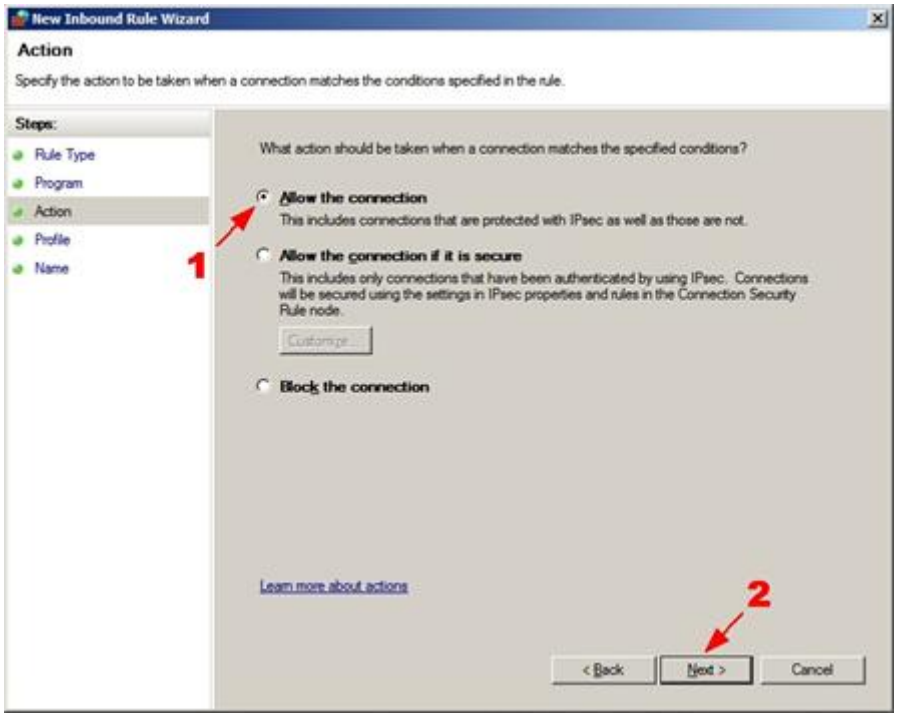


Fig. 16 Rule properties

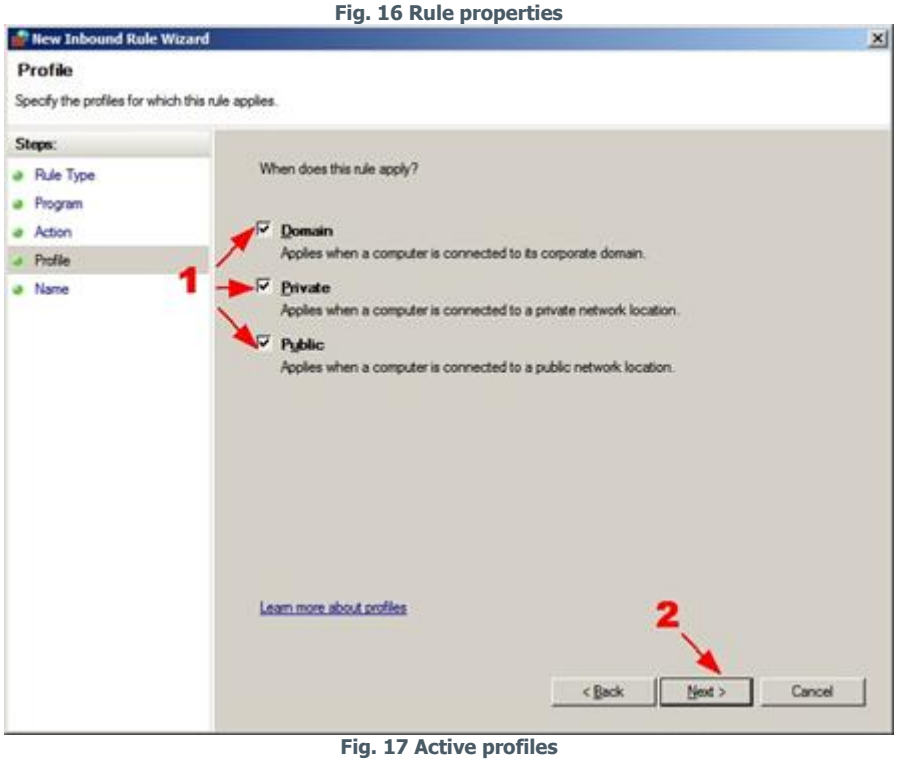


Fig. 17 Active profiles

