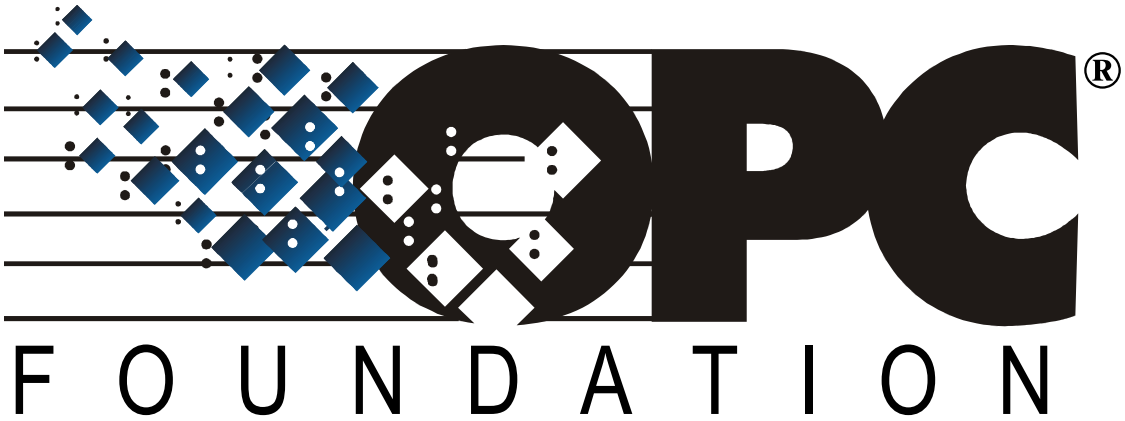


Using OPC via DCOM
with
Microsoft Windows XP Service Pack 2

Version 1.10

Karl-Heinz Deiretsbacher, Siemens AG

Jim Luth, ICONICS, Inc.
OPC Foundation Technical Director

Rashesh Mody, Invensys/Wonderware
OPC Foundation Chief Architect

Kurt T Haus, Advosol Inc.

Abstract

The major goal of Windows XP Service Pack 2 is to reduce common available scenarios for malicious attack on Windows XP. The Service Pack will reduce the effect of most common attacks in four ways:

1. Improvement in shielding Windows XP from the network
    a. RPC and DCOM communication enhancements
    b. Enhancements to the internal Windows firewall
2. Enhanced memory protection
3. Safer handling of e-mail
4. Internet Explorer security enhancements.

Most OPC Clients and Servers use DCOM to communicate over a network and thus will be impacted due to the changes in Service Pack 2. When Service Pack 2 is installed with its default configuration settings, OPC communication via DCOM will cease to work. This paper describes the settings necessary to restore OPC communication when using XP Service Pack 2 (SP2).

SP2 includes many changes and security enhancements, two of which directly impact OPC via DCOM. First new DCOM limit settings have been added. Secondly the software firewall included with XP has been greatly enhanced and is turned on by default.

Since the callback mechanism used by OPC essentially turns the OPC Client into a DCOM Server and the OPC Server into a DCOM Client, the instructions provided here must be followed on all nodes that contain either OPC Servers or OPC Clients.

Note: *OPC communication that is confined to a single machine (using COM, but not DCOM) will continue to work properly after installing XP SP2 without following the instructions in this white paper.*

Windows Firewall

The Windows Firewall allows traffic across the network interface when initiated locally, but by default stops any incoming “unsolicited” traffic. However, this firewall is “exception” based, meaning that the administrator can specify applications and ports that are exceptions to the rule and can respond to unsolicited requests.

