SIEMENS

SIMATIC HMI

Using OPC via DCOM with Windows XP SP3

Readme

01/2010

Safety Guidelines

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠CAUTION

with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.

CAUTION

without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.

NOTICE

indicates that an unintended result or situation can occur if the corresponding information is not taken into account.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The device/system may only be set up and used in conjunction with this documentation. Commissioning and operation of a device/system may only be performed by **qualified personnel**. Within the context of the safety notes in this documentation qualified persons are defined as persons who are authorized to commission, ground and label devices, systems and circuits in accordance with established safety practices and standards.

Prescribed Usage

Note the following:

⚠WARNING

SIEMENS product may only be used for the applications described in the catalog or the technical description and only in connection with devices or components from other manufacturers which have been approved or recommended by Siemens. Correct, reliable operation of the product requires proper transport, storage, positioning and assembly as well as careful operation and maintenance.

Trademarks

All names identified by ® are registered trademarks of the Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

℗ 01/2010

Table of contents

1 Basic Settings

Abstract

The major goal of Windows XP Service Pack 3 is to reduce common available scenarios for malicious attack on Windows XP. The Service Pack will reduce the effect of most common attacks.

Although the paper is based on .best practices as judged by the authors, the OPC Foundation and the authors assume no responsibility for its accuracy or suitability for application by its readers.

User Administration

The same users with administrator rights must be set up on all (DCOM) computers. For the production of the users profiles these users must log in too.

Windows Firewall

The firewall exceptions can be specified at two main levels, the application level and the port and protocol level. To make any OPC client/server application work via DCOM, changes need to be made on both levels.

