InduSoft Web Studio + Windows XP SP2

Procedures for Handling the Windows XP OS + Service Pack 2 and InduSoft Web Studio

Introduction

This document describes the InduSoft Web Studio (IWS) functionalities that may be affected by the latest Microsoft Windows XP release, which is the Service Pack 2

Initial Considerations

One of the critical characteristics of using Windows operating systems has been the vulnerability of their security. In order to try to fix this problem, the Windows XP Service Pack 2 (XPSP2) blocks several of the vulnerable entry points. This type of fix forces the user to consciously open the entry points according to their needs, such as COM and DCOM configurations; the new Windows Firewall, which affects web services such as the Web Server; and TCP/IP & UDP/IP ports.

Before installing the Windows XPSP2, please keep in mind that you may need time, patience and a test procedure to assure that your programs will continue to work as they did before the installation. Avoid trying to install the XPSP2 during production time, while you are in a hurry, or when you are under any kind of pressure, since the installation requires caution and certain knowledge for the upgrade to be successful.

Affected Features

The following InduSoft Web Studio features will be affected after installing the Windows XPSP2. If you are not using these features, your application should work with no problems.

- TCP/IP Client and Server tasks
- Remote OPC Client and Server
- Remote LogWin, Database Spy and Import Wizard for IWS Application Database
- Remote Agent + Execution Environment
- Studio Database Gateway
- Web Solution

Configuring the Windows Firewall

The new Windows Firewall is responsible for managing which programs are authorized to run on your computer and which TCP and UDP/IP ports can be opened. It is also responsible for managing which common services will be enabled, such as receive Echo Request (*ping* command), Web Server, etc.

The first time you run any program that may use TCP/IP, you will receive a message stating that the program has been blocked. You will be asked to specify whether you want to unblock it or keep it blocked. You can expect this kind of message when you call IWS runtime, since it may try to open the TCP/IP port from the TCP/IP task.

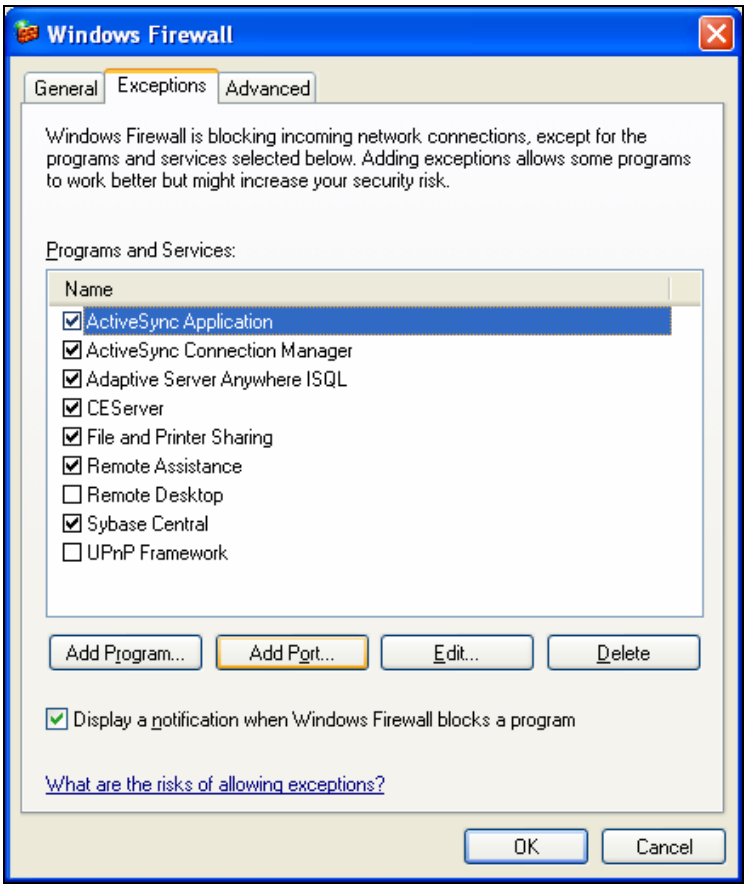
When you see this alert, make sure that you select **Unblock**, after verifying that it is mentioning **Studio Manager** from ILLC (InduSoft LLC)

This action will add a new item in the Exception list, allowing the Studio Manager to run properly

- **Accessing the Windows Firewall**

  You can access the Windows Firewall on the Control Panel by clicking this icon:

- **Configuring Exceptions**



As you call the IWS runtime and unblock it, this information will be saved in the Windows Firewall *Exceptions* list, as well as the TCP/IP ports that are used by this program. These include all the ports used by communication drivers over Ethernet.

There are some programs that you may need to enable manually. If you intend to use remote OPC communications, you may need to manually set the exception to **`OPCEnum.exe`** program, which is used to send the list of registered OPC servers from one computer to another remote one. You can do so by clicking on the **Add Program** button, and selecting **`OPCEnum.exe`**, usually under the **`\Windows\system32\`** folder.

