

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

😺 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
ActiveSync Application
ActiveSync Connection Manager
Adaptive Server Anywhere ISQL
CEServer
✓ File and Printer Sharing
Remote Assistance
Upp Sybase Central
Add Program Add Port Edit Delete
✓ Display a notification when Windows Firewall blocks a program
What are the risks of allowing exceptions?
OK Cancel

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.

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.		
<u>N</u> ame:	DCOM	
<u>P</u> ort number:	135	
	⊙ <u>I</u> CP O <u>U</u> DP	
What are the risks of opening a port?		
Change scope	OK Cancel	

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**.



🐱 Windows Firewall 🛛 🛛 🔀			
General Exceptions Advanced			
Network Connection Settings Windows Firewall is enabled for the <u>c</u> onnections selected below. To add exceptions for an individual connection, select it, and then click Settings:			
✓ Local Area Connection Se <u>t</u> tings			
Security Logging			
You can create a log file for troubleshooting purposes. <u>S</u> ettings			
With Internet Control Message Protocol (ICMP), the <u>Settings</u> computers on a network can share error and status information.			
C Default Settings			
To restore all Windows Firewall settings to a default state, <u>R</u> estore Defaults click Restore Defaults.			
OK Cancel			

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



Advanced Settings ? 🔀
Services ICMP
Select the services running on your network that Internet users can access.
Services
FTP Server
Internet Mail Access Protocol Version 3 (IMAP3)
Internet Mail Access Protocol Version 4 (IMAP4)
Post-Office Protocol Version 3 (POP3)
Remote Desktop
Secure Web Server (HTTPS)
Telnet Server
Web Server (HTTP)
Agd Edit Delete
OK Cancel

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.

Service Settings	?×
Description of service:	
Web Server (HTTP)	
<u>Name or IP address (for example 192.168.0.12) of the</u> computer hosting this service on your network:	
MyWebServerComputer	
External Port number for this service:	
80 <u>I</u> CP <u>U</u>	DP
Internal Port number for this service:	
80	
OK Ca	ncel

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.

Advanced Settings			
Services ICMP			
Internet Control Message Protocol (ICMP) allows the computers on a network to share error and status information. Select the requests for information from the Internet that this computer will respond to:			
Allow incoming echo request			
 Allow incoming timestamp request Allow incoming mask request Allow incoming router request Allow outgoing destination unreachable Allow outgoing source quench Allow outgoing parameter problem Allow outgoing time exceeded Allow redirect 			
Description: Messages sent to this computer will be repeated back to the sender. This is commonly used for troubleshooting, for example, to ping a machine.			
OK Cancel			



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.

Run	28
-	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	dcomenfg
	OK Cancel <u>B</u> rowse

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



Second Services	
🐼 File Action View Window Help	_ 8 ×
← → 🖻 📧 × 🖀 🖉 😫 🏷 🍡 1- 🏥 🏛 🛱 📟	
Console Root My Computer 4 object(s)	
Component Services	
COM+ A Stop MS DTC DCOM Config Distributed Running Transaction Processes	
DCOM C Refresh all components	
Event Viewer (Local New Window from Here	
Properties	
Help	
Opens property sheet for the current selection.	

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.

Access Permission		? 🛛
Security Limits		
Group or user names:		
🚮 ANONYMOUS LOGON		
👧 Everyone		
	A <u>d</u> d	<u>R</u> emove
Permissions for ANONYMOUS LOGON	Allow	Deny
Local Access		
Remote Access		

- 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.