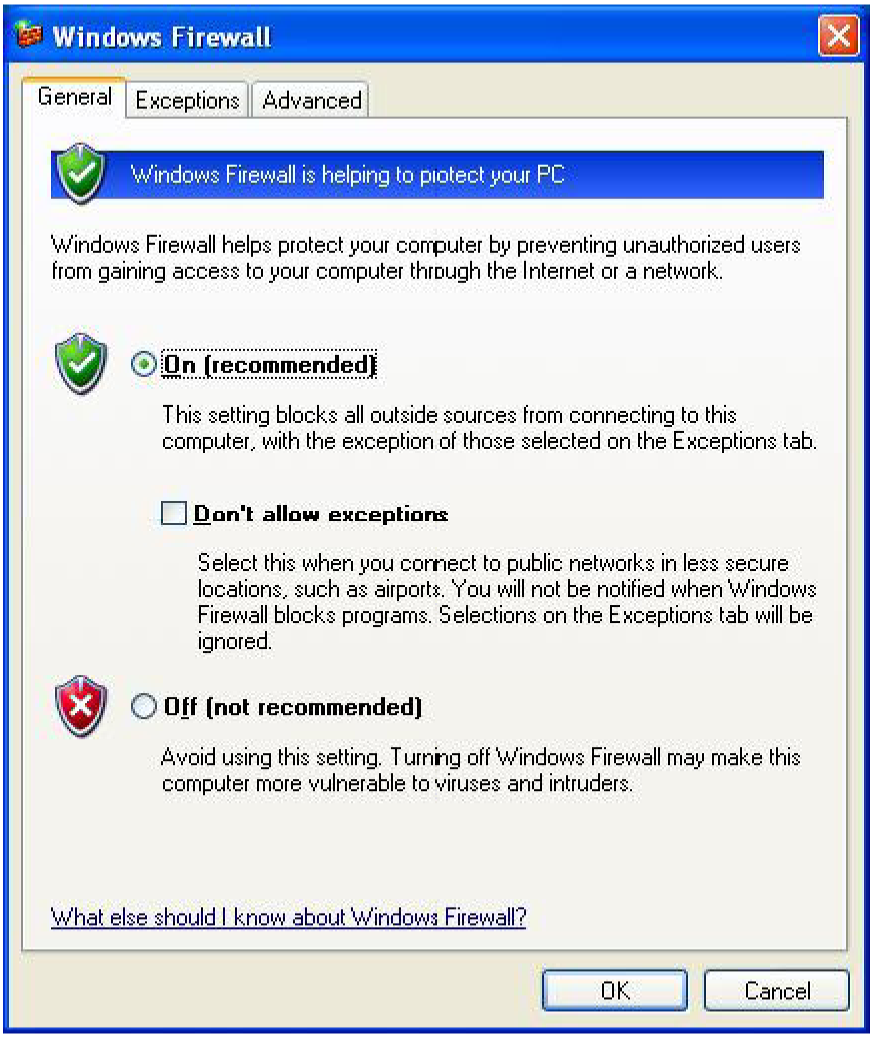
2 Configuring the firewall

2

Configuring the Firewall

1. By default the windows firewall is set to "On".

   It may be appropriate to permanently turn off the firewall if the machine is sufficiently protected behind a corporate firewall.



Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

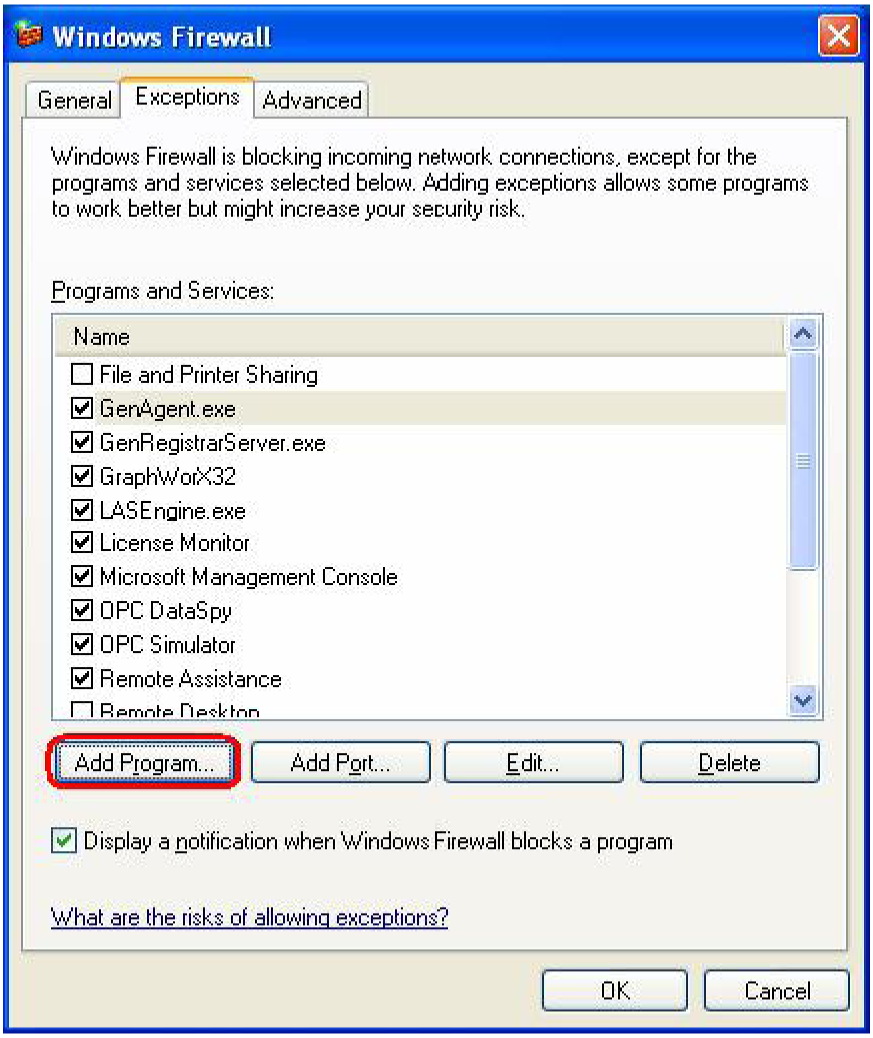
□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

○ Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

2. Select the "Exceptions tab" and add all OPC Clients andServers to the exception list. Also add Microsoft Management Console (used by the DCOM configuration utility in the next section) and the OPC utility OPCEnum.exe found in the Windows\System32 directory. Use the "Browse button" to find other executables installed on the computer.



