

**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.

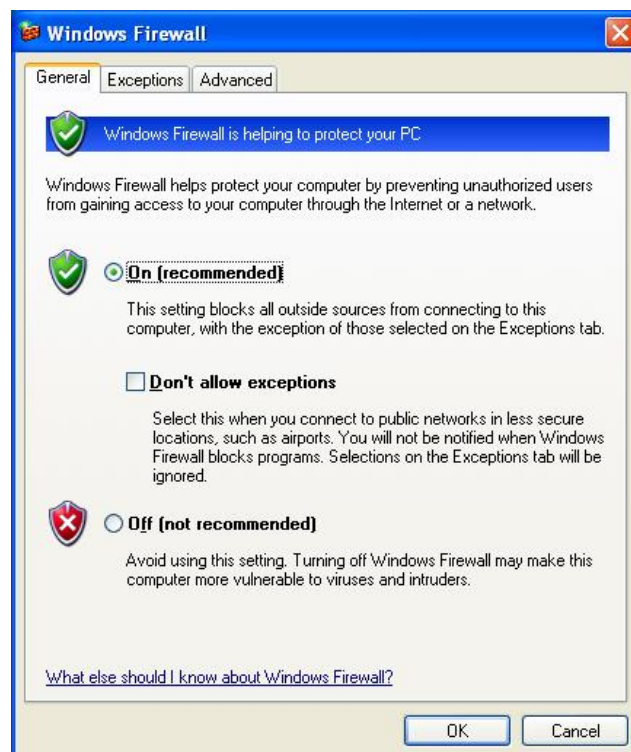
Note: Developers of OPC Products may want to automatically make the necessary firewall settings programmatically. Microsoft supplies the Windows Firewall API to support this:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ics/ics/inetfwauthorizedapplication_name.asp

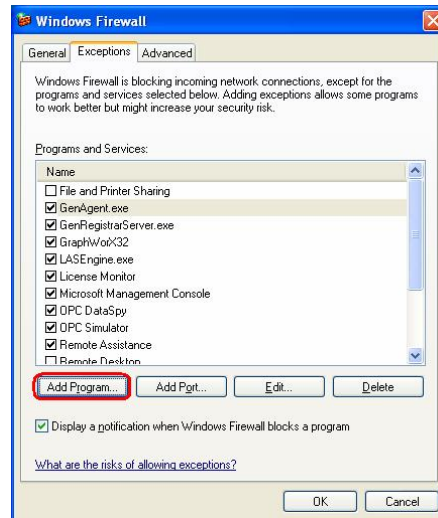
Configuring the Firewall

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.

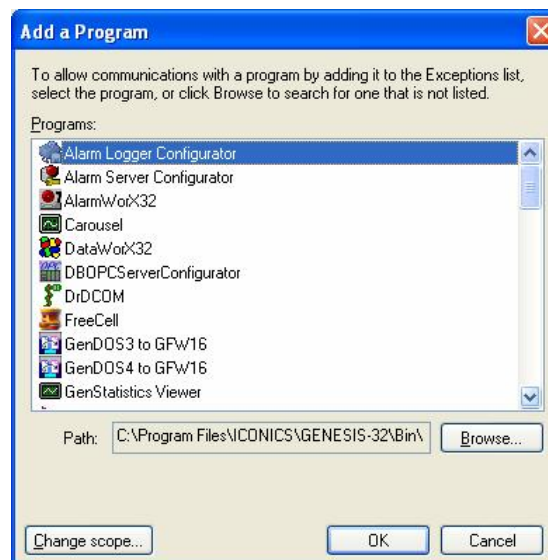


2. Select the “Exceptions” tab and add all OPC Clients and Servers to the exception list. Also add Microsoft Management Console (used by the DCOM configuration utility in the next section) and the OPC utility OPCEnum.exe found in the Windows\System32 directory.