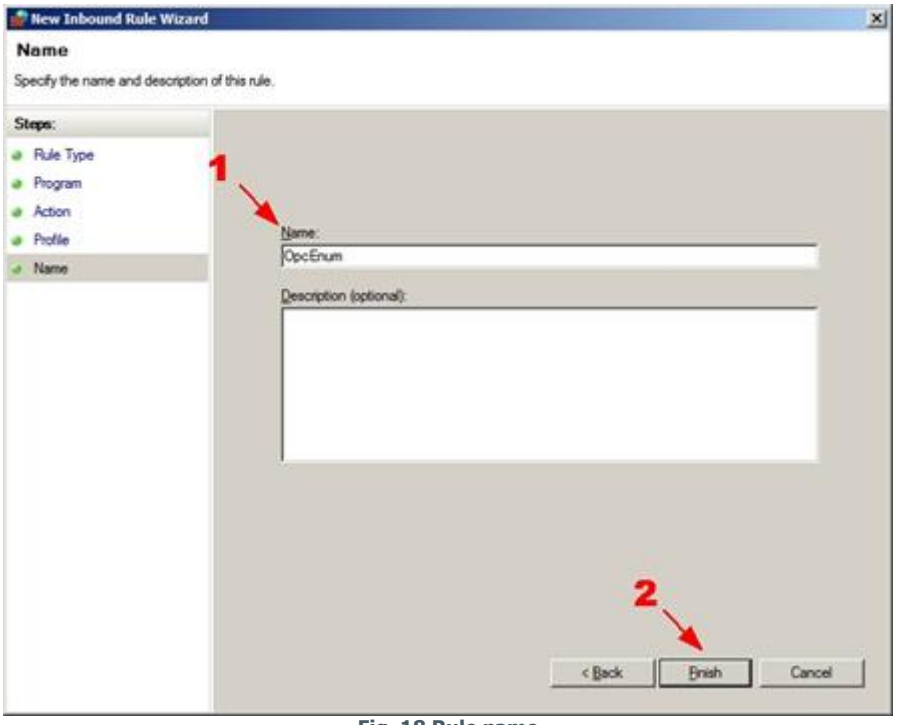


Fig. 18 Rule name

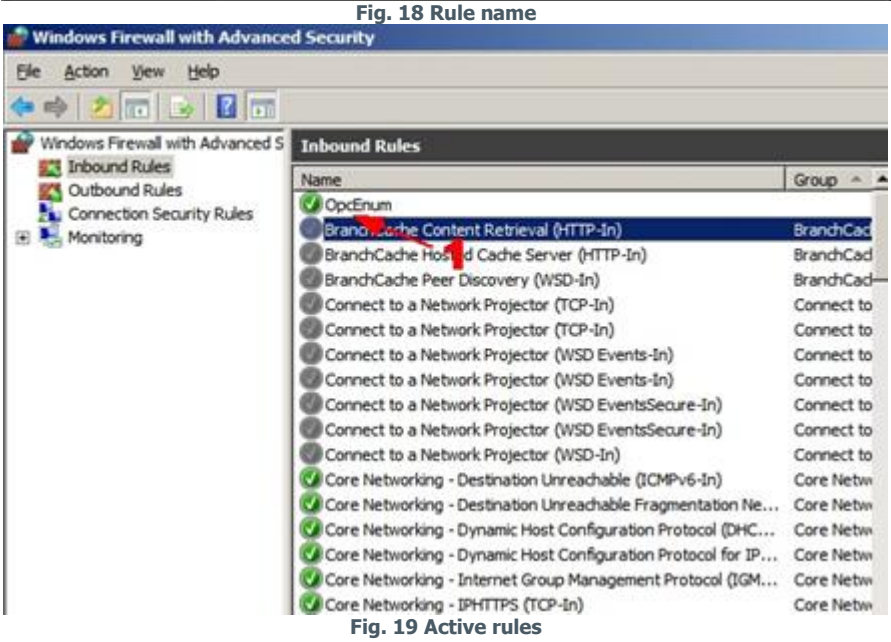
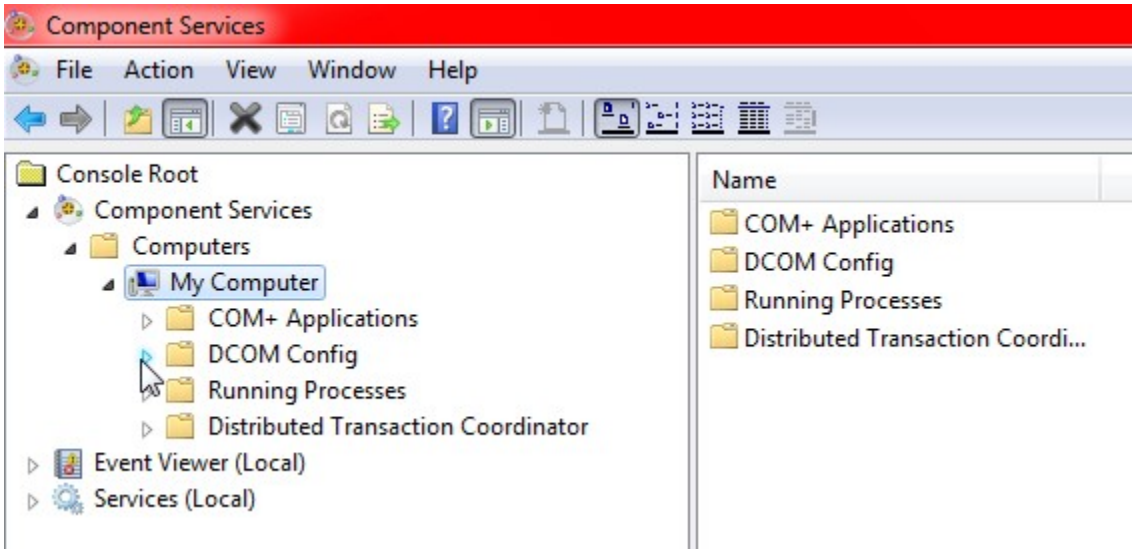