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

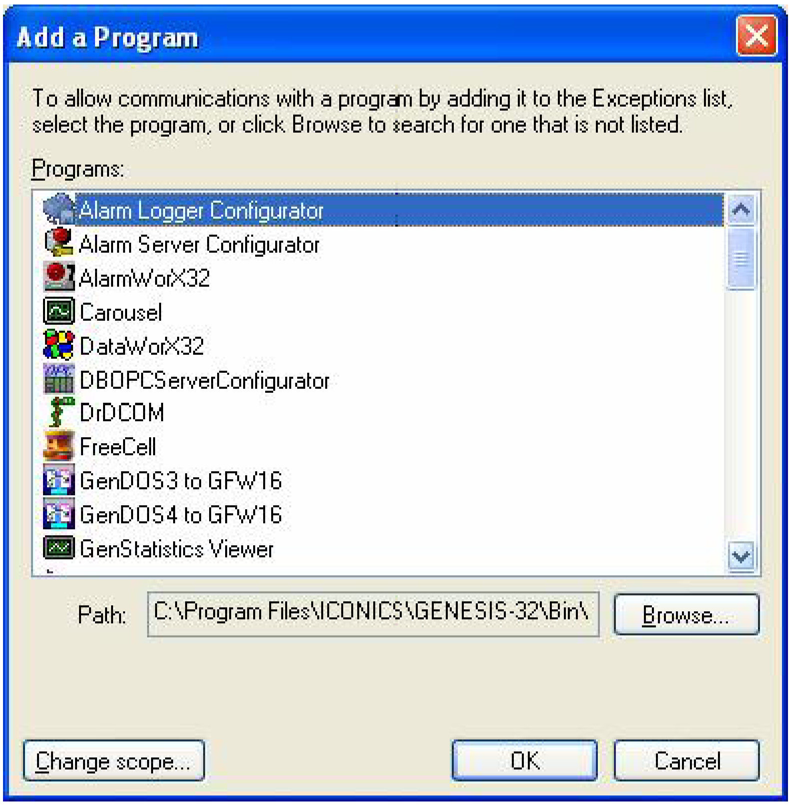
Name
□ File and Printer Sharing
☑ GenAgent.exe
☑ GenRegistrarServer.exe
☑ GraphWorX32
☑ LASEngine.exe
☑ License Monitor
☑ Microsoft Management Console
☑ OPC DataSpy
☑ OPC Simulator
☑ Remote Assistance
□ Remote Desktop

☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

Hinweis

Only EXE files are added to the exceptions list. For in-process OPC Servers and Clients (DLLs and OCXs) you will need to add the EXE applications that call them to the list instead.



Add a Program

To allow communications with a program by adding it to the Exceptions list, select the program, or click Browse to search for one that is not listed.

