

Windows XP Service Pack 2 Impact & Recovery

The links that appear in the PDF version of this document do not work.

The uses of the instructions here in are at the reader's own risk! The contents of this document represent a best effort at identifying the areas modified or added by the service pack named above and providing the instructions to recover normal operations after it is installed. Neither Executive Technologies Corporation (EXECTECH™) nor the author assume responsibility for the accuracy of this document as Microsoft® may alter the content and impact of the service pack at any time.

Computer Reseller News (CRN), a publication directed at computer resellers and integrators, published three articles regarding Service Pack 2 that are worthy of review. We have provided links to them below.

Windows XP Service Pack 2: Install With Care (2 of 5 machines would not restart after installing SP2 – can you take the risk?)

<http://www.crn.com/sections/breakingnews/breakingnews.jhtml?articleId=23905071>

Windows XP Service Pack 2 Breaks Microsoft CRM (Microsoft's own applications are affected by SP2)

<http://www.crn.com/showArticle.jhtml?articleID=26805844>

Microsoft Names Almost 50 Apps That Require SP2 Tweaks (Oops!)

<http://www.crn.com/sections/breakingnews/breakingnews.jhtml?articleId=29100510>

RECOMMENDATION 1: Turn Automatic Windows Update service OFF on all your Windows® XP computers. [Control Panel > Windows Update icon> Uncheck to disable.]

RECOMMENDATION 2: Wait at least two months before installing SP2 to allow Microsoft® to respond to the feedback from the computer user community. Do your Windows Updates manually, but always “remove” SP2 from the selection list.

Why publish this document?

Microsoft® will *significantly modify the functionality and operation* of your Windows® XP operating system with the installation of Service Pack 2. Microsoft® has decided that the user is not intelligent enough to secure the computers against security threats so they are going to do it without providing options at installation time. These security “features” will disable your computer's ability to function in a network, access the Internet, run certain applications, and aggravate and frustrate you. EXECTECH™ has published this document to provide its clients insights into the impact of installing SP2 on their ability to do business and how to mitigate or undo the default settings. **All clients are strongly advised to implement recommendations 1 & 2 above immediately!**

The original **release date** for SP2 is **August 16, 2004**, but has been delayed in typical Microsoft® fashion to **August 25th** to “allow the business community to prepare”. While EXECTECH™ applauds some of the new features such as Bluetooth and Wi-Fi, the alteration of existing functions to lock down the computer for “security” reasons is asinine. Several new features provide interaction with “future” Microsoft® products, which in our opinion is unwarranted at this time and may actually prevent 3rd party applications from running providing an unfair competitive advantage to Microsoft®. It is the first time that a service pack will be

distributed via Windows Update Service (WUS) and in our opinion it has the potential to overload the Internet bandwidth allocation for the WUS servers. The size of the download is **over 260 MB**. Not a smart business move.

Microsoft® has created a new Windows Update Service website for Windows XP. We urge you NOT to use the “express” method. It does not allow the selection of updates to install.

Document Overview

Changed/New “features” below are arranged in descending order of impact in our opinion. The mitigate/undo/workaround instructions are based on Microsoft® published documentation as of August 16, 2004 and may change as more information becomes available and/or actual tests are made by EXECTECH™. For readers who desire detailed and technical information on all of the “features” added or changed by SP2, it is available in the html document at the link below:

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

Only those “features” that will or may negatively impact the business operation of your computer are addressed below.

SP2 Features Impacting Functionality

1 - Windows Firewall (previously called Internet Connection Firewall or ICF)

IMPACT

- Enabled Automatically – **ALL** network connectivity will be blocked until either the Windows Firewall (WF) is disabled or the appropriate exception(s) is set in the Security Settings on the WF properties page.
- New global control application accessed via Control Panel and new icon there. Previously each connection had its own firewall settings.
- Administrative group membership is required to modify the operation of WF or respond to its prompts when a program or service is blocked.
- ALL Remote Procedure Calls (RPC) are disabled as Port 445 is closed by WF.
- Domain member computers with multiple profiles (usually notebooks with “Out-of-Office” and “In-Office” profiles) **MUST** have the same permitted applications set in both profiles.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- Turn off the firewall - All Connections:
 - Control Panel > Windows Firewall icon > General Tab > click on Off radio button > Apply > Ok
- Turn off the firewall – Selected Connection:
 - Control Panel > Windows Firewall icon > Advanced Tab > take check off of selected connection > Apply > Ok
- Reboot the PC by Start > Shutdown > Restart

2 – Remote Procedure Call (RPC) Interface Restriction

IMPACT

The addition of the new **RestrictRemoteClients** registry key is the most significant change. The key modifies the behavior of **ALL** RPC interfaces on the computer and will eliminate remote anonymous access to RPC interfaces on the system, with some exceptions as a default. Other changes include the

EnableAuthEpResolution registry key and three new interface registration flags. This key is designed for software developers to work around the setting in the first key – in other words it is a backdoor. Microsoft® professes that these changes impact only software developers but in our opinion this is a snake in the grass. There is no interface to alter the settings. The user must edit the registry in order to restore functionality.