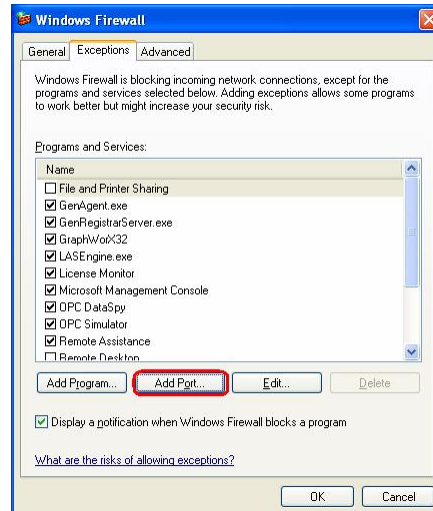


In the Add a Program dialog, there is a listing of most applications on the machine, but note that not all of them show up on this list. Use the “Browse” button to find other executables installed on the computer.

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.

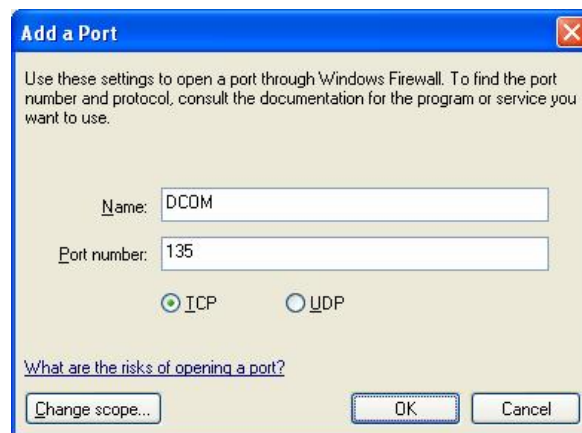


In the Add a Port dialog, fill out the fields as follows:

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.

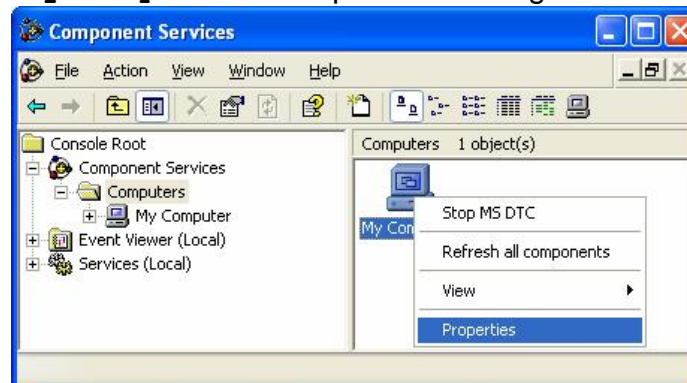
Configuring DCOM Machine Default

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

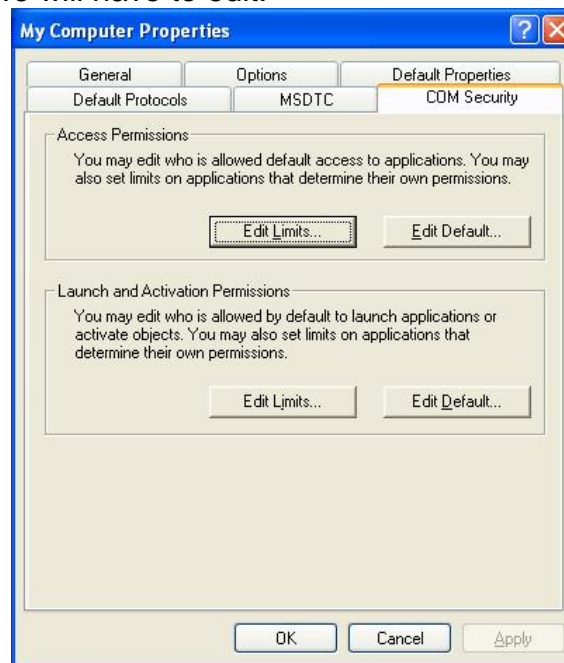
1. Go to **Start** -> **Run** and type **DCOMCnfg** and click on **OK**.