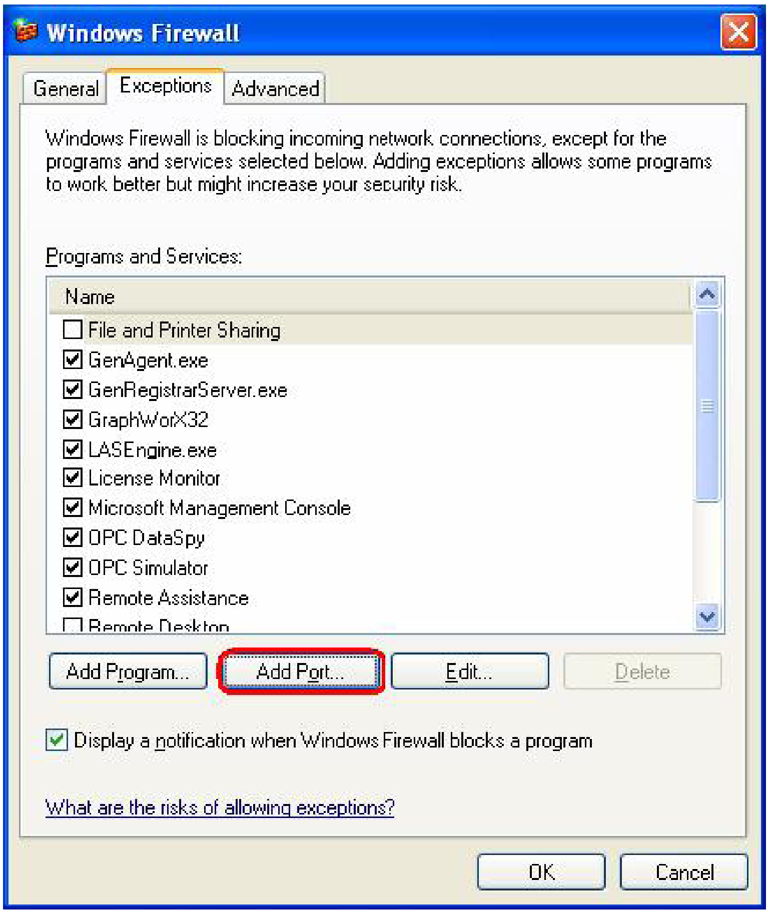
Programs:

- Alarm Logger Configurator
- Alarm Server Configurator
- AlarmWorX32
- Carousel
- DataWorX32
- DBOPCServerConfigurator
- DrDCOM
- FreeCell
- GenDOS3 to GFW16
- GenDOS4 to GFW16
- GenStatistics Viewer

Path: C:\Program Files\ICONICS\GENESIS-32\Bin\

3. Add TCP port 135 as it is needed to initiate DCOM communications, and allow for incoming echo requests.

4. In the "Exceptions tab" of the Windows Firewall, click on Add Port.



Windows Firewall

General | Exceptions | Advanced

Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name
□ File and Printer Sharing
☑ GenAgent.exe
☑ GenRegistrarServer.exe
☑ GraphWorX32
☑ LASEngine.exe
☑ License Monitor
☑ Microsoft Management Console
☑ OPC DataSpy
☑ OPC Simulator
☑ Remote Assistance
□ Remote Desktop

☑ Display a notification when Windows Firewall blocks a program

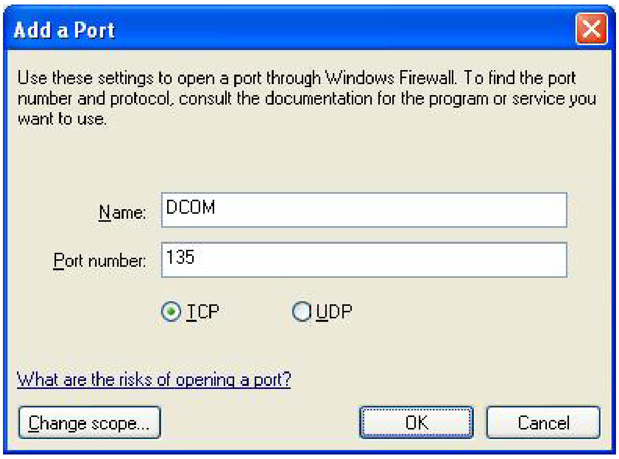
What are the risks of allowing exceptions?

5. In the Add a Port dialog, fill out the fields as follows:

Name: DCOM

Port number: 135

6. Choose the TCP radio button



Add a Port

Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.

Name: DCOM

Port number: 135

● TCP ○ UDP

What are the risks of opening a port?

3 Configuring DCOM

Configuring DCOM

DCOM has settings for: -the machine default -each server.

For using OPC via DCOM the simplest possibility is the configuration over machine default settings.

The settings mentioned in the following must be executed on client and servers side.