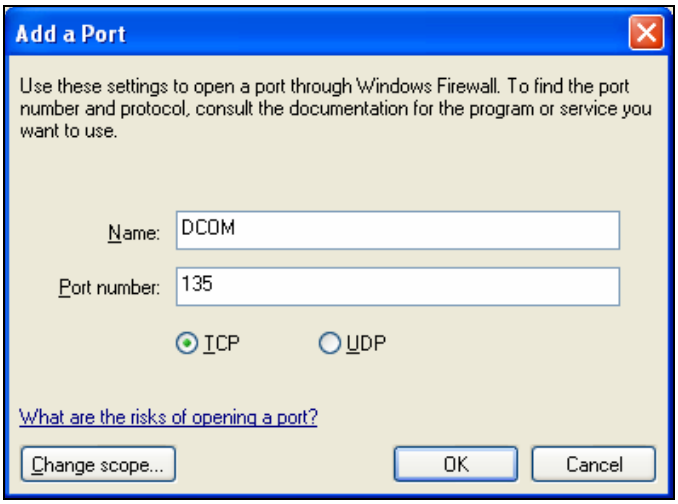
- **Enabling the TCP/IP Ports**

It is recommended that you manually open any port that your communication may need when you are using other gateway software, including the Studio ADO Gateway (if it is running on a remote computer), and the InduSoft Remote Agent program, used to download the applications to remote target systems.

You can manually add a port to the *Exception* list by clicking the **Add Port** button, and entering an identification for the exception and the TCP or UDP/IP port number.

If you intend to use remote OPC communications or one of the IWS remote debugging tools (Remote Database Spy, Remote LogWin or Import Wizard for IWS Application Database), you need to manually open the DCOM TCP/IP port.

To do so, click the **Add Port** button in the *Windows Firewall* dialog, enter **DCOM** in the **Name** field, click the **TCP** radio button, and enter **135** in the **Port Number** field.



- **Advanced Tab**

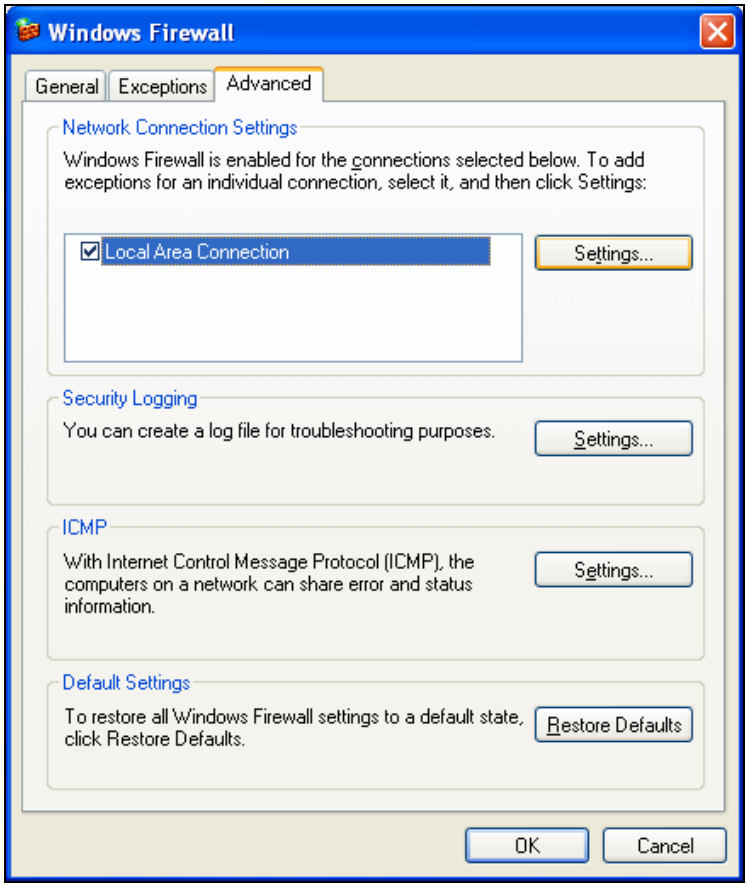
Enabling Web Server and ICMP Settings

After the Windows XPSP2 is installed, it will automatically block any task related to the Internet Control Message protocol as well as any Internet related service, such as FTP server, SMTP server, and so forth. The most important tasks or services affected by this action in applications related to InduSoft Web Studio are the Echo Request (ping) and the Web Server

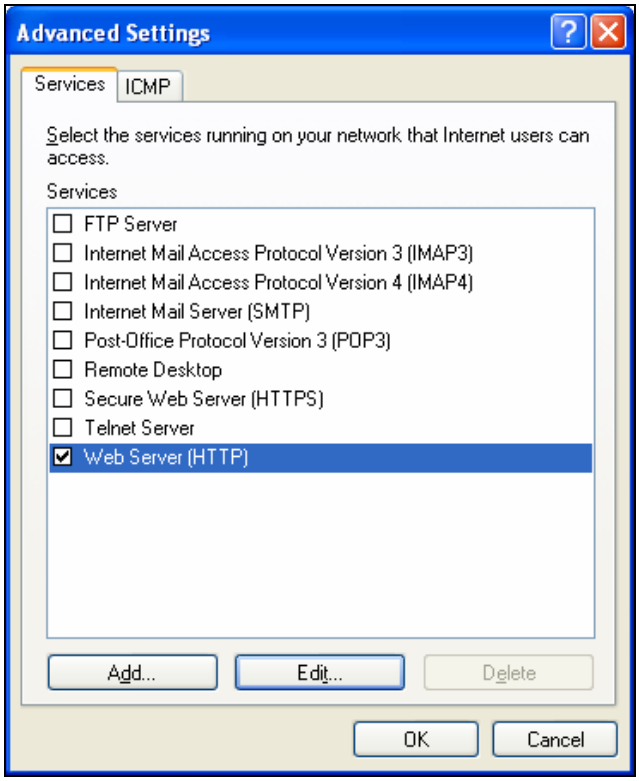
Enabling Web Server

If you are configuring your IWS to use the Windows Web Server provided by the Internet Information Services (IIS) task, you need to manually enable this service.