Launch Permission		? 🔀		
Security Limits				
<u>G</u> roup or user names:				
🚮 Administrators (ANDRENOTE	Administrators (ANDRENOTEBOOK \Administrators)			
🕵 Everyone				
	A <u>d</u> d	<u>R</u> emove		
Permissions for Everyone	Allow	Deny		
Local Launch	~			
Remote Launch				
Local Activation				
Remote Activation				
,				
	ОК	Cancel		

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

Select Users or Groups	? 🛛
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
Erom this location:	
ANDRENOTEBOOK	Locations
Enter the object names to select (<u>examples</u>):	
ANONYMOUS LOGON	Check Names
Advanced	OK Cancel

- 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



Launch Permission		? 🗙	
Security Limits			
<u>G</u> roup or user names:			
Administrators (ANDRENOTE)	300KVAdministra	tors)	
ANUNYMUUS LUGUN			
TTR L Velyone			
	A <u>d</u> d	<u>R</u> emove	
Permissions for ANONYMOUS	Allow	Deny	
Local Launch	~		
Remote Launch			
Local Activation			
Themole Activation			
	OK	Cancel	

- 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.

_



Studio OLE Server Properties ?X			
General Location Security Endpoints Identity			
C Use Default			
© Customize			
Access Permissions			
C Customize			
Configuration Permissions			
C Use Defa <u>u</u> lt			
Customize Edit			
OK Cancel Apply			

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.

Select Users or Groups		? 🛛
Select this object type:		
Users, Groups, or Built-in security principals		Object Types
<u>F</u> rom this location:		
ANDRENOTEBOOK		Locations
Enter the object names to select (<u>examples</u>):		
<u>Everyone</u>		Check Names
Advanced	ОК	Cancel



Launch Permission		? 🗙	
Security			
Group or user names:			
Administrators (ANDRENOTEBOOK \Administrators)			
🕵 Everyone			
	DENOTEDOOKI		
Internet Guest Account (AND			
<			
	A <u>d</u> d	<u>R</u> emove	
Permissions for Everyone	Allow	Deny	
Local Launch	~		
Remote Launch	~		
Local Activation			
Fielifole Activation			
,			
	OK	Cancel	

Select Users or Groups	?	
Select this object type:		
Users, Groups, or Built-in security principals	Object Type	s
Erom this location:		
ANDRENOTEBOOK	Locations	
Enter the object names to select (<u>examples</u>):		
ANONYMOUS LOGON	Check Nam	es
		_
Advanced	OK Cance	<u>.</u> ا



Launch Permission		? 🗙	
Security			
<u>G</u> roup or user names:			
Administrators (ANDRENOTEBOOK \Administrators)			
ANONYMOUS LOGON Everyone W INTERACTIVE			
	DENOTEDOOKI		
	A <u>d</u> d	<u>R</u> emove	
Permissions for ANUNYMOUS	Allow	Deny	
Local Launch			
Local Activation			
Remote Activation	▼		
	OK	Cancel	

- 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.



🐔 Demo Application - M	crosoft Internet Explorer
File Edit View Favorite	Tools Help
G Back 🝷 🕥 🕤 🔀	😰 🚮 🔎 Search 🧙 Favorites 🧐 🔗 - 🌺 🖬 - 📃 💽
Address 🙆 http://10.0.0.20/	;tartup.html
This site might require the f	llowing ActiveX control: 'InduSoft Symbol Control' from 'Indusoft ltd'. Click here to install
	Information Bar Did you notice the Information Bar? The Information Bar alerts you when Internet Explorer blocks a pop-up window or file download that might not be safe. If a Web page does not display properly, look for the Information Bar (near the top of your browser). Do not show this message again. Learn about the Information Bar

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

Internet	Explorer - Security Warning		
Do you want to install this software?			
	Name: <u>InduSoft Symbol Control</u> Publisher: <u>Indusoft Itd</u>		
💙 Mo	re options	Install	Don't Install
1	While files from the Internet can be useful, this file type can potentially harm your computer. Only install software from publishers you trust. <u>What's the risk?</u>		

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 <u>www.opcfoundation.org</u> (under the **Downloads** section, **White Papers** option). We recommend that you also check the **Service Pack 2** section of the Microsoft Web site at <u>http://www.microsoft.com/windowsxp/sp2/default.mspx</u>

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
А	Andre Bastos	September 13, 2005	Initial version