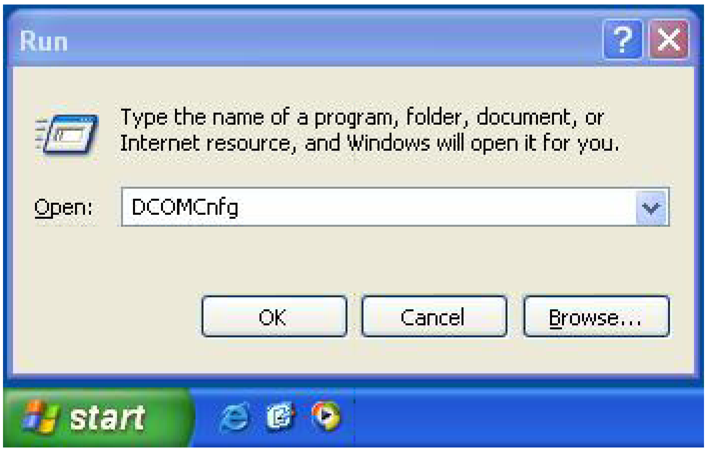
4 Configuring DCOM Machine Default

4

Configuring DCOM Machine Default

Follow these steps to configure the DCOM machine default settings for OPC Communications using Windows XP SP3:

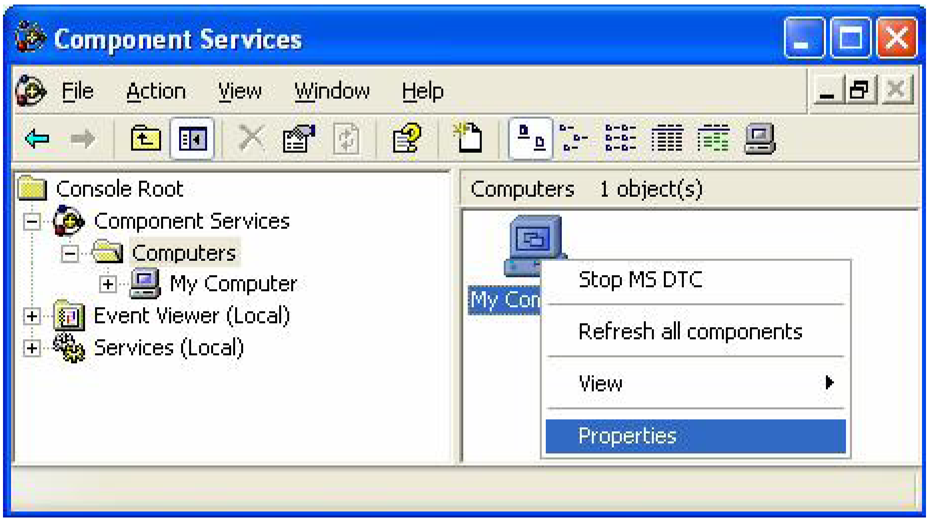
1. Go to Start -> Runt and type DCOMCnfg and click on OK.



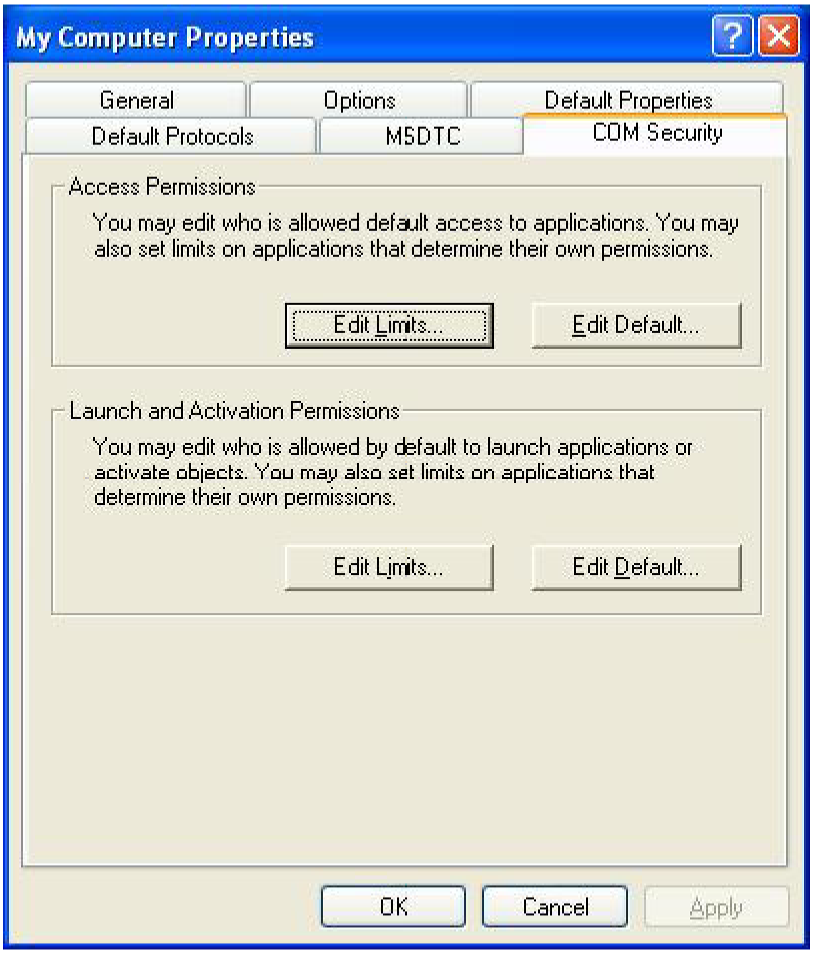
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: DCOMCnfg