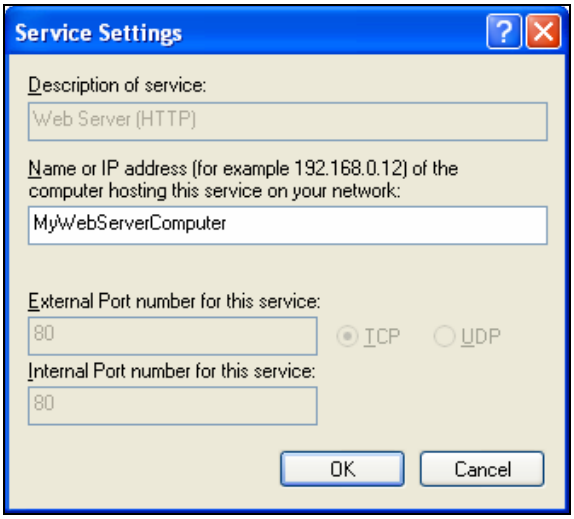
In order to do this, go to the *Advanced* tab, select the Network card that you will be enabling to be a Web Server in the **Network Connections Settings** group and click on **Settings.**



The *Advanced Settings* dialog window will open. Check the **Web Server (HTTP)** option.



You will be prompted to enter the **Name or IP Address** of the computer that is hosting the Web Server service. This is usually your computer's name.



> **Note:** If you are using any other TCP/IP port for the Web Server service, you will need to click the **Add** button in the *Advanced Settings* window. You will then designate a name for the service, such as **Web Server http 8080**, and enter the port number that you configured in the IIS.

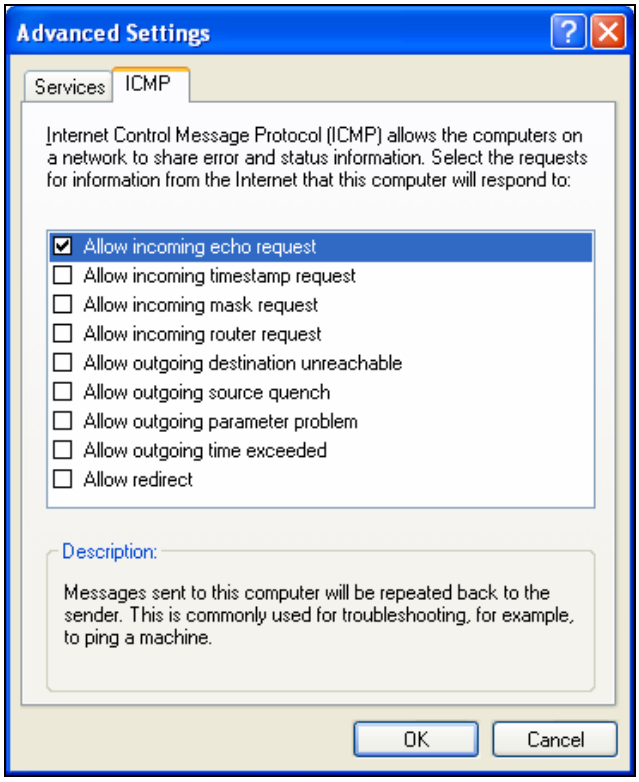
Enabling Echo Request (ping)

It is useful to be able to "ping" a remote computer for debugging purposes, network diagnostics and other tasks.

The command to ping can be issued from the DOS prompt window, where you pass the command and the IP address or computer name that you are trying to reach. For example: **`ping 192.168.0.100`**.

If the command finds the remote computer, it will receive an echo message. By default, this echo message is blocked after the Windows XPSP2 is installed. To enable it, you must navigate to the **Windows Firewall > Advanced** tab, select the network card that you will be enabling to be *pinged* in the **Network Connections Settings** group, and click the **Settings** button.

When the *Advanced Settings* dialog opens, click the *ICMP* tab. Check the **Allow incoming echo request** option.



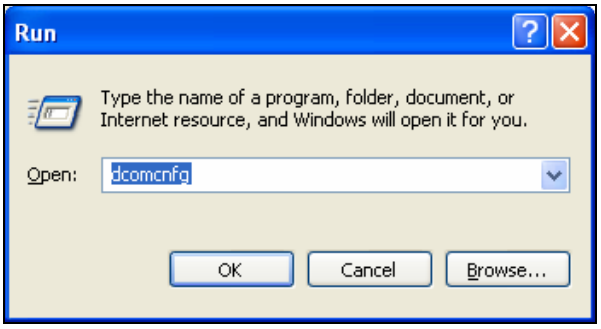
Configuring the DCOM Settings

You will need to configure the DCOM (Distributed Component Object Model), if you intend to use remote OPC communications or one of the following IWS remote tools:

- Remote Database Spy
- Remote LogWin
- Import Wizard for IWS Database

- **Calling the *DCOM Configuration* Program**

In order to start configuring the DCOM settings, you need call the executable program **`DCOMCNFG.exe`**. You can do so with the Windows *Run* command.



