

# DCOM settings for computer-to-computer communication between OPC servers and OPC clients

## 1. Introduction

Under OPC DA, the "dcomcnfg" service program is used for computer-to-computer communication between OPC clients and OPC servers.

This service program will look and behave differently depending on the operating system used (Windows 98 / 2000 / XP / XP SP2). This document refers to Windows 2000 and Windows XP SP2. Aspects which are relevant only to Windows XP SP2 are noted in the text.

DCOM permits only authenticated access between computers. We recommend registering the computers in the same domain and specifying a user group (e.g., "OPC Users") for OPC communication on all computers.



**Note:**

"dcomcnfg" affects the operating system at a very deep level. Faulty configuration can cause the operating system to become unstable or cease functioning. The settings specified here will decrease the security of your system.

As an alternative, you can use the [Softing OPC Tunnel](#) tool. No DCOM settings are necessary with this. The last section briefly introduces this tool.



**Note:**

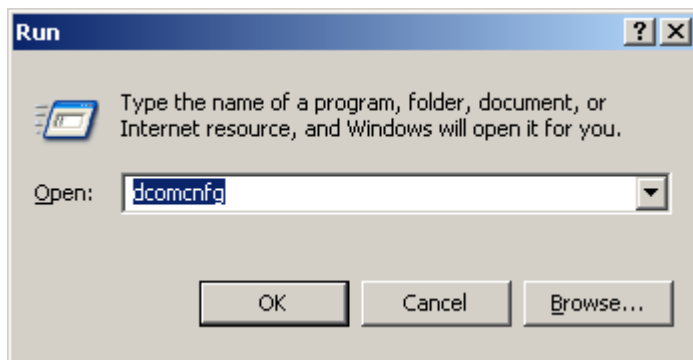
In certain circumstances, "dcomcnfg" may issue DCOM configuration warnings. You will be asked whether you want to automatically correct discrepancies in the DCOM configuration. This is not necessary for the settings described here.

## 2. DCOM settings for system-wide security parameters

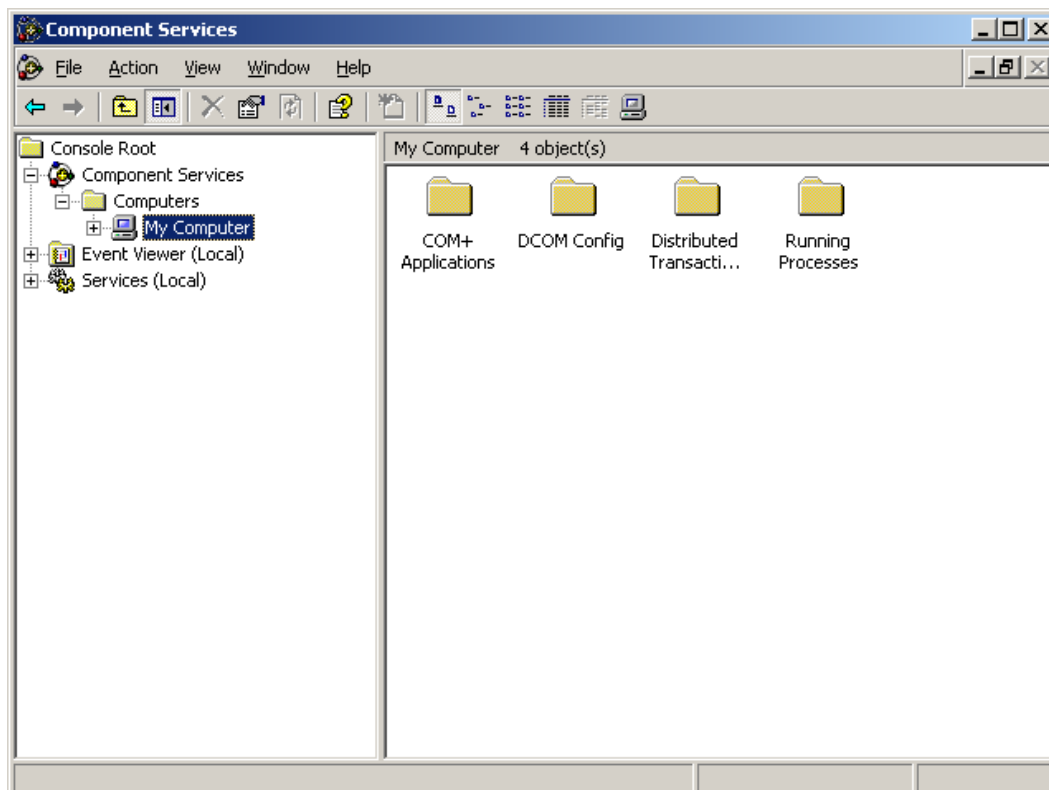
The following preferences should be set on the client computer and the server computer.