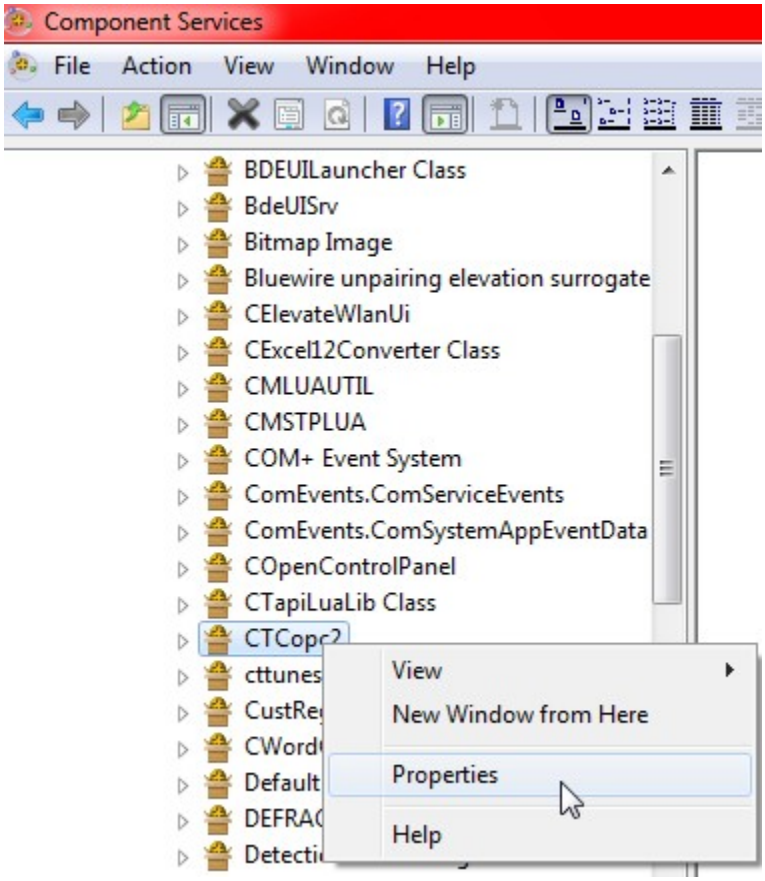


Fig. 19 Active rules

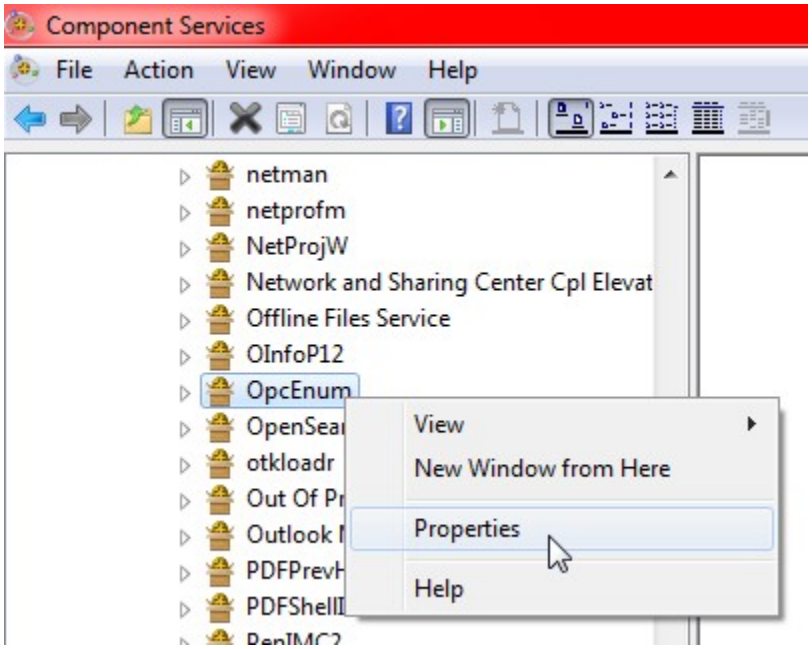
Note: Add CTCOpc.exe to the Windows Fire Wall exception screen.