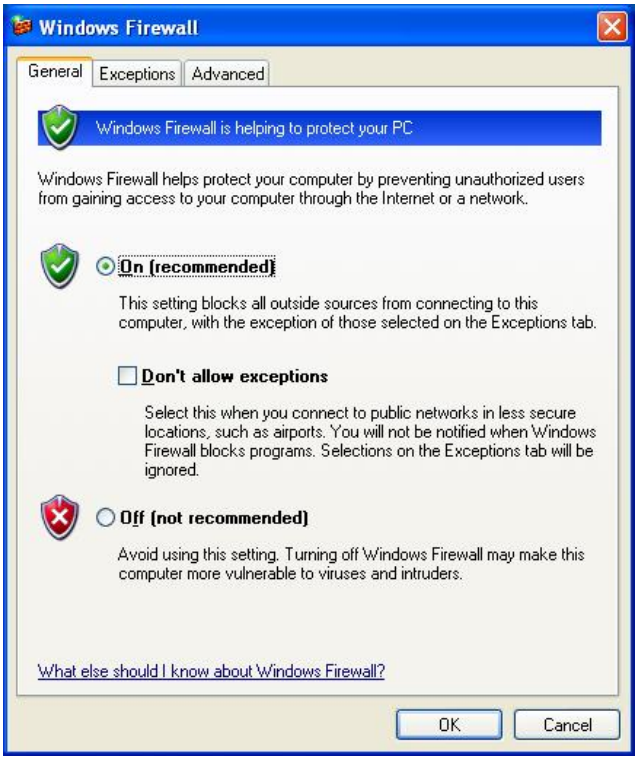
The firewall exceptions can be specified at two main levels, the application level and the port and protocol level. The application level is where you specify which applications are able to respond to unsolicited requests and the port and protocol level is where you can specify the firewall to allow or disallow traffic on a specific port for either TCP or UDP traffic. To make any OPC client/server application work via DCOM, changes need to be made on both levels.

***Note**: Developers of OPC Products may want to automatically make the necessary firewall settings programmatically. Microsoft supplies the Windows Firewall API to support this:*
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ics/ics/inetfwauthorizedapplication_name.asp

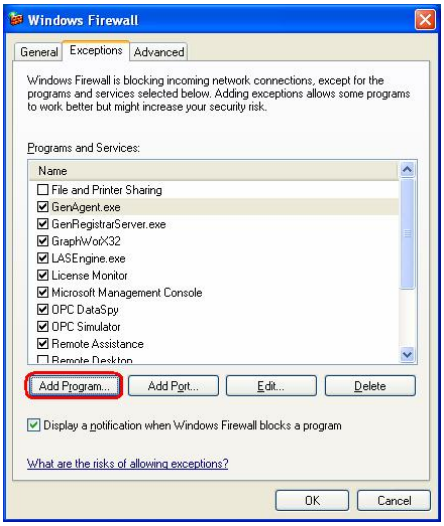
Configuring the Firewall

1. By default the windows firewall is set to “On”. This setting is recommended by Microsoft and by OPC to give your machine the highest possible protection. For trouble shooting, you may wish to temporarily turn off the firewall to prove or disprove that the firewall configuration is the source of any communication failure.

***Note:** It may be appropriate to permanently turn off the firewall if the machine is sufficiently protected behind a corporate firewall. When turned off, the individual firewall settings outlined here need not be performed to allow OPC communication.*

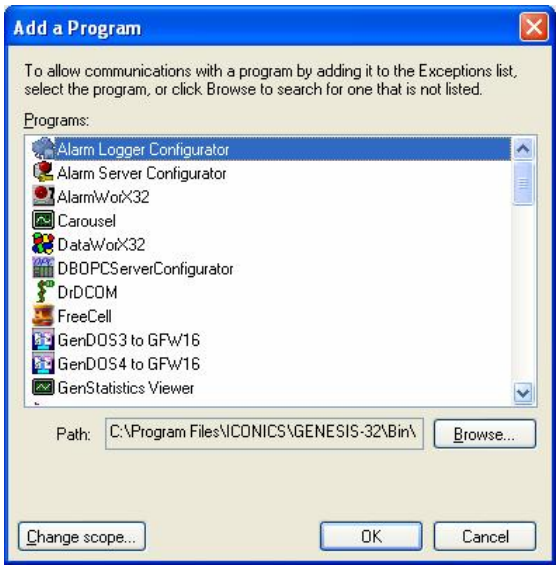


2. Select the “Exceptions” tab and add all OPC Clients and Servers to the exception list. Also add Microsoft Management Console (used by the DCOM configuration utility in the next section) and the OPC utility OPCEnum.exe found in the Windows\System32 directory.