### 2.1. Start "dcomcnfg"

- Log in with administrator rights
- Open the Windows start menu
- Select "Run"
- Enter "dcomcnfg"
- Click "OK"



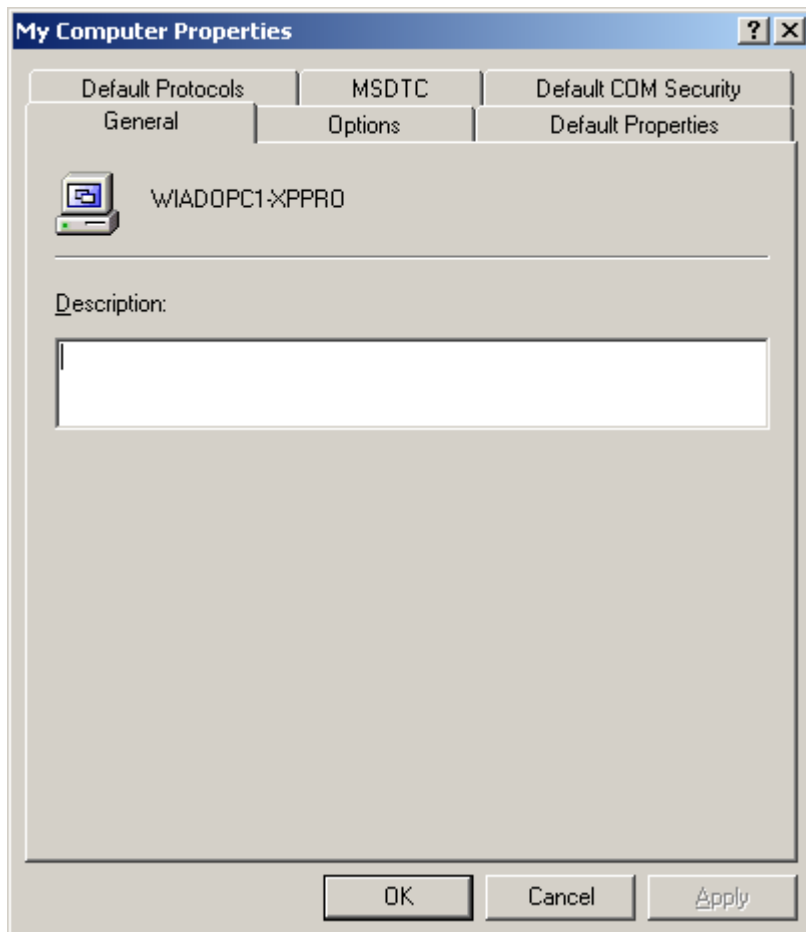
**Image 1: "Run" dialogue in Microsoft Windows**



**Image 2: "dcomcnfg" start page**

## 2.2. Open the "My Computer Properties" dialogue

- Select "Console Root / Component Services / Computers / My Computer" in the tree view
- Open the context menu (right mouse button) → Properties



**Image 3: "My Computer Properties" start page**

## 2.3. Set "Default Properties"

- Select the "Default Properties" tab
- Enable Distributed COM on this computer
- Default Authentication Level: None
- Default Impersonation Level: Impersonate