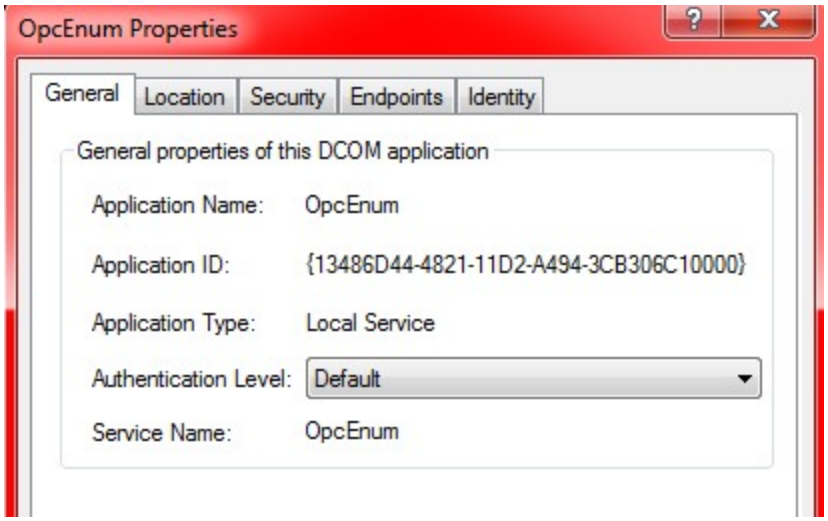
DCOM Configuration:

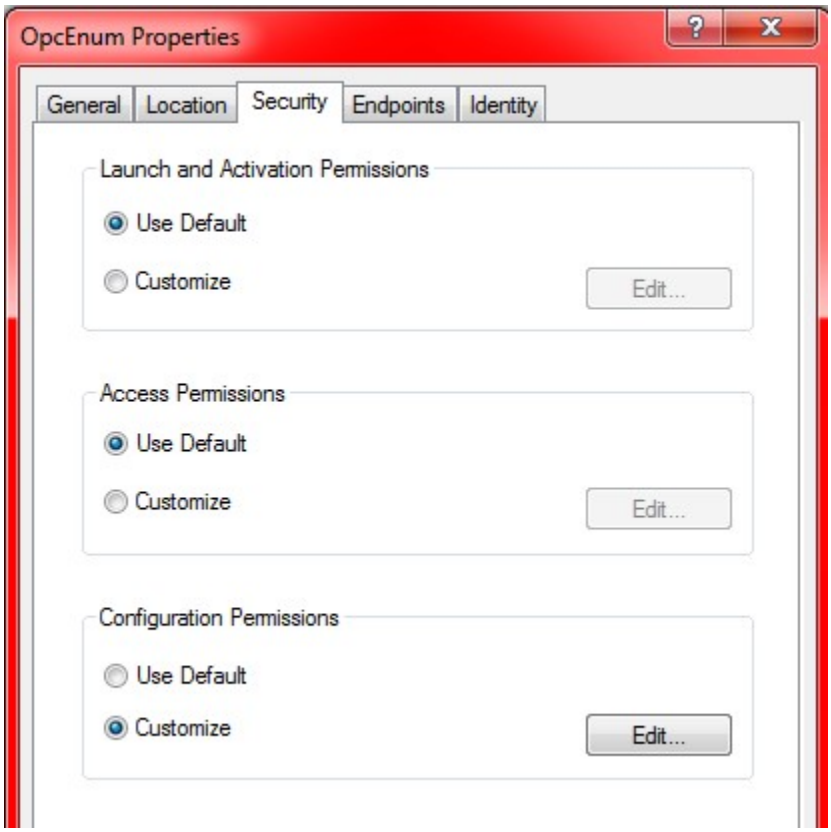




CTCopc2 Properties
General
Location
Security
Endpoints
Identi
Which user account do you want to use to run this application?
The interactive user.
The launching user.
This user.
User:
Browse...
Password:
Confirm password:
The system account (services only).


Component Services
File
Action
View
Window
Help
netman
netprofm
NetProjW
Network and Sharing Center Cpl Elevat
Offline Files Service
OInfoP12
OpcEnum
View
New Window from Here
Properties
Help


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: Default
Service Name: OpcEnum


OpcEnum Properties
General
Location
Security
Endpoints
Identity
Launch and Activation Permissions
Use Default
Customize
Edit...
Access Permissions
Use Default
Customize
Edit...
Configuration Permissions
Use Default
Customize
Edit...