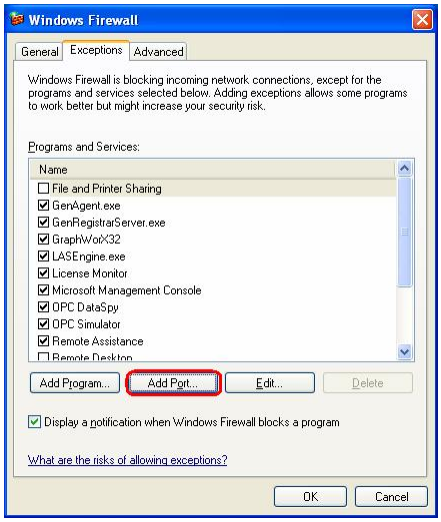


In the Add a Program dialog, there is a listing of most applications on the machine, but note that not all of them show up on this list. Use the “Browse” button to find other executables installed on the computer.

Note: *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.*



3. Add TCP port 135 as it is needed to initiate DCOM communications, and allow for incoming echo requests. In the Exceptions tab of the Windows Firewall, click on Add Port.

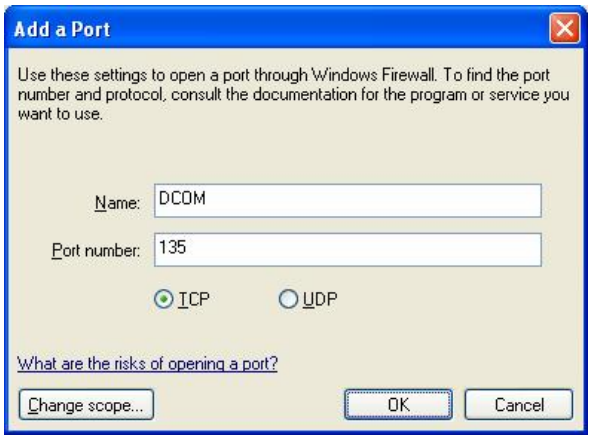


In the Add a Port dialog, fill out the fields as follows:

Name: DCOM

Port number: 135

Choose the TCP radio button



DCOM Enhancements

Service Pack 2 for Windows XP has also made some security enhancements to DCOM; two in particular need to be taken into consideration when using OPC on a network: First, the default Launch and Access permissions dialogs have been modified to allow the user to configure “limits” on the permissions given to applications using DCOM. Secondly, for each user now defined in the Launch and Access permissions, both local and remote access can be explicitly defined.

A brief background on default Launch and Access permissions in DCOM: Launch permissions define who can launch a COM based application (such as an OPC server) both over the network or locally. Access permissions define who can access that application once it has been launched. Applications can get their Launch and Access permissions from one of three places: they can use explicitly defined setting for their application, they can use the default permissions or they can set their own permissions programmatically. Because an application could set its own permissions programmatically, the explicitly defined or default settings, although set properly, may not be used and therefore the user is not able to explicitly have control over these settings. To overcome this security flaw, Microsoft has added “limits” to the DCOM security settings from Launch and Access to limit the permissions that an application can use. This limit prevents the application from using permissions beyond what is specified in the DCOM configuration settings. By default the limits set by Service Pack 2 will not allow for OPC communications over the network.

In addition to the new permissions limits, one must now specify if the user or group specified has permissions locally or remotely (or both). In order for OPC applications to work over the network with DCOM, the permissions must be set such that remote users can launch and/or access the OPC servers and clients on the machine.

Configuring DCOM

DCOM has settings for:

- the machine default
- each server

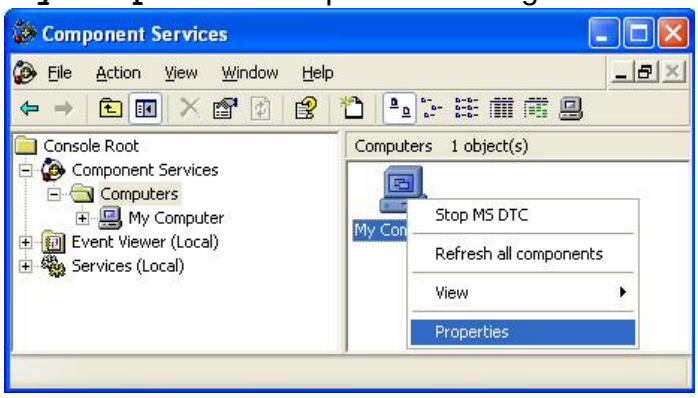
The machine default settings are used when there are no custom settings for the specific COM (OPC) server. If a server has custom settings then changes in the default settings have no effect for this server.