Restrict Remote Clients

Key Name: **RestrictRemoteClients**
Type: DWORD
Values: 0 = No Restrictions
1 = Reject Anonymous Calls with exceptions (**DEFAULT**)
2 = Reject ALL

Enable Authentication End Point Resolution

Key Name: **EnableAuthEpResolution**
Type: DWORD
Values: 0 = Disabled (**DEFAULT**)
1 = Enabled

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

Use extreme care in following these instructions. Changing the wrong value may destroy access to your computer or an application.

- Start > Run > enter “Regedit” without the quotes > click on Ok
- Drill down by clicking the plus (+) signs on the left to Hkey_Local_Machine > Software > Policies > Microsoft > Windows NT > RPC
- Double click on the key on the **RestrictRemoteClients** key
- Change the value to 0 (zero)
- Click on *Registry* in the menu bar at the top of the window and click on *Exit*.
- Restart the PC by Start > Shutdown > Restart

3 – Microsoft® Distributed Transaction Coordinator (MSDTC)

Microsoft® describes the function of the MSDTC as: “The Distributed Transaction Coordinator (DTC) service coordinates transactions that update two or more transaction-protected resources, such as databases, message queues, files systems, and so on. These transaction-protected resources may be on a single computer or distributed across many networked computers.”

IMPACT

- Disables the update capability in and out of the items named above; i.e. your ability to do business may be blocked.
- A new tab is added to the Systems Properties control function in the form of an MSDTC tab.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- Control Panel > Administrative Tools > Component Services > open Component Services > open Computers folder > right click on My Computer and click Properties
- Click on the MSDTC tab
- Network DTC – set to ON (SP2 DEFAULT is OFF)
- Allow Inbound – set to ON (SP2 DEFAULT is OFF)

- Allow Outbound – set to ON (SP2 DEFAULT is OFF)
- Add MSDTC.EXE to exception list in Windows Firewall if it is enabled

4 – Distributed Component Object Model (DCOM) Security Enhancements

DCOM governs how OLE (Object Linking & Embedding) functions on the PC for the local user and other users that access applications running on it.

IMPACT

- All access requests are checked as a result of the new settings and can prevent access to applications and data locally and remotely.
- The Launch Local, Launch Activation, Remote Launch & Remote Activation are restricted to members of the Administrators group rather than the Everyone Group.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- Least desirable option: Make all users members of the Administrators group
- Use the Component Services Microsoft Management Console (MMC) to alter the settings for the computer and COM components.
 - Control Panel > Administrative Tools > Component Services
 - Drill down by clicking on the plus (+) signs: Component Services > Computers > My Computer > COM+ Applications
 - Click the plus (+) sign next to each application in the COM+ Applications folder
 - Click the Roles folder underneath each. Ignore those with no user or group defined.
 - The System Application folder is the likely place where you will find multiple roles defined. Those that are customarily set to the group Everyone are:
Any Application
Reader
Server Application
 - Add the Everyone group back the respective Role if missing.

5 - Data Execution Prevention (DEP) – NEW

This new “feature” raises an exception when program code attempts to run from unauthorized/restricted areas of memory (RAM). Two implementations of this “feature” exist: Hardware (HW) and Software (SW). For all intents this is a “future” provisioning by Microsoft®, but may present issues for current applications since the foundation in hardware and software does not exist at this time.

The SW implementation does not become effective unless a program is compiled with a compiler using Microsoft’s Safe Structured Handling Exception code. The HW implementation is dependent upon the processor in your computer. If it has the feature encoded, it will be utilized.