2. Click on Component Services under the Console Root to expand it.
3. Click on computers under Component Services to expand it.
4. Right click on My Computer in the pane on the right and select Properties.



5. Go to the COM Securiyt tab and note these are the four permission configurations that we will have to edit:



Access Permissions

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

Launch and Activation Permissions

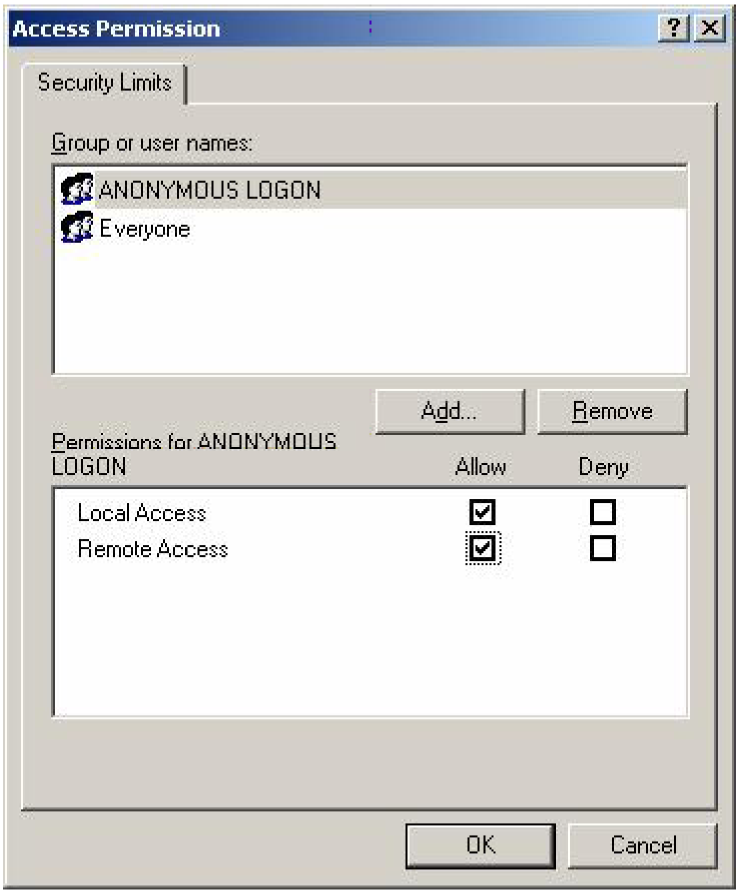
You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions.

Edit the Limits for Access and Launch:

- Access Permissions

  If not exsists, inserting the users "Administrators" and "Everyone".

  For all users the remote access and the local access must be activated.