Configuring DCOM Machine Default

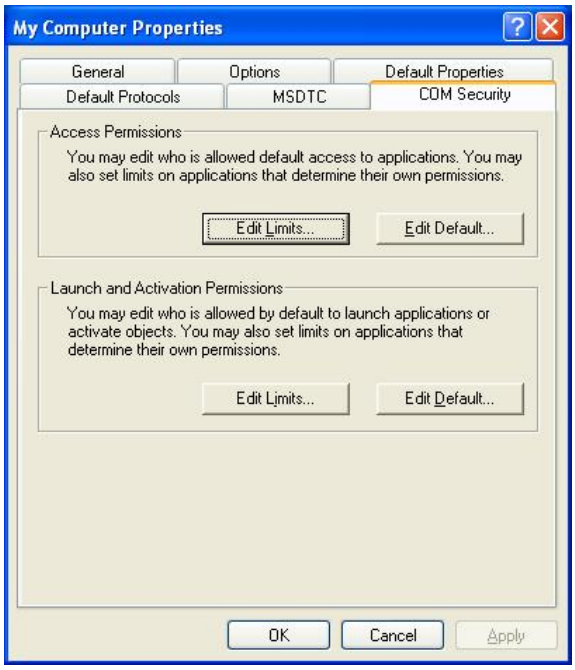
Follow these steps to configure the DCOM machine default settings for OPC Communications using Windows XP Service Pack 2:

1. Go to `Start -> Run` and type **DCOMCnfg** and click on **OK**.

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`

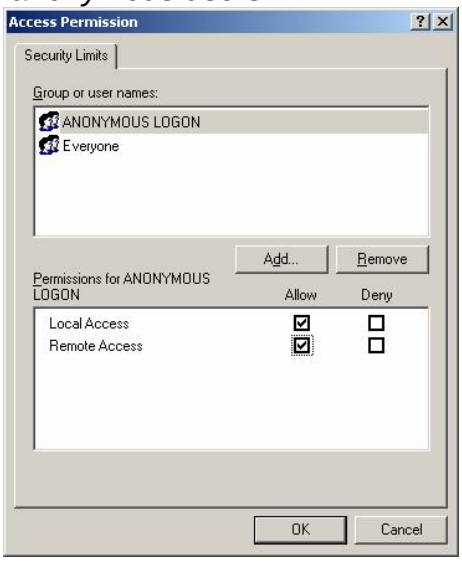


5. Go to the `COM Security` tab and note these are the four permission configurations that we will have to edit:



6. Edit the Limits for Access and Launch
   a. Access Permissions – **`Edit Limits...`**
      You need to check the Remote Access box for the user labeled `ANONYMOUS LOGIN` in this dialog.

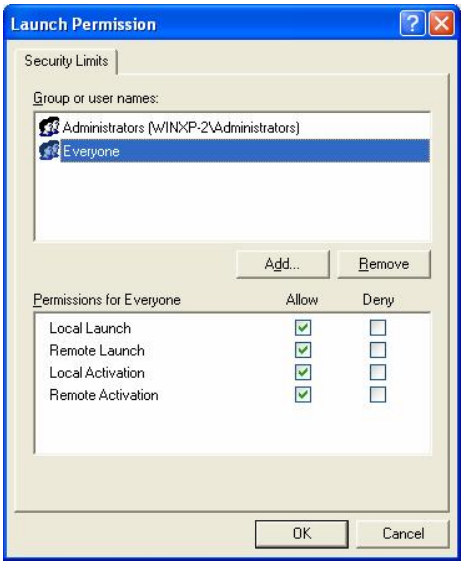
Note: *This setting is necessary for* ***OPCEnum.exe*** *to function and for some OPC Servers and Clients that set their DCOM 'Authentication Level' to 'None' in order to allow anonymous connections. If you do not use* ***OPCEnum*** *you may not need to enable remote access for anonymous users.*



b. Launch and Activation Permissions – **`Edit Limits...`**

You need to check the remote boxes for the user labeled `Everyone` in this dialog.