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:

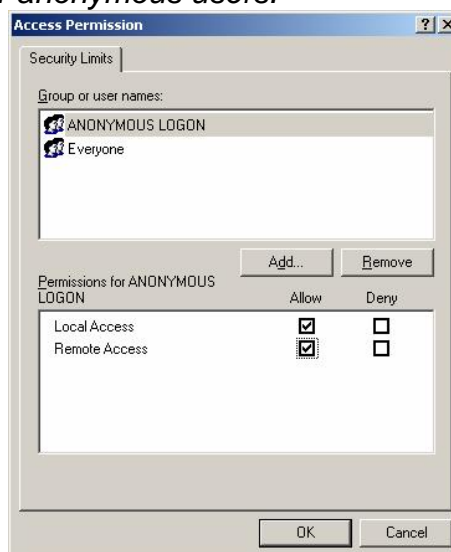


6. Edit the Limits for Access and Launch

a. Access Permissions – **Edit Limits...**

You need to check the Remote Access box for the user labeled
ANONYMOUS LOGIN in this dialog.

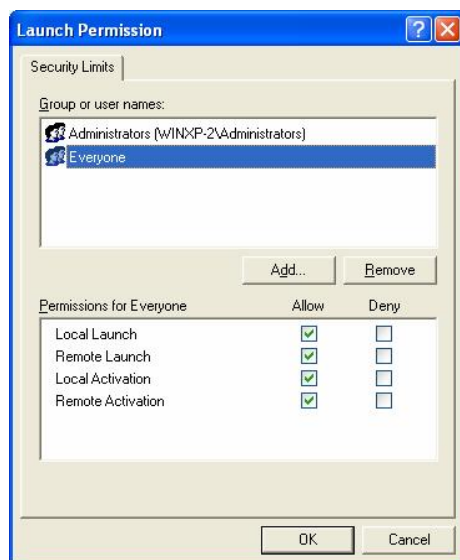
Note: This setting is necessary for **OPCEnum.exe** to function and for some OPC Servers and Clients that set their DCOM 'Authentication Level' to 'None' in order to allow anonymous connections. If you do not use **OPCEnum** you may not need to enable remote access for anonymous users.



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:

Permissions for Everyone	Allow	Deny
Local Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Launch and Activation permissions per user:

Permissions for Everyone	Allow	Deny
Local Launch	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Launch	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Local Activation	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Remote Activation	<input checked="" type="checkbox"/>	<input type="checkbox"/>

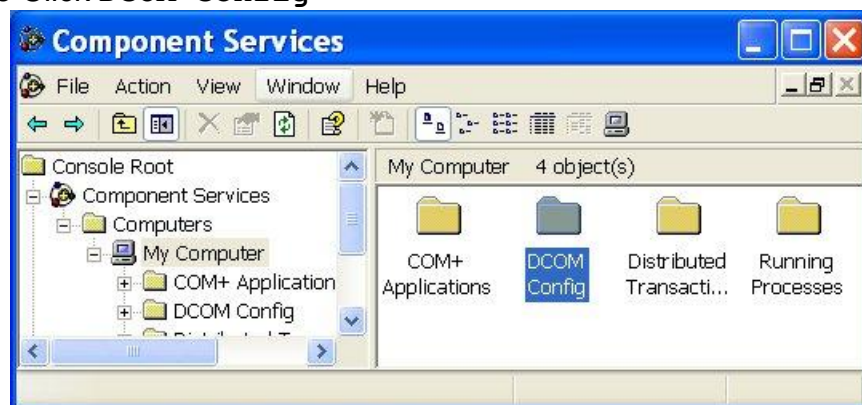
Configuring DCOM for an individual OPC Server

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

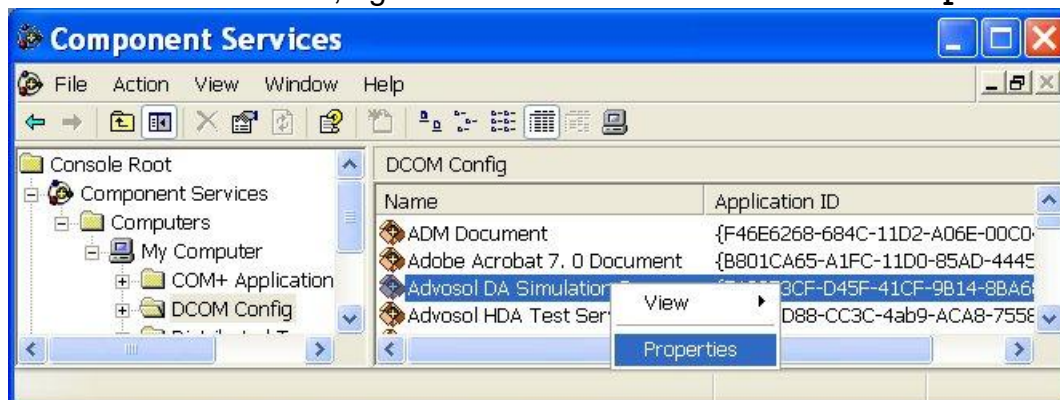
1. Go to Start -> Run and type **DCOMCnfg** and click on **OK**.



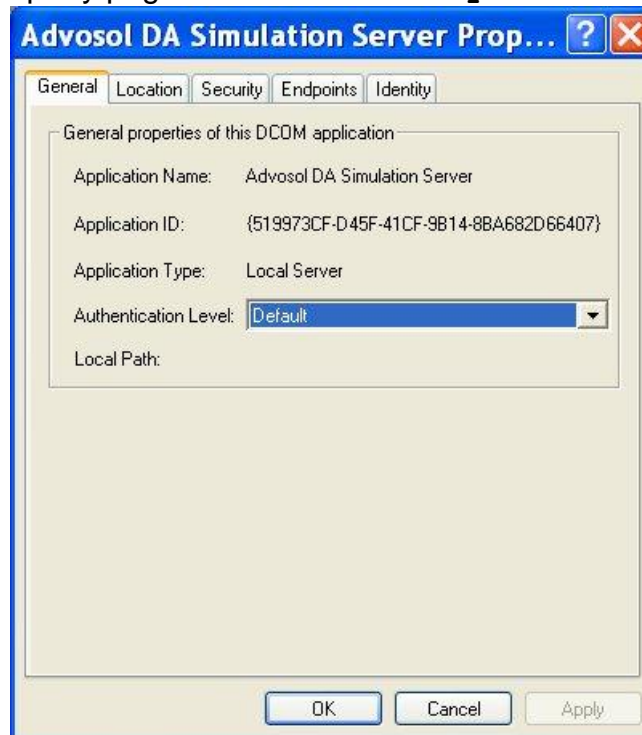
2. Click on **Component Services** under the Console Root to expand it.
3. Click on **Computers** under Component Services to expand it.
4. Right click on **My Computer** in the pane on the right and select **Properties**
5. Double Click **DCOM Config**



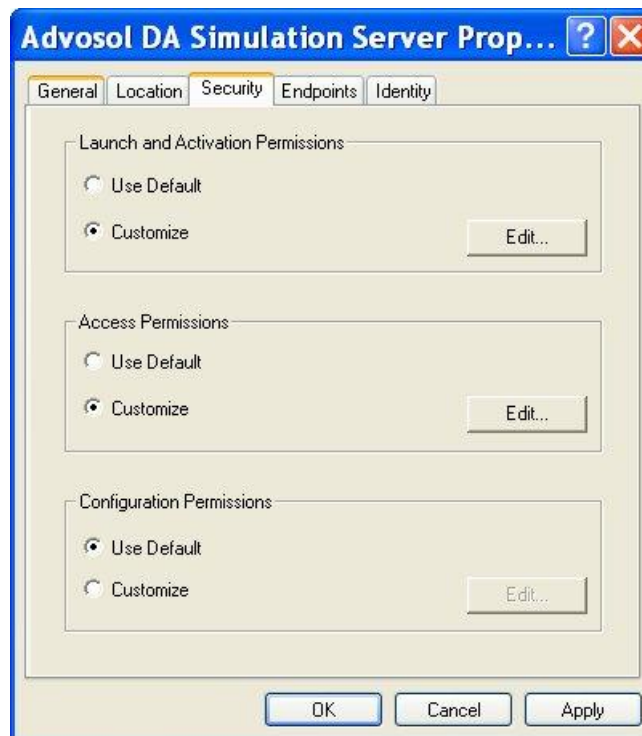
6. Select the OPC Server, right click the selection and then click **Properties**



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



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

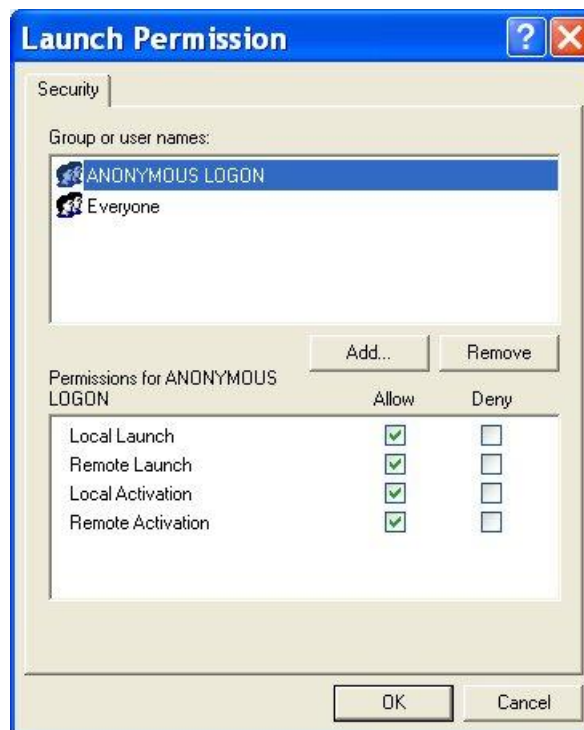


9. Edit the Launch/Activation Permissions

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.

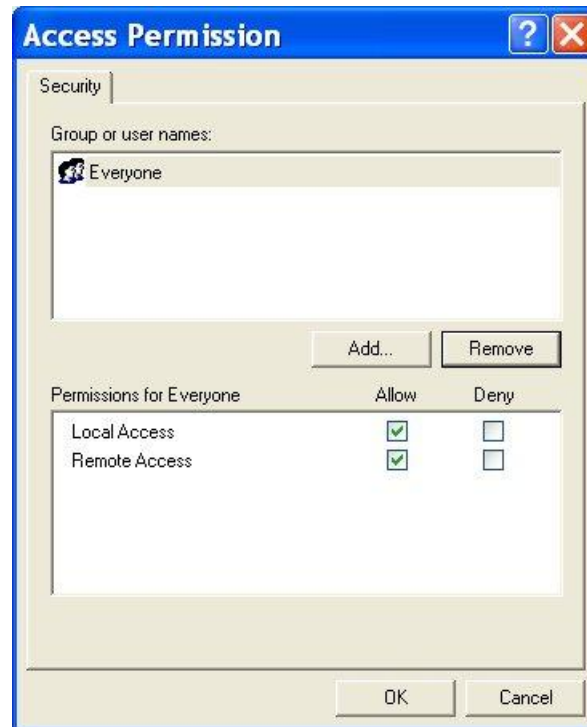
Note: Since *Everyone* includes all authenticated users, it is often desirable to add these permissions to a smaller subset of users. One suggested way to accomplish this is to create a group named “OPC Users” and add all user accounts to this group that will execute any OPC Server or Client. Then substitute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



TechNet Home

TechCenters

Downloads

TechNet Program

My TechNet

Security Bulletins

Archive

Exchange Server

Office

Operations Manager

Small Business Server

SQL Server

Systems Management Server

Windows Server 2003

Windows XP Professional

Windows Vista

More...

Desktop Deployment

Interop & Migration

IT Solutions

Script Center

Security

Community

Events & Webcasts

IT Training & Certification

Troubleshooting & Support

TechNet Worldwide

[TechNet Home](#) > [Products & Technologies](#) > [Desktop Operating Systems](#) > [Windows XP Professional](#) > [Service Pack 2: IT Resources](#)

Changes to Functionality in Microsoft Windows XP Service Pack 2

Introduction

Published: August 9, 2004 | Updated: September 15, 2004

By Starr Andersen, Technical Writer; Vincent Abella, Technical Editor

This Guide is available in multiple languages:



This document is Part 1 of “Changes to Functionality in Windows XP Service Pack 2” and provides an introduction to Microsoft® Windows® XP Service Pack 2 (SP2). You can obtain the other parts of the paper in the Microsoft Download Center, at <http://go.microsoft.com/fwlink/?LinkId=28022>.

This document applies to Microsoft Windows XP Service Pack 2 (SP2) for the 32-bit versions of Windows XP Professional and Windows XP Home Edition. It does not describe all of the changes that are included in the service pack, but instead highlights those changes that will have the most impact on your use of Windows XP SP2 and provide references to additional information.

On This Page

- ↓ [What's New in This Version](#)
- ↓ [Abstract](#)
- ↓ [Other Resources and Feedback](#)
- ↓ [Component Sections](#)
- ↓ [Scope of This Document](#)
- ↓ [Overview of Windows XP Service Pack 2 Security Technologies](#)

What's New in This Version

- Added new sections: Distributed Transaction Coordinator, Internet Information Services.

In This Article

- Introduction
- [Part 2: Network Protection Technologies](#)
- [Part 3: Memory Protection Technologies](#)
- [Part 4: E-mail Handling Technologies](#)
- [Part 5: Enhanced Browsing Security](#)
- [Part 6: Computer Maintenance](#)
- [Part 7: Other Technologies](#)
- [Part 8: Conclusion and Appendices](#)

- Revised sections: Windows Firewall, Setup, Resultant Set of Policy, Windows Update, Internet Explorer Feature Control Settings in Group Policy, Internet Explorer URLAction Security Settings in Group Policy, Internet Explorer MIME Handling Enforcement, Internet Explorer Network Protocol Lockdown, Internet Explorer Local Machine Lockdown.
- For information regarding changes in previous versions, see Appendix A, "Document History."

[⬆Top of page](#)

Abstract

In Windows XP Service Pack 2, Microsoft is introducing a set of security technologies that will help to improve the ability of computers running Windows XP to withstand malicious attacks, especially those from viruses and worms. The technologies include these improvements:

- Network protection
- Memory protection
- E-mail handling
- Web browsing security
- Computer maintenance

Together, these security technologies will help to make it more difficult to attack Windows XP, even if the latest updates are not applied.

In addition, this service pack also includes updates designed to improve the performance and stability of several Windows features.

[⬆Top of page](#)

Other Resources and Feedback

If you have any other questions that are not answered by this paper, "Windows XP Service Pack 2 Resources for IT Professionals" on TechNet at <http://go.microsoft.com/fwlink/?linkid=20969> has links to many other resources regarding Windows XP SP2. This page is updated periodically with the most recent information that is available.

In addition, we appreciate feedback on our documentation and our product. The following resources are available to you for providing feedback:

- Windows XP Service Pack 2 Newsgroups.** Newsgroups are a great place to ask questions of other users and find general information about other user's experiences with Windows XP SP2. You can examine some of the newsgroups using a Web browser on the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=32745>.
- Product Support Services.** If you are having a problem with your computer after installing Windows XP Service Pack 2, check the product support Web site on Microsoft.com first to see if your issue has been identified in the Frequently Asked Questions or by a KB article. If not, you can contact Product Support Services to get help with your issue. To start, see "Windows XP Support Center" on the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=32754>.
- Microsoft Wish Program.** If you have a suggestion about how to improve a feature in Windows that you would like considered for the next service pack or major Windows version, you can contact the Microsoft Wish Program and tell them your idea. To find out how to send a comment or suggestion, see "How to Contact the Microsoft Wish Program" on the Microsoft Knowledge Base at <http://go.microsoft.com/fwlink/?LinkId=32748>.
- Documentation feedback.** If you have any comments or suggestions about Windows XP Service Pack 2 documents, on the Web version of this document, on the Microsoft Web site at <http://go.microsoft.com/fwlink/?linkid=29126>, at the bottom of the page, click **Comments** and tell us what you think. Note that this is only for comments on the documentation, not the product itself.

[⬆Top of page](#)

Component Sections

Part 1: Introduction

Part 2: Network Protection Technologies

Part 3: Memory Protection Technologies

Part 4: E-mail Handling Technologies

Part 5: Web Browsing Security

Part 6: Computer Maintenance

Part 7: Updated features

Part 8: Conclusion and Appendices

[⬆Top of page](#)

Scope of This Document

This document specifically focuses on the changes between earlier versions of Windows XP and Windows XP Service Pack 2 (SP2) and reflects the current thinking of Microsoft about Service Pack 2 and its implications for developers. Examples and details are provided for several of the technologies that are experiencing the biggest changes: such as remote procedure calls (RPC), DCOM, Windows Firewall (previously called Internet Connection Firewall or ICF), and data execution prevention.

Additional information is available to developers on the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=20969>. The goal for Service Pack 2 is to build on the Trustworthy Computing efforts of Microsoft that have previously been applied to Windows Server 2003. For an overview of the Microsoft Trustworthy Computing initiative, see “Trustworthy Computing Defined,” on the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=20970>.

[↶Top of page](#)

Overview of Windows XP Service Pack 2 Security Technologies

In Windows XP Service Pack 2, Microsoft is delivering several improved security technologies that help protect customers against malware and other risks to their computer. These technologies are not intended to replace periodic security updates as they are released, but rather to help strengthen Windows XP's overall defenses against malicious attacks.

•**Network protection.** These security technologies help to provide better protection against network-based attacks, like MSBlaster, through a number of innovations, including enhancements to Windows Firewall and a reduced RPC attack surface. These enhancements include turning on Windows Firewall in default installations of Service Pack 2, closing ports except when they are in use, improving the user interface for configuration, improving application compatibility when Windows Firewall is on, and enhancing enterprise administration of Windows Firewall through Group Policy. The attack surface of the Remote Procedure Call (RPC) service is reduced, and you can run RPC objects with reduced credentials. The DCOM infrastructure also has additional access control restrictions to reduce the risk of a successful network attack.

- Memory protection.** Some attacks by malicious software leverage software security vulnerabilities that allow too much data to be copied into areas of the computer's memory. These vulnerabilities are typically referred to as *buffer overruns*. Although no single technique can completely eliminate this type of vulnerability, Microsoft is employing a number of security technologies to mitigate these attacks from different angles. First, core Windows components have been recompiled with the most recent version of our compiler technology, which provides added protection against buffer overruns. Additionally, Microsoft is working with microprocessor companies to help Windows support hardware-enforced *data execution prevention* (DEP) on microprocessors that contain the feature. Data execution prevention uses the CPU to mark all memory locations in an application as non-executable, unless the location explicitly contains executable code. This way, when an attacking worm or virus inserts program code into a portion of memory marked for data only, an application or Windows component will not run it.
- E-mail handling.** Security technologies help to stop viruses (such as SoBig.F) that spread through e-mail and instant messaging. These technologies include default settings that have enhanced security, improved attachment control using the Attachment Execution Service (AES) API. This results in security and reliability enhancements for communications applications such as Microsoft Outlook, Outlook Express and Windows Messenger. As a result, potentially unsafe attachments that are sent through e-mail and instant messages are isolated so that they are less likely to affect other parts of the system.
- Browsing security.** Security technologies that are delivered in Microsoft Internet Explorer provide improved protection against malicious content on the Web. One enhancement includes locking down the Local Machine zone to help prevent the running of malicious scripts and fortifying against harmful Web downloads. Additionally, better user controls and user interfaces are provided that help prevent malicious ActiveX® controls and spyware from running on customers' systems without their knowledge and consent.
- Computer maintenance.** A very important part of any security plan is keeping computers updated with the latest software and security updates and understanding the role they play in protecting your computer. Ensuring that you have current knowledge of security attacks and trends is also important. For example, some software updates that mitigated known viruses and worms were available days or weeks before any significant attacks began. New technologies are being added to help the end user stay up-to-date. These technologies include Security Center, which provides a central location for information about the security of your computer, and Windows Installer, which provides more security options for software installation.

Microsoft understands that security technologies are only one

aspect of a sound defense-in-depth security strategy. The security technologies outlined here are the next steps being taken in the Trustworthy Computing initiative to make customers' systems more resilient to malicious attacks.

[⬆Top of page](#)

1 of 8 [▶](#)

[Manage Your Profile](#) | [Contact Us](#) | [Newsletter](#)

© 2006 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

Microsoft

[MSDN Home](#)[Developer Centers](#)[Library](#)[Downloads](#)[How to Buy](#)[Subscribers](#)[Worldwide](#)

Search for

Microsoft® Security Developer Center

Helping developers to create secure software

[MSDN Home](#) > [Security Developer Center](#) > [Product Information](#) > Windows XP SP2

Advanced Search

[Security Developer Center](#)[Product Information](#)[Visual Studio 2005 Security](#)[Understanding Security](#)[Writing Secure Code](#)[Downloads](#)[Community](#)[Security Resource Kit](#)

Windows XP Service Pack 2 - Security Information for Developers

With Windows XP Service Pack 2 (SP2),

Microsoft is introducing a set of security

technologies that will help improve



Windows XP-based computers' ability to withstand malicious attacks from

viruses and worms.

These technologies include:

- Network protection
- Memory protection
- Improved email security
- Safer browsing

Together, these security technologies will help make it more difficult to attack Windows XP, even if the latest patches or updates aren't applied.

These security technologies together are particularly useful mitigation against worms and viruses. To developers these technologies will have impacts on the applications that they create and the tools they use. This page contains resources to assist developers in dealing with these impacts.

Other Resources


- [Windows XP Service Pack 2 Support Center](#)
- [Microsoft TechNet Windows XP SP2 Page](#)
- [Microsoft Security Home Page](#)
- [Microsoft Windows Home Page](#)

Downloads


Microsoft is making the Windows XP Service Pack 2 download available to developers for testing their applications. Microsoft recommends that consumers turn on [automatic updates](#) and wait for the release through [Windows Update](#).

[Microsoft Windows Update](#)

Windows XP Service Pack 2 is now available through Windows Update. Windows Update is your best option for updating a single machine to Service Pack 2.

[Windows XP Service Pack 2 Available to MSDN Subscribers](#)

Microsoft Windows XP Service Pack 2, available through Subscriber Downloads. (MSDN subscribers should use this link.)

[Windows XP Service Pack 2](#)

Microsoft Windows XP Service Pack 2, available from the Microsoft Download Center.

Articles and White Papers

[Windows XP Service Pack 2](#)

[Overview White Paper](#)

Windows XP Service Pack 2 addresses new challenges to the security of personal computers by making a number of basic improvements to the operating system. This white paper introduces Windows XP Service Pack 2 and provides an overview of what the service pack provides. (1.5 MB Word Document)

[Fine-Tune Your Web Site for Windows XP Service Pack 2](#)

Make your Web site work well with the new security features in Windows XP SP2 that affect ActiveX controls, file downloads, pop-up windows, and more.

[How to Enable Remote](#)

[Debugging on Windows XP Service Pack 2](#)

Windows XP Service Pack 2 introduces several security enhancements that increase security in Microsoft Windows. See



[Windows XP Service Pack](#)

[2 Checked Build](#)

This is the "Checked Build" of Microsoft Windows XP Service Pack 2, available from the Microsoft Download Center.

Note that this is a special build of Windows XP Service Pack 2 for developers using the program for debugging and testing their applications. Do not install this version on a production machine. It is for test purposes only.



[Windows XP SP2 Platform](#)

[SDK](#)

The Windows XP Service Pack 2 Platform SDK contains the information you need to develop applications for Microsoft Windows XP Service Pack 2.

Training

the steps you need to take in order to enable remote debugging on a Windows XP Service Pack 2 machine.

[Changes to Functionality in](#)

[Microsoft Windows XP Service Pack 2](#)

This document specifically focuses on the changes between earlier versions of Windows XP and Windows XP Service Pack 2 and reflects Microsoft's early thinking about Service Pack 2 and its implications for developers.



[Windows XP Service Pack](#)

[2 Training for Developers](#)

Learn how you, the developer, are affected by Windows XP Service Pack 2 and the implications for end users running on the Windows XP Professional and Windows XP Home Editions. The course covers the rationale for increased security in Windows XP SP2 and provides a technical review of Windows XP SP2. It also covers impacts to existing applications and includes code samples



[Microsoft Executive Circle](#)

[Webcast: Securing the Perimeter through Best Practices and Increasing System Resiliency in Windows XP SP2](#)

Microsoft's senior executive in charge of security Mike Nash gives updates on the upcoming service packs to Windows XP and Windows

2003 which are focused on
developing system resiliency,
as well as updates on new
security resources and
guidance for customers.

 [Top of Page](#)

[Manage Your Profile](#) | [Legal](#) | [Contact Us](#) | [MSDN Flash Newsletter](#)

© 2006 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

Microsoft