IMPACT

- May prevent your current programs from running thereby forcing an upgrade or replacement of it.
- Adds new interface under System Properties > Advanced > Performance Settings to turn off/on and provide exempt applications.
- Modifies the hidden file boot.ini on the root drive of the computer.
- New BOOTCFG.EXE program to configure the boot.ini file.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- Open Control Panel
- Click on System > Advanced > Performance Settings > Data Execution Prevention tab
- Click on enable for all programs (2nd option)
- Add exempt applications
- Click on Apply
- Click on Ok
- Click on Ok/Close to exit System Properties
- Restart the PC by Start > Shutdown > Restart

Note: Instructions on using the BOOTCFG.EXE program are not provided at this time, as we do not have access to it. Future releases may contain such instructions.

6 – TCP/IP

Microsoft® describes the impact of the changes to TCP/IP in Windows XP by SP2 as: “A very small number of Windows applications make use of raw IP sockets, which provide an industry-standard way for applications to create TCP/IP packets with fewer integrity and security checks by the TCP/IP stack. The Windows implementation of TCP/IP still supports receiving traffic on raw IP sockets.”

IMPACT

- TCP data cannot be sent over raw sockets.
- UDP datagrams with invalid source addresses cannot be sent over raw sockets. The IP source address for any outgoing UDP datagram must exist on a network interface or the datagram is dropped.
- The number of incomplete outbound TCP connection attempts will be monitored and an exception recorded in the System Event Log if the limit is reached. Those requests over the limit will be queued and resolved at a fix rate. This may cause a significant reduction in speed of the computer.
- Layered Service Provider (LSP) applications such as Content Filtering, Parental Controls, anti-virus programs and the like may not be able to run/update.
- Provisions have been made for a “self healing” Winsock in the netsh.exe command line utility to allow the removal of corrupted LSP settings.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- Obtain the patches to and/or upgrade the applications impacted by this change.

7 – Alerter and Messenger Services Disabled

Microsoft® describes the services: “The Alerter and Messenger services are components of Windows that allow simple messages to be communicated between computers on a network. The Messenger service relays messages from different applications and services, while the Alerter service is intended specifically for administrative alerts.” Historically the Messenger service starts automatically with the computer while the Alerter is started manually or when a program calls for it.

IMPACT

- Alerter service stopped and set to Disabled. This may prevent your applications from advising you of operational issues encountered.
- Messenger service stopped and set to Disabled. May prevent certain system monitoring applications such as power utilization and battery backup monitoring to fail.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- Control Panel > Administrative Tools > Services
- Double click on Alerter
 - Change Startup Type to “Manual”
 - Click on Apply button
 - Click on Ok button
- Locate Messenger and double click on it
 - Change Startup Type to “Automatic”
 - Click on Apply button
 - Click on Ok button
- Close Services
- Close Administrative Tools
- Close Control Panel
- Restart the PC by Start > Shutdown > Restart

8 – USB Memory Devices (Memory Sticks & Hard Drives)

A new key will be added to the registry that enables turning off the ability to write to USB memory devices.

IMPACT

- Creates new registry key:
Hkey_Local_Machine\System\CurrentControlSet\Control\StorageDevicePolicies
Type: DWORD
Value: 0 = Disabled (**DEFAULT**) [writing to devices will be allowed]
 1 = Enabled
- May prevent writing to USB memory device if changed by an application or Windows update.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- No action required unless you are unable to write to a device you could before. You must edit the registry in order to verify/change the setting.

9 – New Windows Installer 3.0***IMPACT***

- Uses a new installation format that will force software providers to update their software IF they call the Windows Installer.
- May impact the add/remove programs such that programs installed with an earlier version will not uninstall properly and/or completely.
- ALL installations from FTP or GOPHER (UNIX/LINUX) sites will fail if run over the Internet.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- Follow manufacturer’s instructions for manual removal of software or download an uninstall program from that company.
- Download the desired program from the FTP/GOPHER site to your hard drive and run it from there.

10 – Wireless Network Setup Wizard

Claimed to simplify setting up a secure wireless network, but on the backside requires that the wireless network be secure.

IMPACT

- Forces utilizing secure wireless communications when a wireless network is involved. Existing wireless network functionality may be disabled.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- Anticipate that wireless connectivity will not be available and make accommodations for using a wired network attachment until wireless connectivity can be restored.
- Step through the Wireless Network Setup Wizard to configure your wireless network.

11 – Windows Messenger

Provides a new security configuration for instant messaging communication with Windows Messenger (WM) and MSN Messenger.

IMPACT

- A plug-in is added to Internet Explorer 6.0 (IE 6.0) for Windows Messenger
- A user display name will be required.
- File transfers that it deems to be “unsafe” will be blocked.
- Windows Firewall has provisioning for the Windows Messenger.
- The add/remove of WM in Windows Components has no functionality after SP2 is installed.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- **We are unaware of any way to remove WM.**
- **We recommend that it not be used by disabling it in IE 6.0**
 - To disable in IE 6.0:
 - Tools > Internet Options > Programs > Manage Add-ons button > Windows Messenger > Disable > Ok > Ok

12 – Bluetooth – NEW

Bluetooth is a wireless technology that allows communication between dissimilar devices equipped with it. The functionality of Bluetooth has been dependent upon drivers and applications from 3rd party providers prior to SP2.

IMPACT

- May cause 3rd party applications and devices to malfunction or not work at all.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- Check with the device manufacturer for new drivers and/or updated software. Install as appropriate.
- Interim measures should be taken to provide the same functionality through other devices if they are of a critical business nature.

13 – Windows Media Player 9

If Windows Media Player is not installed, it will be without option.

IMPACT

- Licenses for digital media will be lost.
- The application will be installed regardless of your desire.

MITIGATE/UNDO/WORKAROUND (must have administrators group membership)

- Backup your digital media license files using License Management in Media Player BEFORE installing SP2.
- Uninstall it after SP2 has been installed via the Add/Remove Programs in Control Panel under Windows Components.

SUMMARY

There are many more new and updated features contained in SP2. We reiterate that those covered above represent the most potentially dangerous to your business in our opinion. There could be others that are undocumented by Microsoft® that will only become apparent after SP2 is installed on each computer. We encourage you to contact your application software vendors to determine compatibility with SP2.

In reality there is not any one new or enhanced feature in SP2 that warrants installing it in a business network. If your company can abandon using Windows Automatic Update, then it is the most secure and economical safeguard that can be taken. Remember that 2 of 5 computers that had SP2 installed resulted in a failed installation and a “blue screen of death” requiring hours of high-level technical recovery. Is it worth the risk?

If installing SP2 is forced on you, then do the following:

1. Go to the Windows XP home page from the www.microsoft.com and do a search for “SP2 Applications” to get a listing of knowledgebase articles that disclose compatibility issues with applications. This will enable you to anticipate problems you may encounter.
2. Confirm compatibility with providers of your critical applications. Download any updates or patches to your hard drive before installing SP2.
3. Make a full system image backup using Symantec Ghost or some other reliable hard disk imaging software. *Author’s Note:* The reason this is recommended is that after 16 years of dealing with Microsoft®, I have come to distrust their software’s ability to uninstall itself properly. The image you create is our second level of protection.
4. Place that image on a device/media with the capacity to be accessed in MS DOS mode. Be sure the drivers for the device are on your boot diskette.
5. If it is on another computer’s hard drive, make sure that you have the proper drivers for the network card in your computer on the diskette. Few, if any, USB devices are not accessible in MS DOS mode.
6. Test the boot diskette/CD/Zip at least 2 times successfully.
7. If you are unable to complete steps 1 through 4, then make a backup of ALL your data files on removable media (diskette, Zip disk, CD, tape or a network drive).
8. Locate the Windows XP CD and keep it at hand.
9. Any diskettes/CDs that contain drivers and programs for your computer should be located and close at hand as well.
10. Turn on System Restore on the XP computer. Control Panel > System > System Restore tab > uncheck the box. **Warning!** Make sure you have sufficient space available on your hard disk drive to do this, if you do not, then you will have to leave System Restore disabled.
11. Set your screen saver to “None”. Control Panel > Display > Screen Saver tab > select None from dropdown list > Apply > Ok
12. Turn off ALL power saving features. Control Panel > Power Options > Make all settings equal Never on the first tab > on the Hibernate tab uncheck if checked > Apply > Ok
13. Notebook computers MUST be on AC power.

14. Make sure the user you are logged on to the computer, as is the owner or is a member of the computer's administrators group and to the local/computer domain (not your network domain). Verify by viewing membership to the Administrators group in Control Panel > Users.

If the volume of data on your hard drive is too large to image, then **BACKUP ALL** of your **DATA FILES** to another device. Test the access to those data files on the storage media randomly for each type of data file you have saved on it. The programs can always be re-installed but the data cannot be easily created.

We stand ready to assist you in the event SP2 is accidentally installed, or your attempt fails. Priority will be given to those clients that maintain a block of service hours with us. All others will be handled on a first come, first served basis.

There is no intent on the part of the author or EXECTECH™ to assume or take ownership or title of any registered, copyrighted, or trademarked name, product or document referenced here in. They remain the sole property of their respective owners/authors.