Group or user names:

- ANONYMOUS LOGON
- Everyone

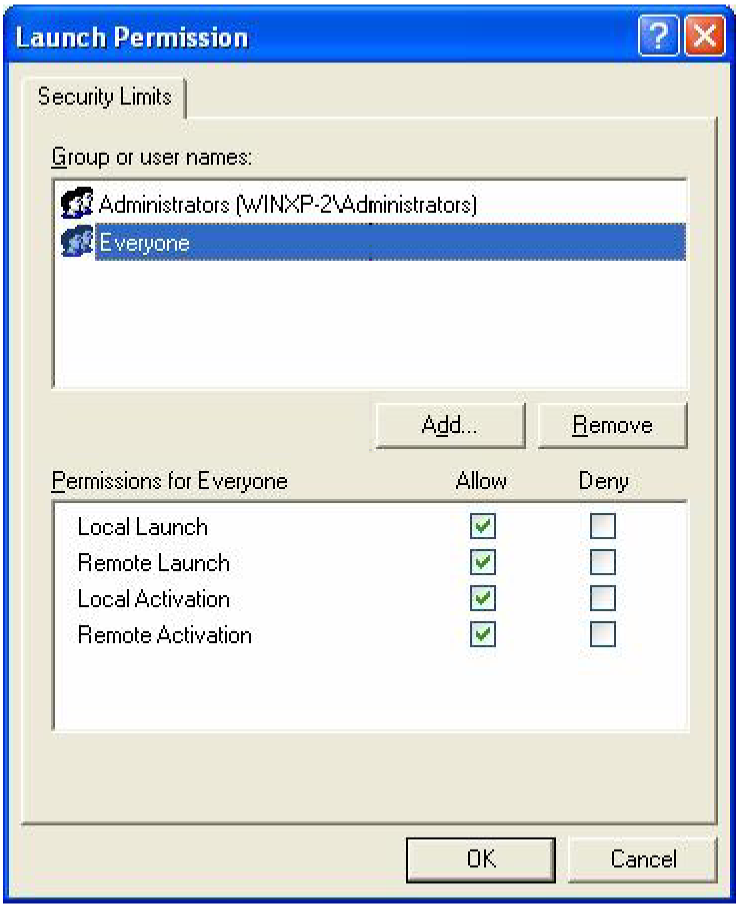
Permissions for ANONYMOUS LOGON

	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

- Launch and Activation Permissions

  If not exsists, inserting the users "Administrators" and "Everyone".

  For all users the remote access and local access must be activated.



Launch Permission

Security Limits

Group or user names:

- Administrators (WINXP-2\Administrators)
- Everyone

Add... Remove

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

OK Cancel

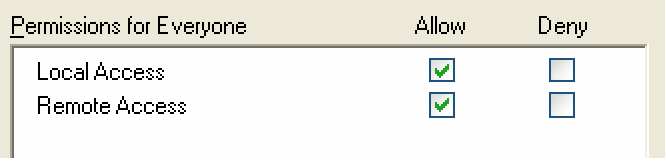
Edit Default Permissions for Access and Launch:

- Access Permissions

  If not exsists, inserting the users "Administrators" and "Everyone".

  For each user (or group) that participates in OPC communication (e.g. .OPC Users), make sure that both the Local Allow and Remote Allow checkboxes are both checked.

  Access Permissions per user:



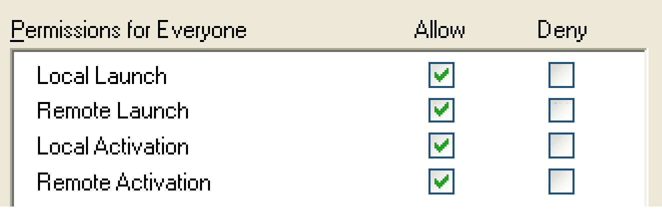
Permissions for Everyone	Allow	Deny
Local Access	☑	□
Remote Access	☑	□

- Launch and Activation Permissions

  If not exsists, inserting the users "Administrators" and "Everyone".

  For each user (or group) that participates in OPC communication (e.g. .OPC Users), make sure that both the Local Allow and Remote Allow checkboxes are both checked.

Launch and Activation permissions per user:



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