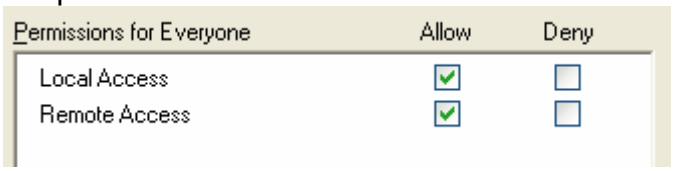
Note: *Since `Everyone` includes all authenticated users, it is often desirable to add these permissions to a smaller subset of users. One suggested way to accomplish this is to create a group named "OPC Users" and add all user accounts to this group that will execute any OPC Server or Client. Then substitute "OPC Users" everywhere that `Everyone` appears in these configuration dialogs.*



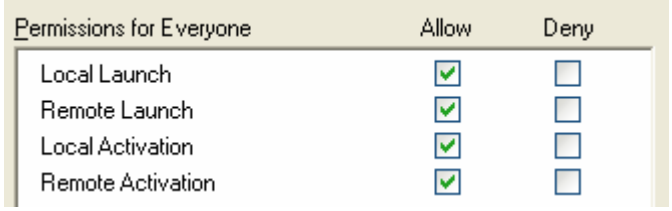
7. Edit Default Permissions for Access and Launch

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:



Launch and Activation permissions per user:

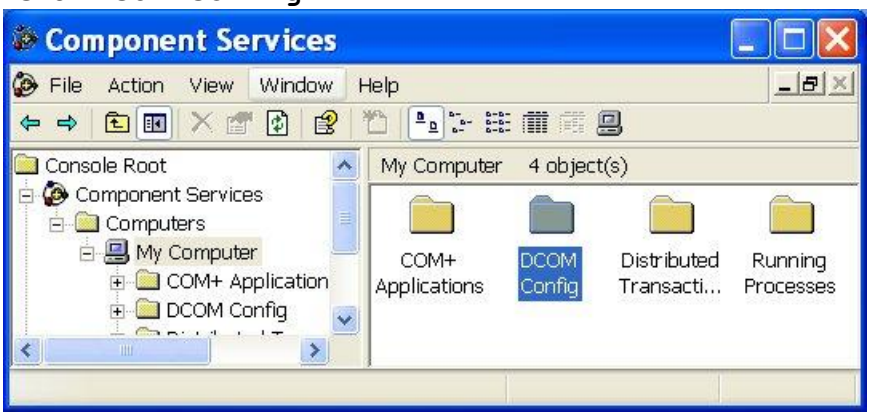


Configuring DCOM for an individual OPC Server

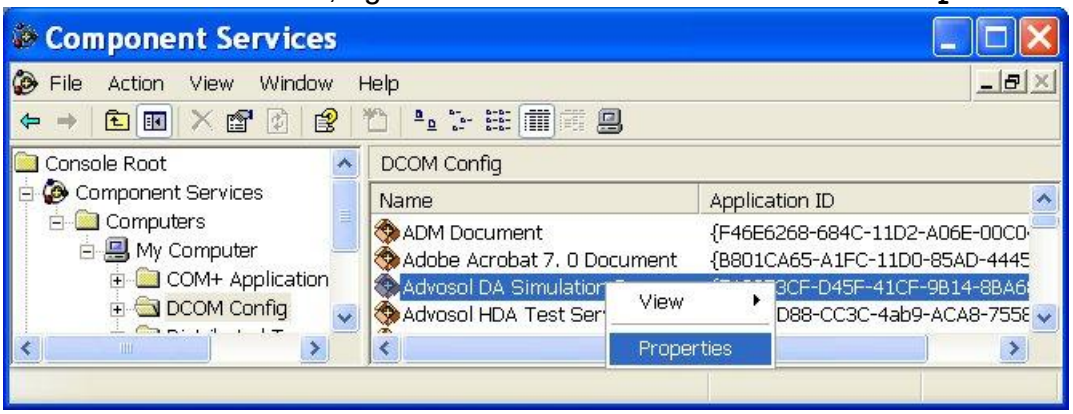
Follow these steps to configure DCOM for a specific COM server for OPC Communications using Windows XP Service Pack 2:

1. Go to `Start -> Run` and type **DCOMCnfg** and click on **OK**.

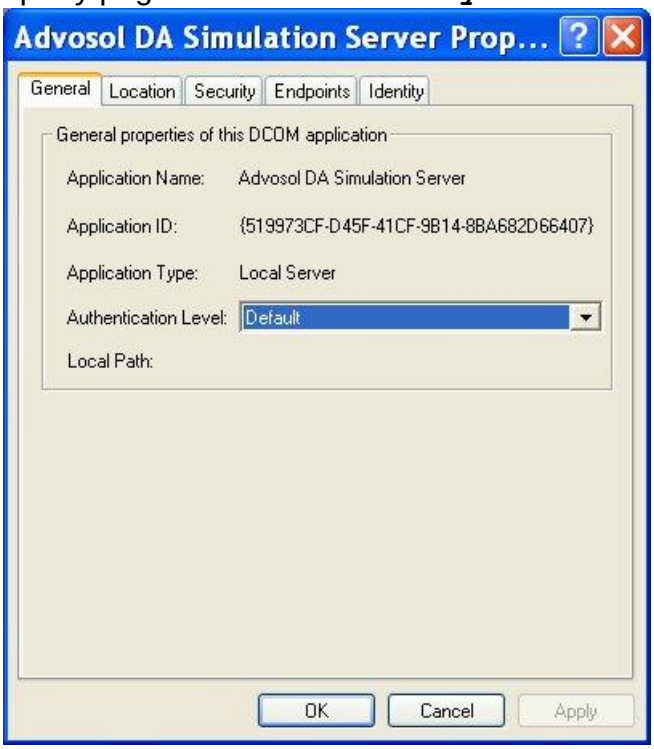
2. Click `on` **`Component Services`** under the Console Root to expand it.
3. Click on **`Computers`** under Component Services to expand it.
4. Right click on **`My Computer`** in the pane on the right and select `Properties`
5. Double Click **`DCOM Config`**



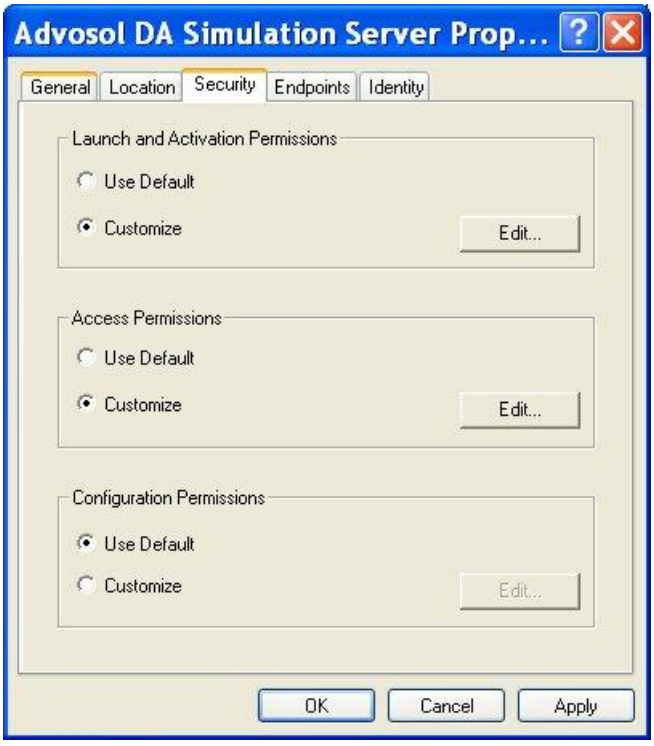
6. Select the OPC Server, right click the selection and then click **`Properties`**