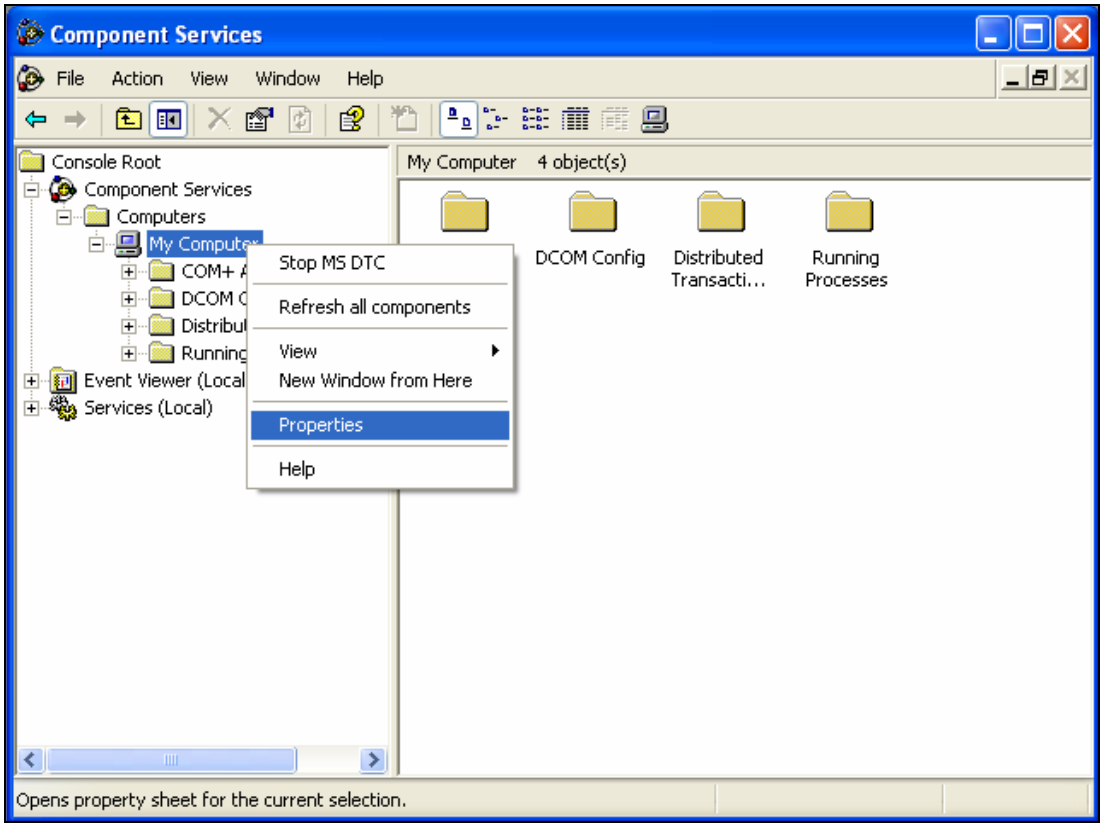
- **Editing the COM Security Limits**

One of the new features of the Windows XPSP2 is Limits, which refers to the limits to the COM applications. This feature joins the already existing Access and Launch Permissions.

> **Note:** You MUST properly configure the limits as shown below in order to have your DCOM application working properly; otherwise, it may not work at all.

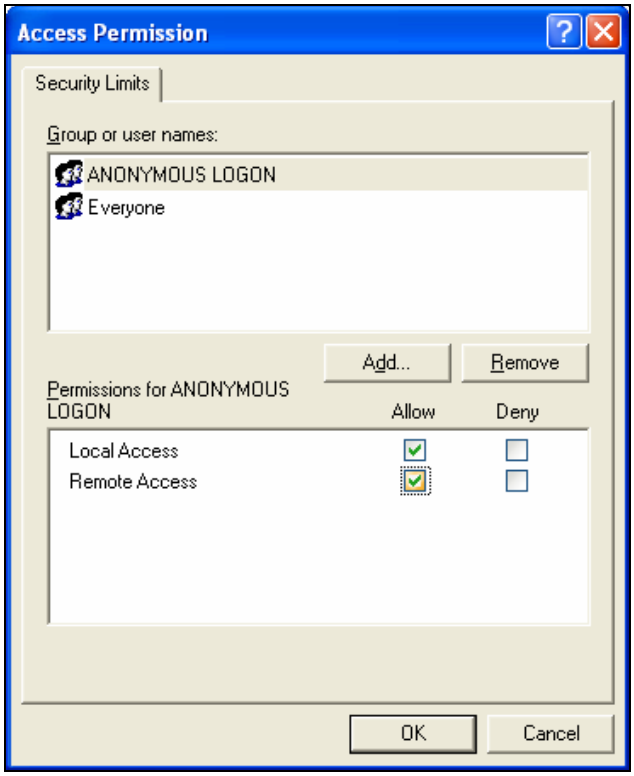
After calling the **`DCOMCNFG`** program, you will see the *Console Root* tree view. Please expand **Component Services > Computers > My Computer**. You must unblock this program when you are given the choice to do so.

Next, right-click on **My Computer**, and select **Properties**



Click the **COM Security** tab. Here you will find the new **Edit Limits** button. You must perform the following configurations:

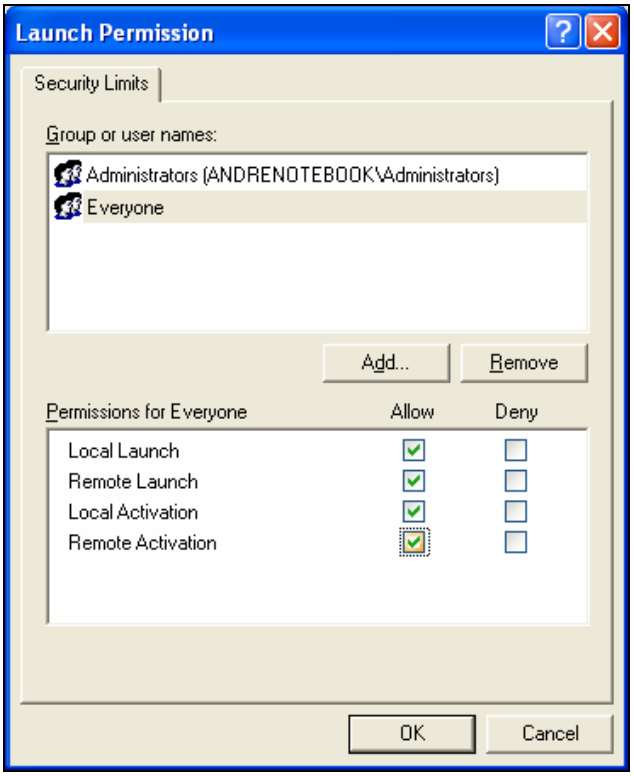
- In the **Access Permissions** group, click **Edit Limits**. The *Access Permission* dialog opens.



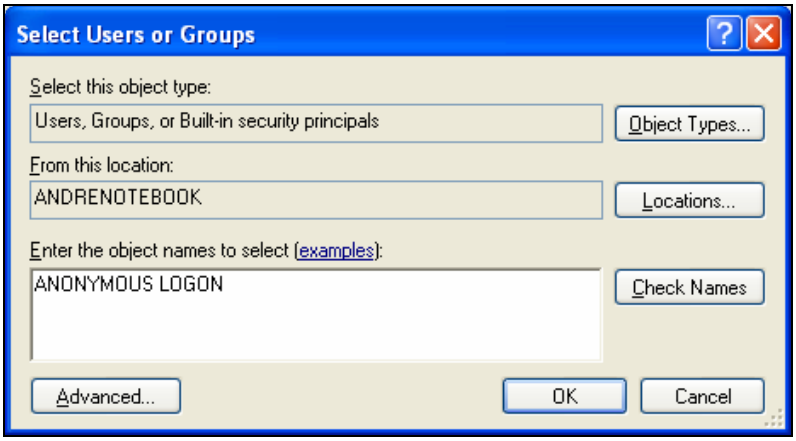
- On the *Security Limits* tab, select **ANONYMOUS LOGON**
- In the **Permissions for ANONYMOUS LOGON** group, check both **Local Access** and **Remote Access**.
- Repeat the procedure after selecting the **Everyone** group or user name.

> **Note:** If you do not see either **ANONYMOUS LOGON** or **Everyone** in the **Groups or user name** list, you can click the **Add** button to create them in the **Object Names** list

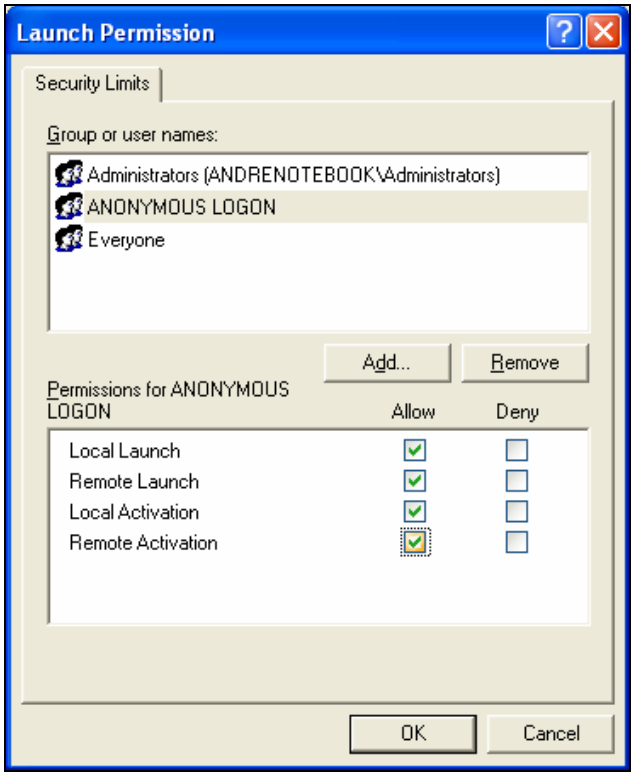
- Click **OK** to finish the *Access Permission* configuration.
- Return to the *COM Security* tab and click the **Edit Limits** button, in the **Launch and Activation Permissions** group.
- The *Launch Permission* dialog opens. Select **Everyone** in the **Group or user names** list. In the **Permissions for Everyone** list, you must check the **Allow** boxes for all the local and remote permissions.



- Click the **Add** button.
- Type **ANONYMOUS LOGON**, and click **Check Names**.
- If the text you typed becomes underlined, you completed the step correctly. Click **OK** in the *Select Users or Groups* dialog.



- Return to the *Launch Permission* window, and select **ANONYMOUS LOGON**. You must check the **Allow** boxes for all the local and remote launch and activation permissions



- Click **OK** to finish the Launch Permissions configuration.

- Return to the My Computer *Properties* window, click **Apply**, followed by **OK**, to finish configuring the COM security settings.

- **Configuring Permissions for each DCOM Server**

  So far, you have allowed your computer to accept ANONYMOUS LOGON and EVERYONE DCOM connections. But the Windows XPSP2 by default will also block all the DCOM servers, so you need to manually configure the permissions for each of them.

  The three DCOM Servers related to InduSoft Web Studio are:

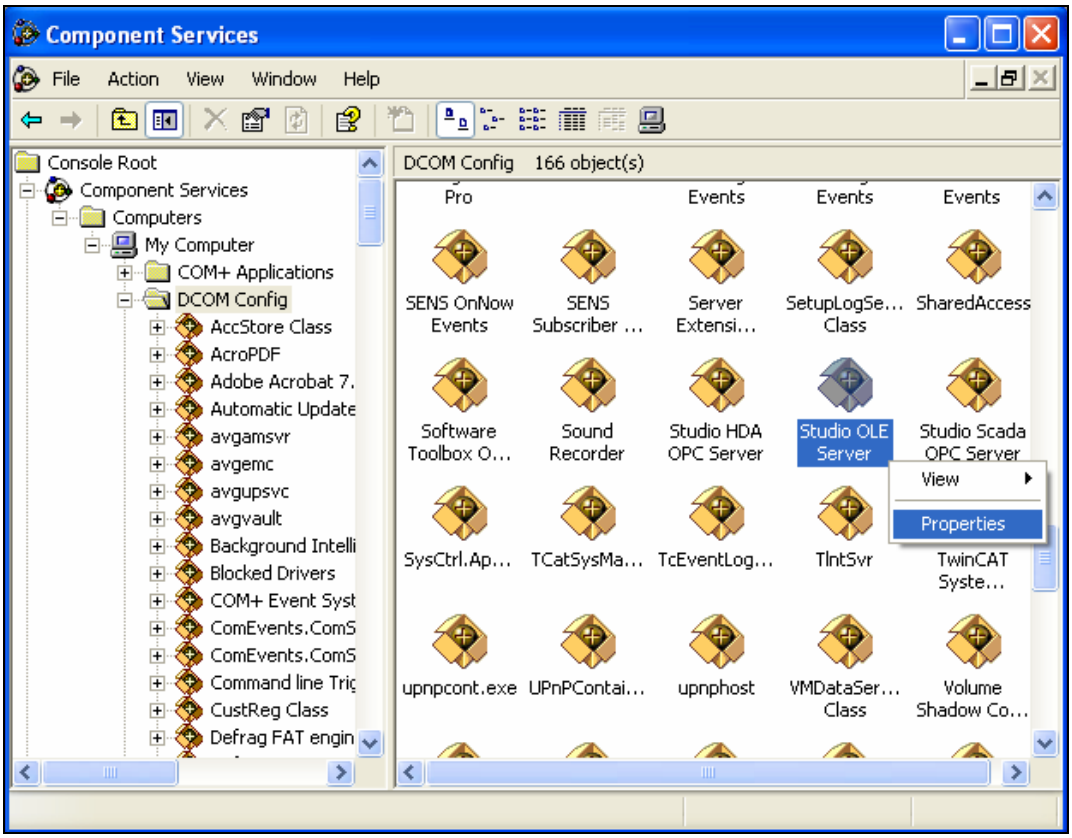
  - Studio HDA OPC Server – InduSoft Web Studio Historical Data Acquisition OPC Server
  - Studio Scada OPC Server – InduSoft Web Studio Data Acquisition OPC Server
  - Studio OLE Server – InduSoft Web Studio OLE Server used by the Remote Logwin, Remote Database Spy and Import Wizard for IWS Remote Database

  If your network uses a domain, it should be able to handle the permissions by itself. However, if your network uses a workgroup, you need to perform the following actions:

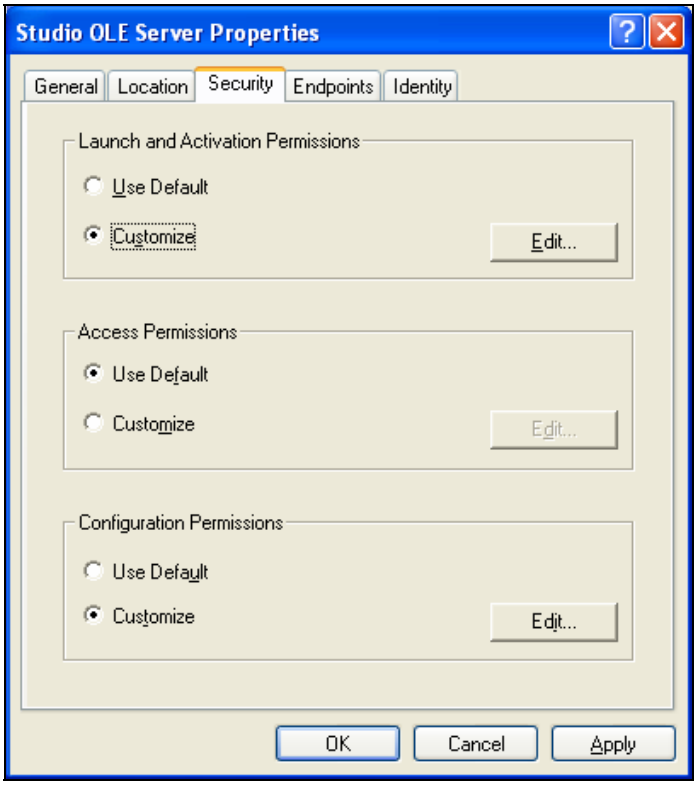
  - In the **DCOMCNFG** program, navigate to the **Console Root > Component Services > Computers > My Computer > DCOM Config** folder.

  - When you open this folder, it will display all the DCOM servers registered on your computer. In the following example, you will configure the permissions for the Studio OLE Server. Keep in mind that this procedure must be repeated for the Studio SCADA OPC Server and the Studio HDO OPC Server, as well as for any other third party OPC Server that you may be using.

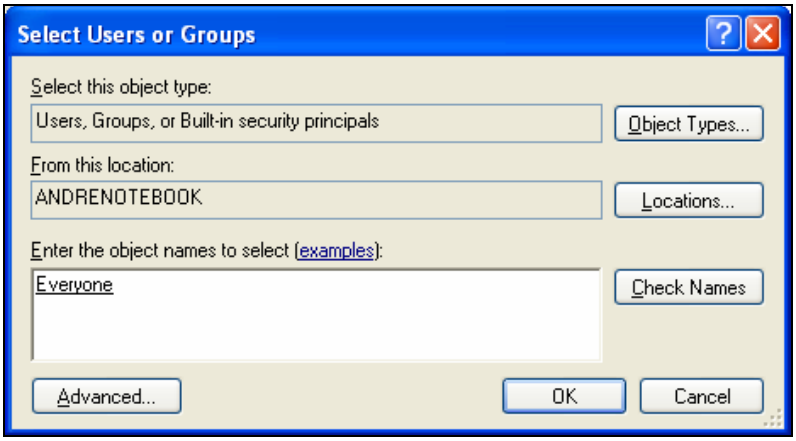
- Right-click on **Studio OLE Server**, and select **Properties**.

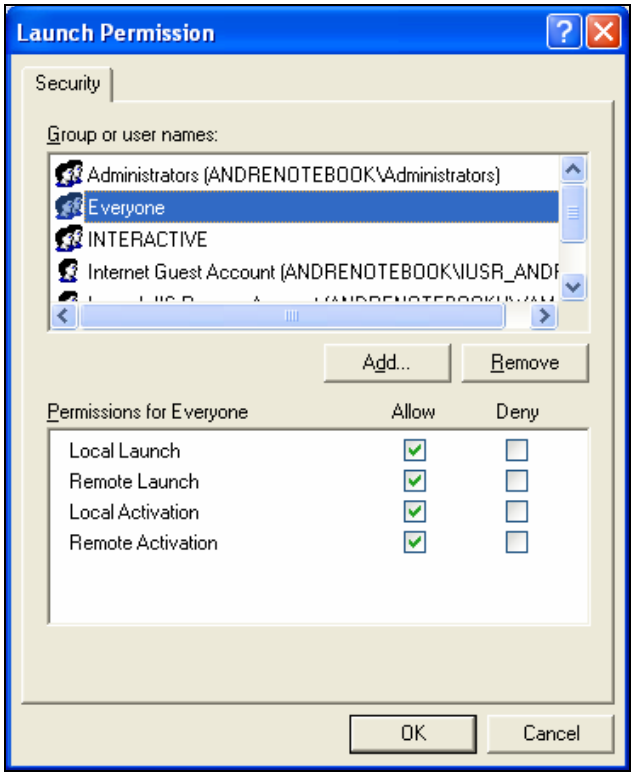


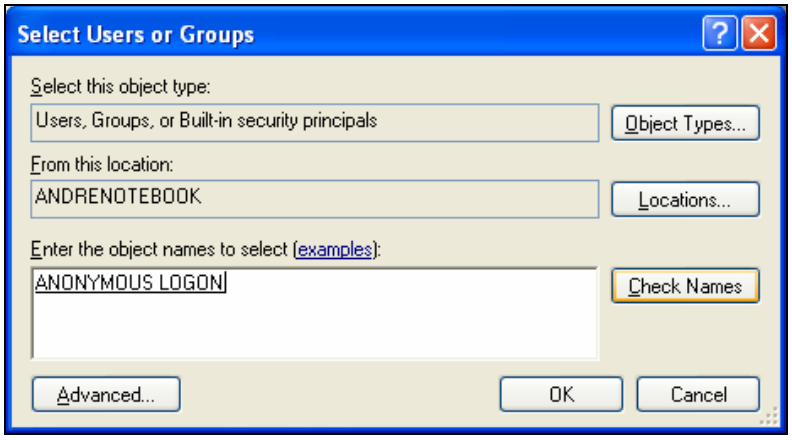
- Click the *Security* tab. Under **Launch and Activation Permissions**, click **Customize**. This action will enable the **Edit** button; please click on it.

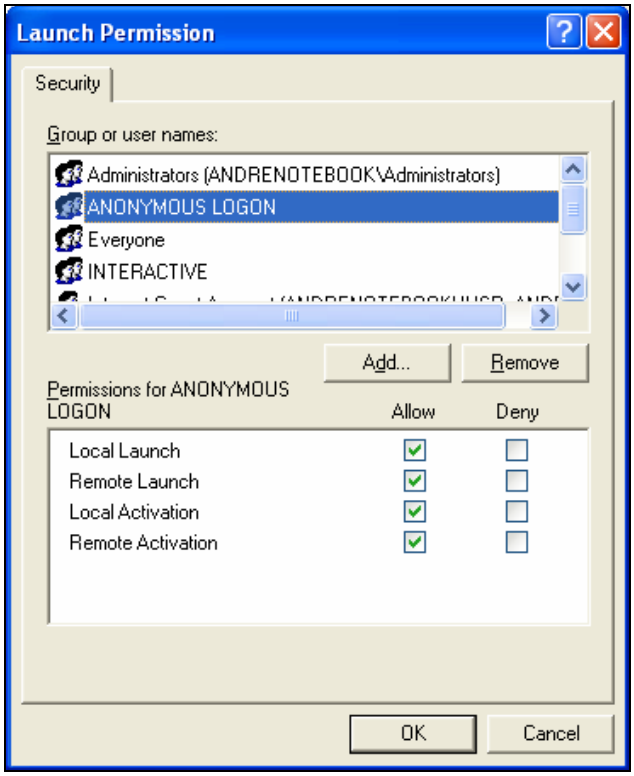


- The *Launch Permissions* dialog that opens is the same one that we used to configure the COM security settings. But in this case, you must manually create/add both **Everyone** and **ANONYMOUS LOGON**, making sure that you check the **Allow** boxes for all the local and remote launch and activation permissions. Refer to the directons in the previous section if you need help.









- After you add and properly configure **ANONYMOUS LOGON** and **Everyone**, click **OK** to finish the Launch Permissions configuration.

> **Note:** You should not need to configure/customize the Access Permissions**.** However, if you experience remote connection issues, you may consider also adding **ANONYMOUS LOGON** and **Everyone** to the Access Permissions settings.

InduSoft Web Plug-in ActiveX Object ISSymbol.OCX

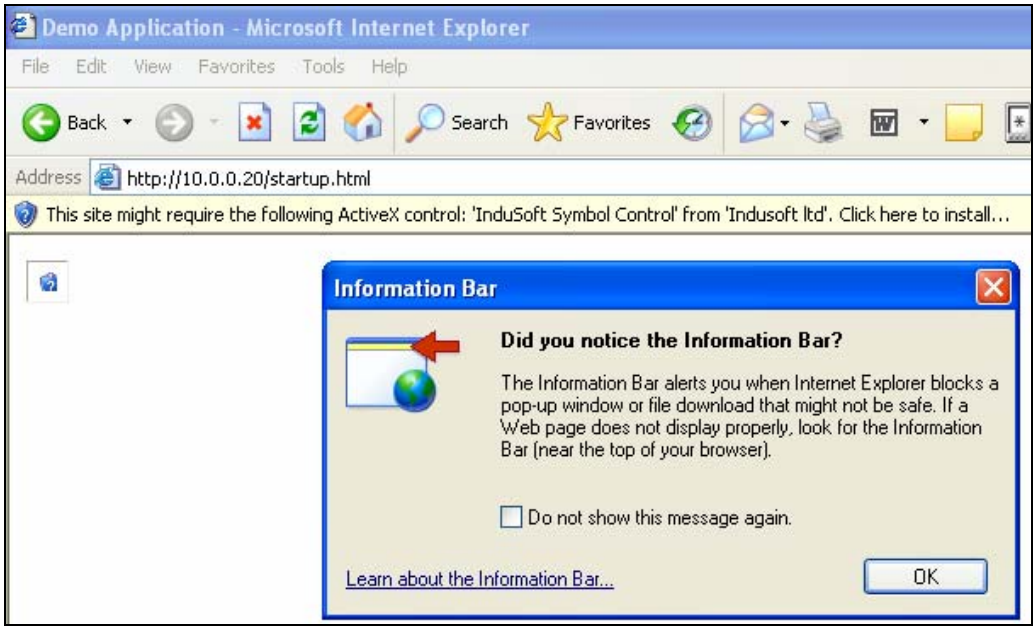
Among the innovations introduced by Windows XPSP2, there is a new way to manage plug-ins, add-ons, ActiveX and anything related to web applications.

Since one of the InduSoft Web Studio web solutions is the ActiveX object **`ISSymbol.ocx`**, you will see a new *Information Bar* warning that a file download is required if you try to open a web page generated by IWS on an XPSP2 computer that does not have IWS installed on it. You can confirm this message by clicking the **OK** button. You will see the following message on the *Information Bar* before the main IE Window that will display the web page:

`This site might require the following ActiveX control: 'InduSoft ISSymbol Control' signed by 'InduSoft ltd'. Click here to install…`

Click on the *Information Bar*, and select **Install this ActiveX**. The **`ISSymbol.cab`** file will start downloading, which will install all the required files to the InduSoft web solution.

> **Note:** The **`ISSymbol`** component is about 2MB large, so, depending on your internet connection, the download may take several minutes.



Once you see the *Security Warning* asking if you want to install InduSoft Symbol Control by publisher InduSoft ltd, please click on **Install** to finish this configuration.

Final Considerations

The new Windows XPSP2 brings a lot of security mainly to issues related to hackers and attacks over the Web. Following the procedures above, you will be consciously opening and configuring the items and features required to properly run your InduSoft Web Studio application.

You can find more information and tutorials about how Windows XPSP2 affects the DCOM applications, on the OPC Foundation web site www.opcfoundation.org (under the **Downloads** section, **White Papers** option). We recommend that you also check the **Service Pack 2** section of the Microsoft Web site at http://www.microsoft.com/windowsxp/sp2/default.mspx

The Software Toolbox web site also provides a very comprehensive tutorial with consideration of the effect of WinXPSP2 on OPC applications. You can find that tutorial at http://www.softwaretoolbox.com/xpsp2/

Map of Revision

Revision	Author	Date	Comments
A	Andre Bastos	September 13, 2005	Initial version