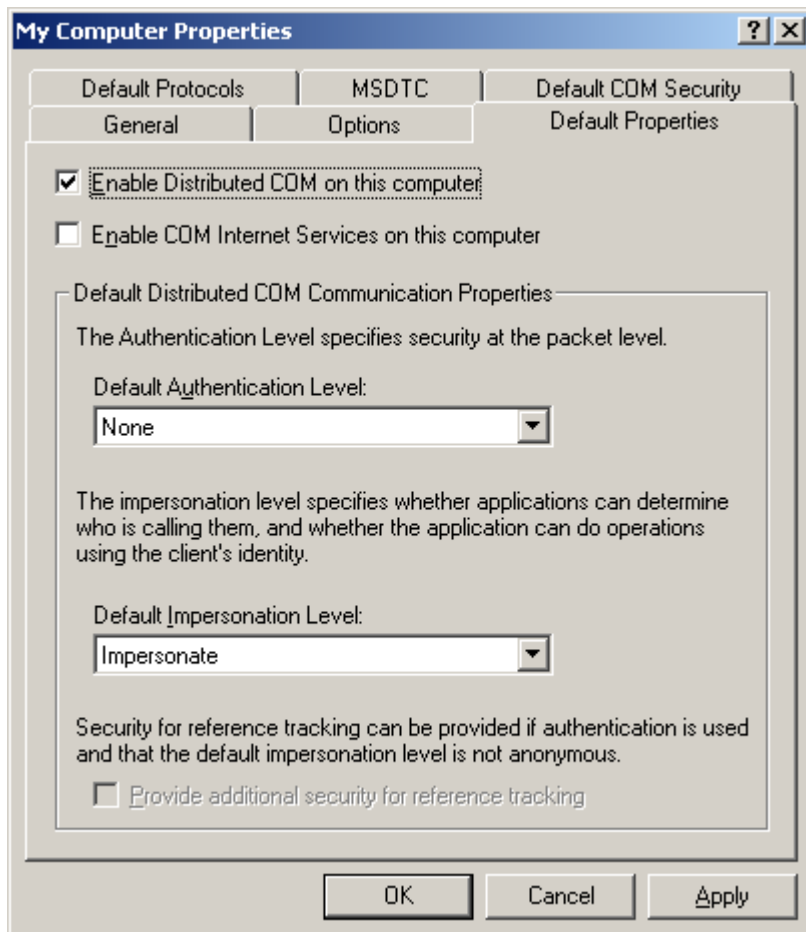


Image 4: "Default Properties" tab



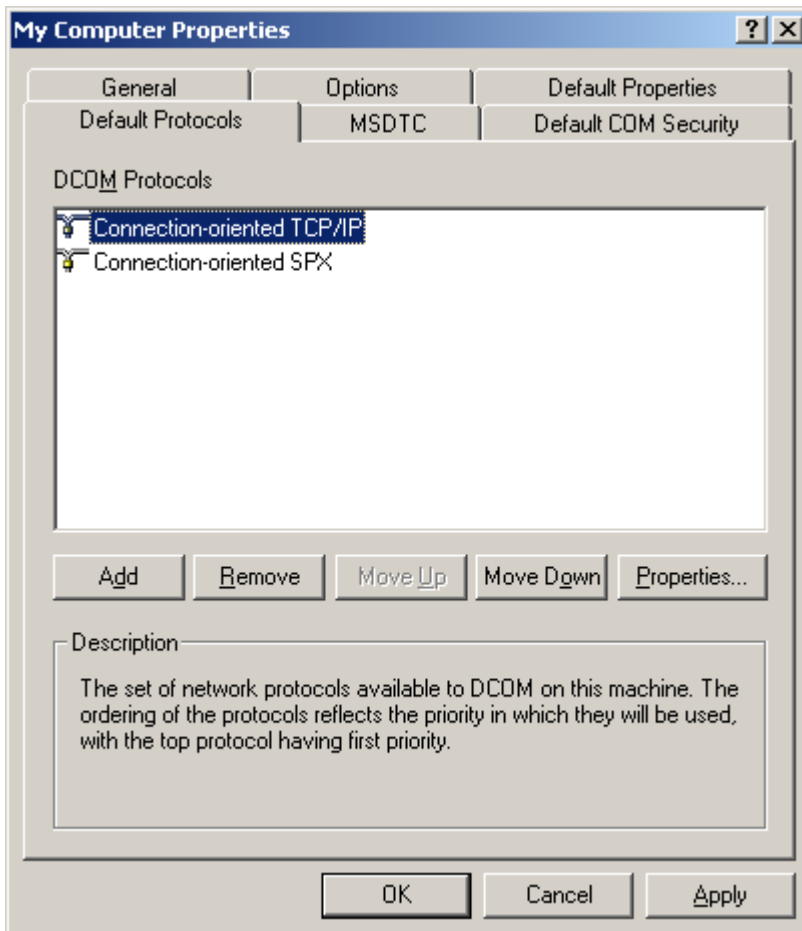
### Note:

**Default Authentication Level:** Indicates when authentication should be carried out (never, when connecting, for every packet, etc.)

**Default Impersonation Level:** Indicates whether applications can determine who is calling them and carry out operations using the client's identity.

## 2.4. Set "Default Protocols"

- Select the "Default Protocols" tab
- Check that "Connection-oriented TCP/IP" is in the first position



**Image 5: "Default Protocols" tab**



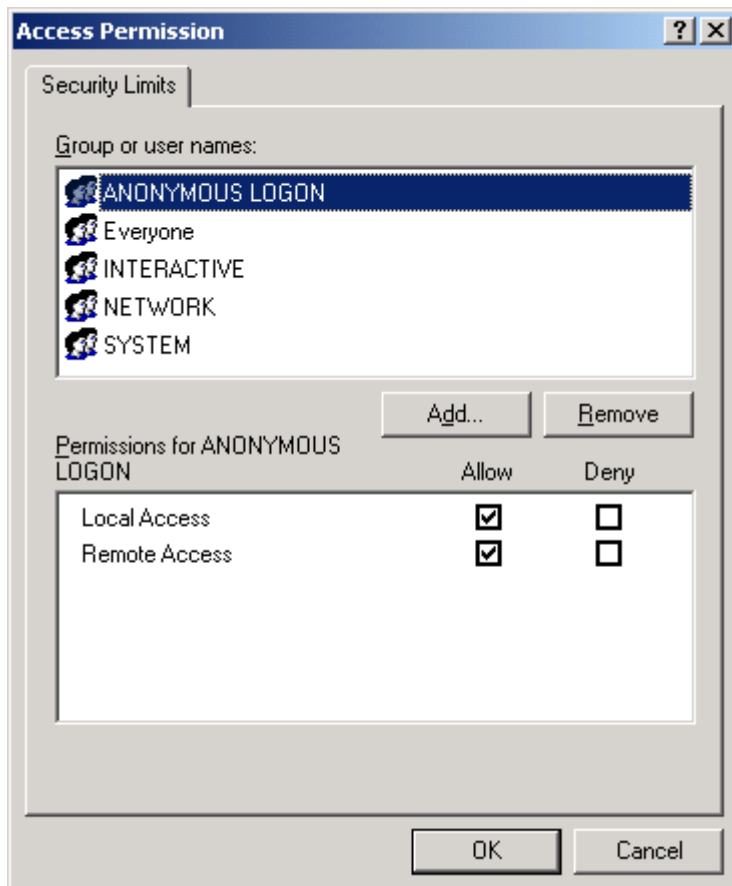
**Note:**

Windows checks the protocols in the order in which they are displayed here. If "Connection-oriented TCP/IP" is not in the first position, there will be delays. If the time it takes to establish a connection is longer than the time allocated for the server, the server will not be able to start.

A high number of DCOM protocols will lead to unnecessary delays if the connection is broken. Unnecessary entries should therefore be deleted.

## 2.5. Set "COM Security"

- Select the "COM Security" tab
- Click the "Access Permission: Edit Limits" button
- Add "ANONYMOUS LOGON", "Everyone", "INTERACTIVE", "NETWORK" and "SYSTEM" as user names (see note)
- Allow "Local Access" and "Remote Access" for these user names
- Click "OK"



**Image 6: Setting "Access Permission"**



### Note:

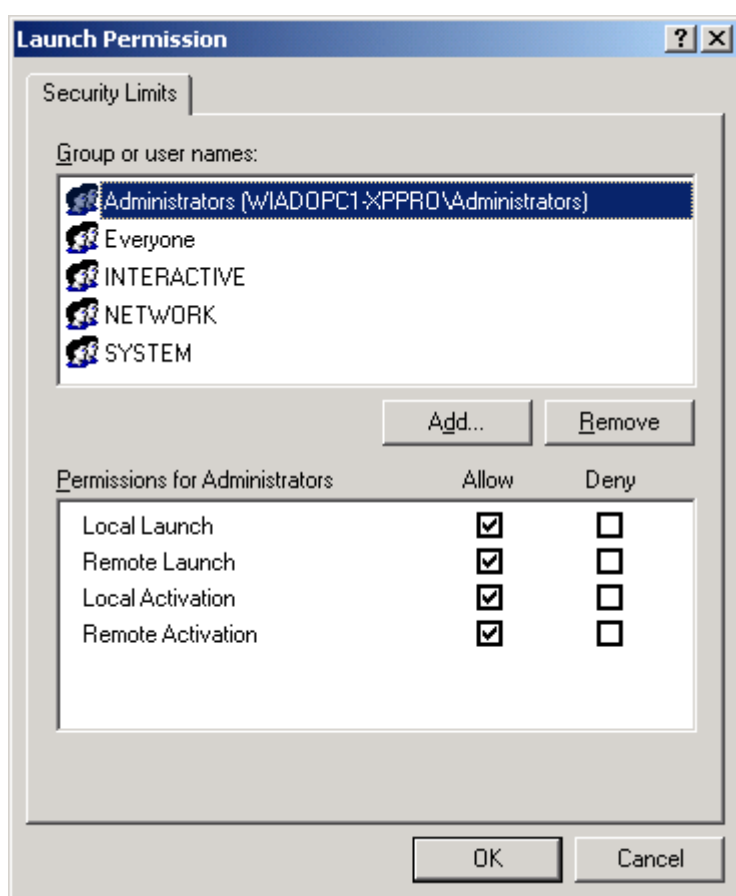
If a desired group or user name does not appear in the selection window, it can be added as follows:

- Click "Add"
- Click "Advanced"
- Click "Find Now"
- Mark "Group or user names" (multiple selections are possible by holding down the "Ctrl" key)
- Click "OK"


**Note:**

The "Everyone" user group contains all users (local and domain). You can also create permissions for a group (e.g., "OPC Users") and add all OPC users to this group. This group must then exist on the server computer and client computer. Windows does not allow empty passwords for DCOM communication.

- Launch and Activation Permissions: Click "Edit Limits"
- Add "Everyone", "INTERACTIVE", "NETWORK" and "SYSTEM" as user names
- Allow "Local Launch", "Remote Launch", "Local Activation" and "Remote Activation" for these users and the administrator
- Click "OK"



**Image 7: Setting "Launch Permission"**

- Access Permission: Click "Edit Default"
- Add "Everyone", "INTERACTIVE", "NETWORK" and "SYSTEM" as user names
- Allow "Local Access" and "Remote Access" for these users and the administrator
- Click "OK"
  
- Launch and Activation Permissions: Click "Edit Default"
- Add "Everyone", "INTERACTIVE", "NETWORK" and "SYSTEM" as user names
- Allow "Local Launch", "Remote Launch", "Local Activation" and "Remote Activation" for these users and the administrator
- Click "OK"
  
- "My Computer Properties" dialogue: Click "OK"

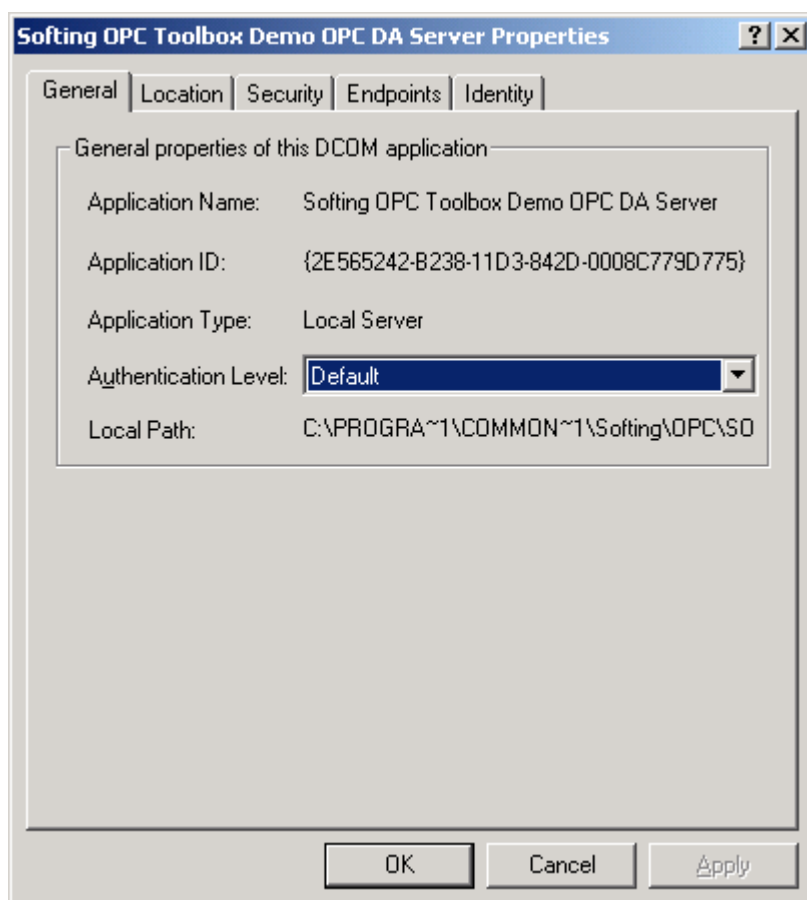


### 3. DCOM settings for application-specific security parameters

Carry out the following steps for your OPC server and OPCenum.exe on the server computer.

#### 3.1. Open the "Properties" dialogue for an OPC server

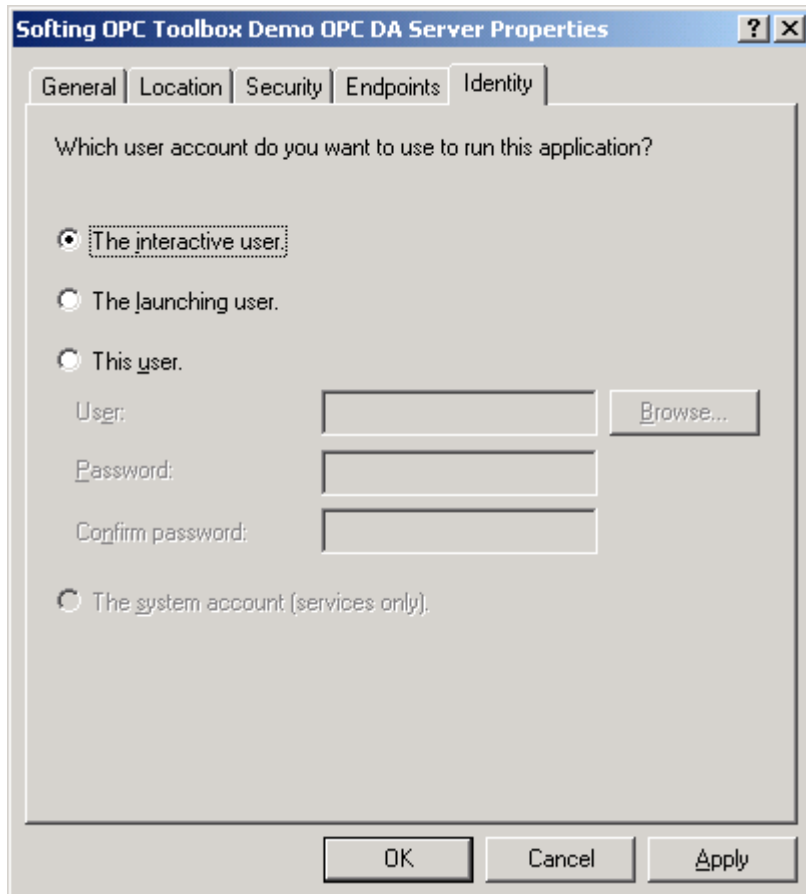
- Start "DCOM Config" (see section 2 DCOM settings for system-wide security parameters)
- Select "Console Root / Component Services / Computers / My Computer / DCOM Config" in the tree view
- Select DCOM server (right side)
- Open context menu (right mouse button) → Properties



**Image 8: Application-specific start page for DCOM configuration**

### 3.2. Identity

- Select the "Identity" tab
- Select "The interactive user"



**Image 9: Setting the identity**



**Note:**

If an OPC server is running as a "service", the "interactive user" and "launching user" lines will be grayed out. In this case, choose "This user" and enter a user (preferably one from the "OPC Users" group) (see note in section 2, "DCOM settings for system-wide security parameters")

### 3.3. Set security preferences

- Select the "Security" tab
- Launch and Activation Permissions: Select "Use Default"
- Access Permissions: Select "Use Default"
- Configuration Permissions: Select "Customize" and click "Edit"
- Add "Everyone", "INTERACTIVE", "NETWORK" and "SYSTEM" as user names
- Allow "Full Control" and "Read" for these users and the administrator
- Click "OK"



**Note:**

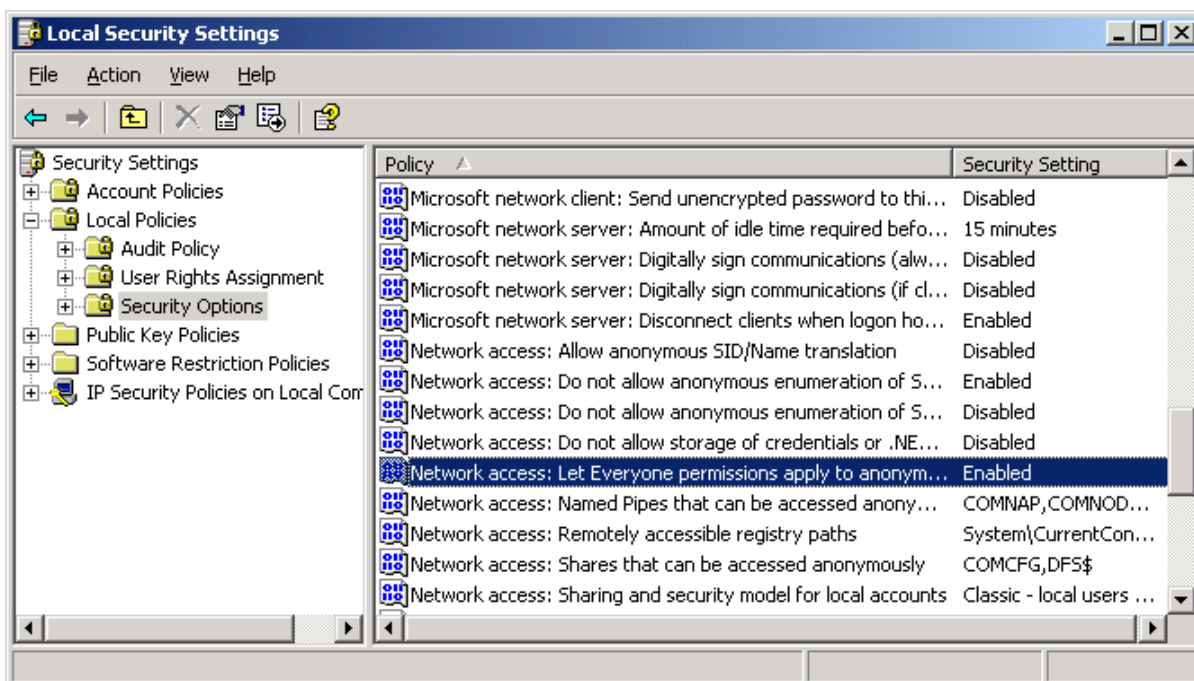
In order to enable the "dcomcnfg" settings, the OPC server and OPC client must be restarted.

## 4. Activating guest access

This section is only relevant to Windows XP. With the standard XP installation, users are authenticated on remote computers as guests. This means that a DCOM client will not be able to connect to a server until guest access has been activated and the guest has sufficient permissions to access the server.

The following preferences should be set on the client computer and the server computer.

- Open the Windows start menu
- Select "Settings / Control Panel"
- Select "Administrative Tools"
- Select "Local Security Policy"
- Select "Local Policies / Security Options" in the tree view
- Double-click "Network access: Sharing and security model for local accounts"
- Select "Classic – local users authenticate as themselves"
- Double-click "Network access: Let Everyone permissions apply to anonymous users"
- Select "Enabled"



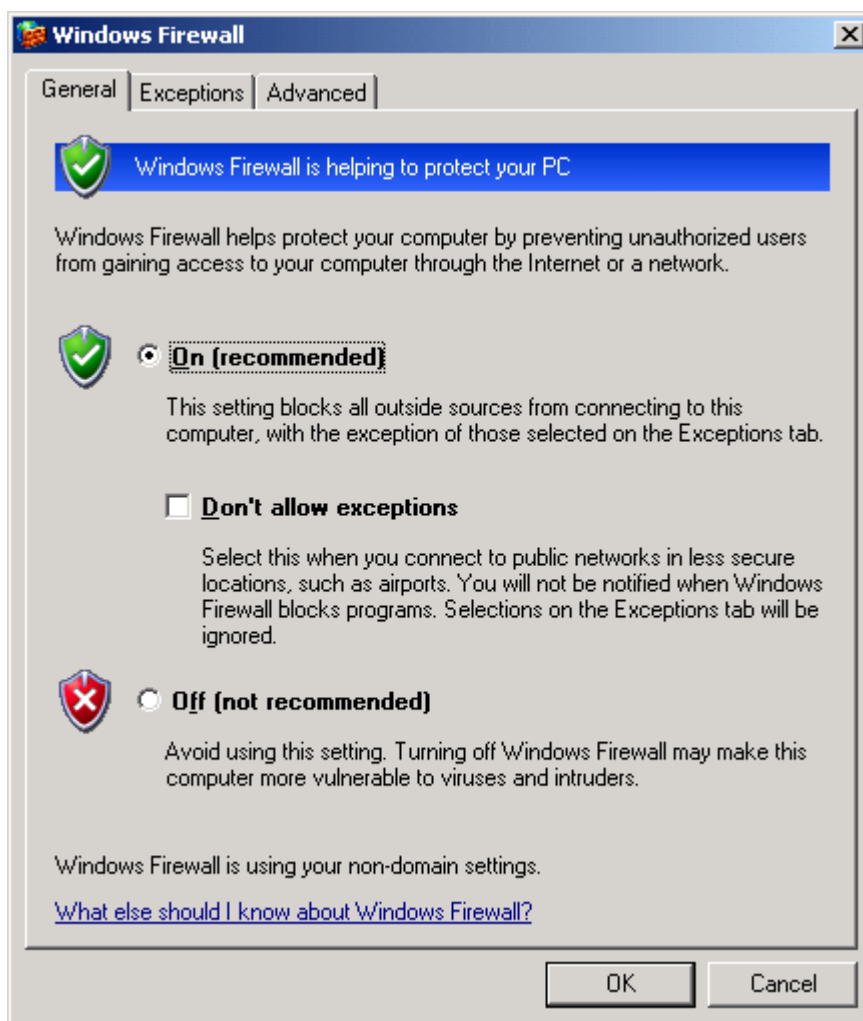
**Image 10: Establishing "Local Security Settings"**

## 5. Configuring the Windows Firewall

This section refers to the firewall in Windows XP SP2. However, these settings generally apply to all other firewalls as well. The configuration should be carried out on the client computer and the server computer.

### 5.1. Start "Windows Firewall" configurator

- Open the Windows start menu
- Select "Settings / Control Panel"
- Select "Windows Firewall"



**Image 11: The Windows Firewall**

## 5.2. Specify "Exceptions"

- Select the "Exceptions" tab
- Click "Add Program"
- Add the following programs:
  - o All OPC clients / OPC servers
  - o Microsoft Management Console
  - o "OPCEnum.exe" (Windows/System32)



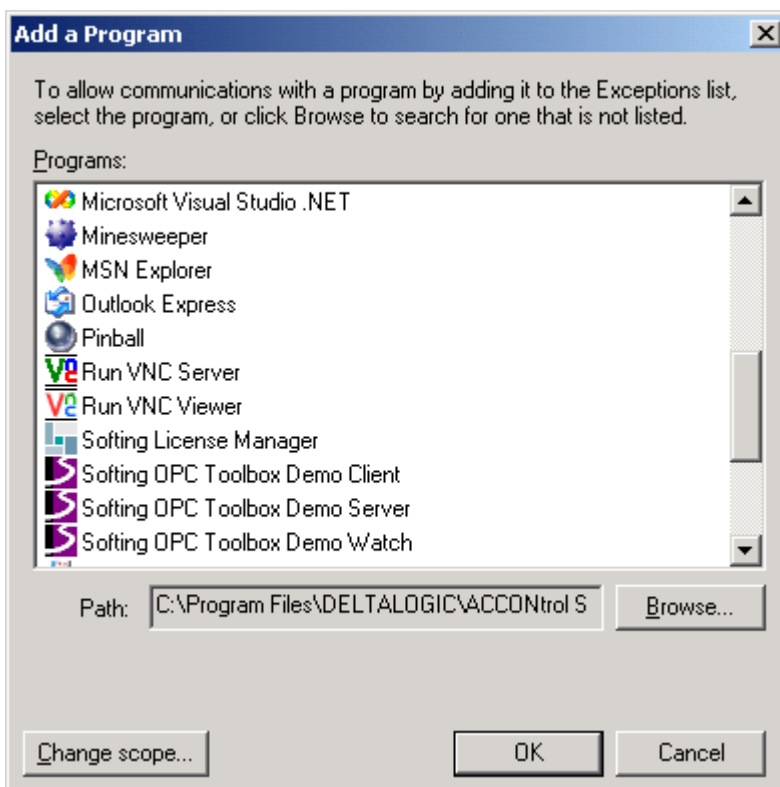
### Note:

Not all applications are shown in the "Add a Program" dialogue. Other applications can be found using the "Browse" button.



### Note:

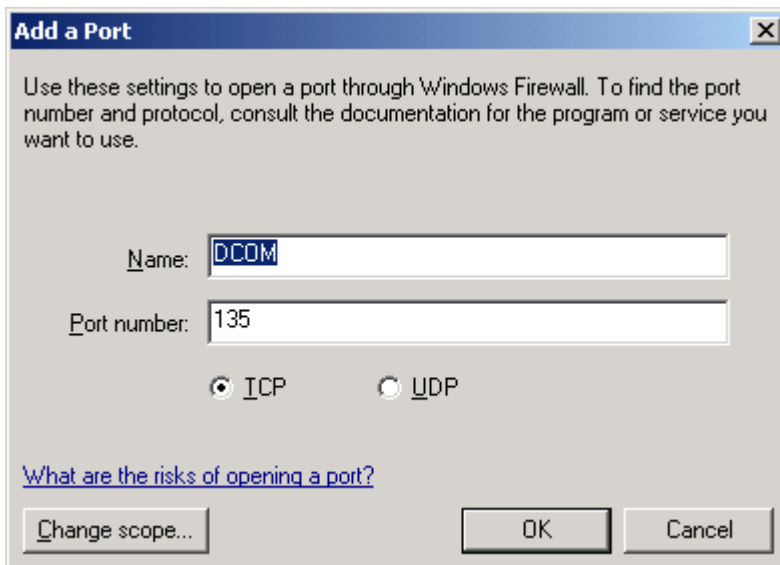
Only \*.exe files are included in the exceptions list. For an in-process server, please select the application which the server calls.



**Image 12: Specifying exceptions**

### 5.3. Open port

- Select the "Exceptions" tab
- Click "Add Port"
- Set the following preferences:
  - o Name: "DCOM"
  - o Port number: "135"
  - o Select "TCP" radio button
- Click "OK"



**Image 13: Opening a port for DCOM**



**Note:**

Opening port 135 creates a critical security hole. This allows applications to carry out remote procedure calls over the network and thus influence Windows components. This creates a gateway for many computer viruses. Please ensure that port 135 remains closed between your company network and the Internet.

## 6. DCOM under Windows CE

Under Windows CE, the security settings for computer-to-computer OPC communication are even more restrictive. There is also no program available for DCOM configuration. It is therefore impossible to provide a generic description here. If you have any questions, please contact our support team ([support.automation@softing.com](mailto:support.automation@softing.com)).

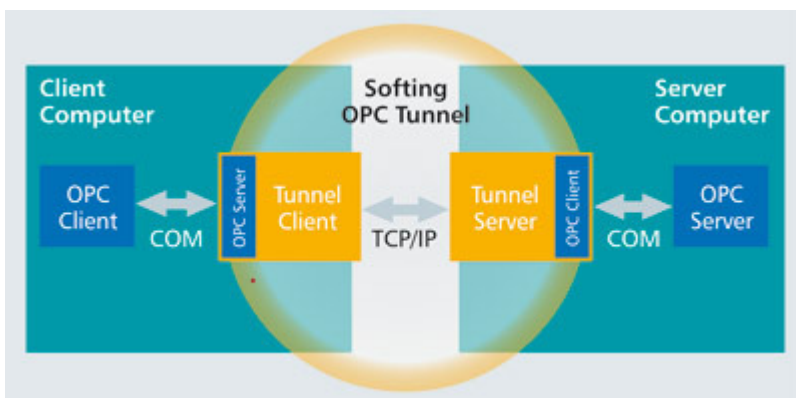
## 7. OPC Tunnel connector tool

The OPC Tunnel is a "DCOM bypass" which enables communication between OPC components on networked computers. The OPC Tunnel must be installed on both the OPC client computer and the OPC server computer.

Communication between the client- and server-side OPC Tunnels takes place via a TCP/IP connection which can be encrypted. In this way, data exchanged between the client and server applications is "tunneled" through TCP/IP. DCOM is completely circumvented.

Configuration is carried out using a self-explanatory assistant. Essentially, configuration involves defining the IP address of the server computer and a port for TCP/IP communication.

The OPC Tunnel is available for Windows NT4, 2000, XP, 2003 and Windows CE, and it supports Data Access 1.0a, 2.05 and 3.0, as well as Alarms&Events 1.10.



**Image 14: Computer-to-computer communication with the OPC Tunnel**