7. In the server property page select the **`Security`** tab



8. Edit the server permissions settings. Select **`Customize`** and click the **`Edit`** button.

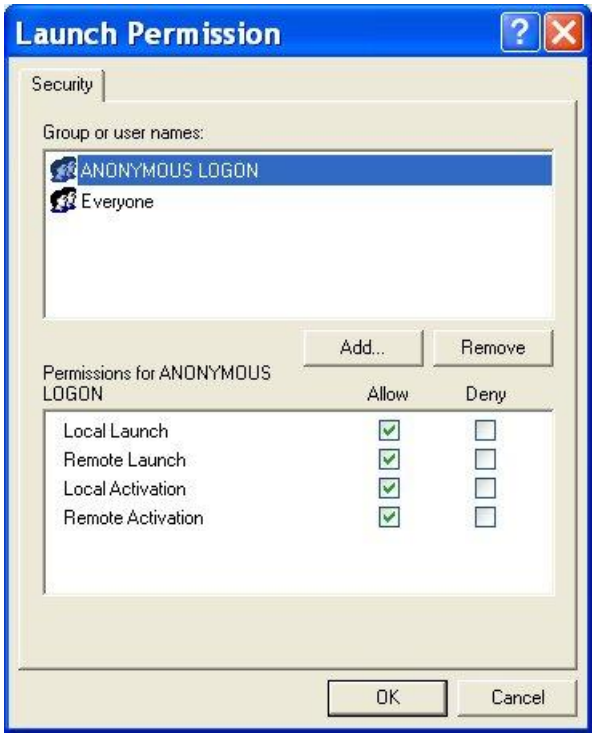


9. Edit the Launch/Activation Permissions

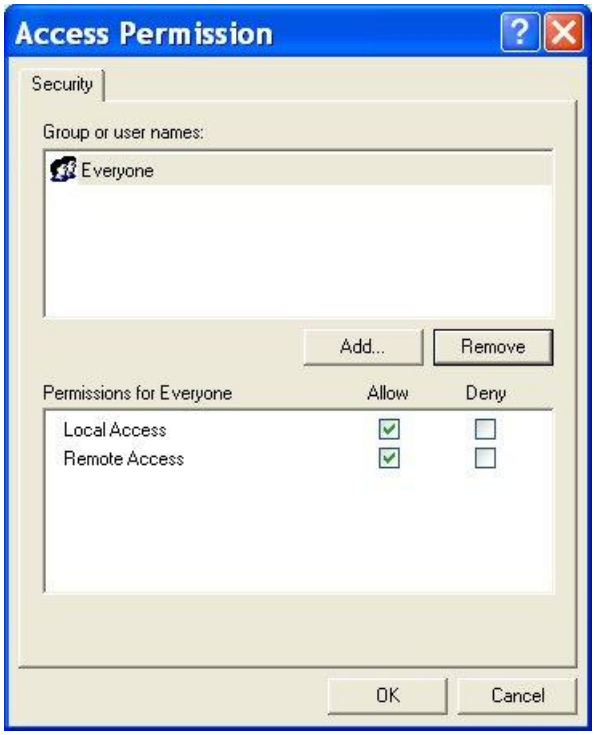
For each user (or group) that participates in OPC communication (e.g. “OPC Users”), make sure that both the **`Local Allow`** and **`Remote Allow`** checkboxes are both checked.

Note: This setting is necessary for OPCEnum.exe to function and for some OPC Servers and Clients that set their DCOM 'Authentication Level' to 'None' in order to allow anonymous connections. If you do not use OPCEnum you may not need to enable remote access for anonymous users.

Note: Since `Everyone` includes all authenticated users, it is often desirable to add these permissions to a smaller subset of users. One suggested way to accomplish this is to create a group named “OPC Users” and add all user accounts to this group that will execute any OPC Server or Client. Then substitute “OPC Users” everywhere that **`Everyone`** appears in these configuration dialogs.



10. Edit the Access Permissions
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.
Note: The Launch and Access users are not necessarily the same, even for a single client application. Windows uses the thread security token for the launch/activation but the process token for the access. The two security tokens may be different.



Disclaimer

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.

References

1. MS White paper: Windows XP Service Pack 2 Overview

Published: February 2004 For the latest information, please see http://msdn.microsoft.com/security

2. Windows XP Service Pack 2 - Security Information for Developers

http://msdn.microsoft.com/security/productinfo/XPSP2/default.aspx

3. Changes to Functionality in Microsoft Windows XP Service Pack 2

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx