Global Information Assurance Certification Paper

Windows XP Service Pack 2 - Assessment, Installation and Secure Configuration

9th January 2005
GSEC 1.4c

Aaron Webber

Introduction

The focus of this paper is on Service Pack 2 (SP2) for Windows XP. Microsoft released SP2 in August 2004, and since then, millions of users worldwide have installed SP2 with a mixed response. Many users have been reluctant to proceed with the SP2 installation due to the risk of system crash and application problems; and some users simply do not see value in the extra security and functionality provided by the update. Now that much of the initial hype and installation concerns surrounding SP2 are behind us, this paper will look at the security benefits provided by SP2, and help users determine if the update would be of benefit to them. If users believe there is too much risk or their current system set up is secure, a list of key internet security guidelines have been provided as an alternative. This paper will also provide a "how to" guide to install and securely configure SP2, assisting users to understand what the SP2 security configurations actually mean and how they are applied. Content discussed is focussed from the perspective of a user with a typical home PC set up; therefore SP2 changes that were designed for corporate environments have not been covered. This paper will focus on the security features of SP2, and is not intended to provide an assessment of extra operating system or application functionality.

Despite the extra functionality provided by SP2, clearly Microsoft's focus was to improve security. A number of known vulnerabilities have been addressed and security improvements made through SP2. This has been achieved through the introduction of the Security Center; and changes to Automatic Updates, Internet Connection Firewall (ICF), Internet Explorer (IE) and Outlook Express (OE). Overall, Microsoft has had a good attempt at fixing a number of security issues associated with Windows XP.

Service Pack 2 - Background

A Service Pack is defined as a number of individual patches combined into one to prevent users having to install new non-critical updates every few days. Microsoft releases Service Packs about once a year.[1] Service Pack 1 (SP1) for Windows XP was released by Microsoft in 2002[2]. Despite the fixes that were implemented as part of the SP1 update, a myriad of other security issues have since arisen with Windows XP, IE, and OE. Hackers have exploited vulnerabilities in the XP code, ICF, IE, and OE to gain access to our PCs, personal details and credit card information. As the next version of Windows (code named Longhorn) was not due for release until 2007, Microsoft decided it could not wait any longer to fix the security holes in XP, hence the release of SP2[3]. So far, over 100 million copies of SP2 have been distributed to users worldwide[4].

---

[1] PC Authority, p.8
[2] Spanbauer, p.1
[3] PC Authority, p.9
[4] Australian IT, http://australianit.news.com.au/articles/0%2C7204%2C11137838^15321^^nbv^15306%2C00.html

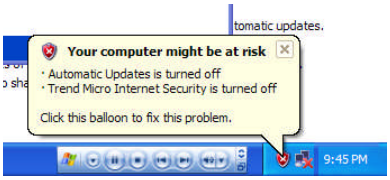
SP2 Security Features and Changes

Windows Update

Changes have been made to the Windows Update site, however these changes are not made through the installation of SP2. The site has been moved from version four to version five, allowing users to resume downloading if the internet connection is lost[5]. This is particularly useful given the large size of the SP2 download.

Security Center

One of the most noticeable changes SP2 makes is the introduction of the Security Center, a tool which checks to ensure your system is running a software firewall, up-to-date anti-virus program, and that Automatic Updates are set to download and install updates (recommended Microsoft guideline)[6]. If one of these security components is not installed or the settings lower computer security, the Security Center places a red shield icon in the notification area. Clicking on the icon opens the Security Center, provides the reason for the security notification, and details a recommendation of how to fix the issue[7]. It also allows users to access the Windows Firewall (WF), Automatic Updates and IE security settings from one central location.



Automatic Updates

Automatic Updates are not new to SP2. When Automatic Updates are turned on, Windows takes responsibility for alerting the user when updates are available. This feature prevents users having to remember to regularly check the Windows Update site. If Automatic Updates are turned off or are set differently than the recommended Microsoft guidelines, the Security Center alerts users to change the settings[8].

Windows Firewall

One of the best changes made by SP2 is the WF. The ICF had many limitations and

[5] PC Authority, p.9
[6] Microsoft, http://www.microsoft.com/windowsxp/using/security/internet/sp2_wscintro.mspx
[7] Microsoft, http://www.microsoft.com/windowsxp/sp2/technologiesoverview.mspx
[8] Microsoft, http://www.microsoft.com/windowsxp/sp2/technologiesoverview.mspx

consequently has been replaced by the WF. "WF is a stateful filtering firewall, which means it analyses each packet for more than just its source and destination, as would be done with a static packet filter. Instead it looks at the content of the packet, as well as the connection it is using to see whether it should be allowed[9]."

WF consists of a wide range of features to help protect computer security including:

- WF is much easier to locate than the ICF
- WF is on during boot-up[10]
- WF is enabled by default[11]
- Exceptions can be configured both in the form of programs and port numbers (TCP and UDP)
- Specific network connections (such as LAN or broadband) can have their own individual firewall rules
- WF allows traffic logging, both dropped packets and successful connections.

As WF is on by default, some applications may not be able to access the internet after you install SP2[12]. You may be required to set exceptions as discussed later on.

Note that WF only scans incoming traffic, therefore if your computer is infected by a worm or trojan, it can still access the internet[13]. Installing a third-party software firewall is required to provide outbound traffic protection as well.

Anti-virus software

Anti-virus software is not included as part of the SP2 upgrade. SP2 does however (through the Security Center) alert you to have an anti-virus program installed, keep it up-to-date, and set real time scanning.

Internet Explorer

SP2 makes a number of changes to improve security in IE including:

- Pop-ups are blocked through the Pop-up Blocker
- Add-ons can be disabled through the Add-on Manager[14]
- Drive-by downloads (files downloaded onto a computer automatically without user permission when visiting a malicious web site) are blocked[15].

[9] PC Authority, p.124
[10] Thurrott, http://winsupersite.com/reviews/windowsxp_sp2.asp
[11] Microsoft, http://www.microsoft.com/windowsxp/sp2/technologiesoverview.mspx
[12] PC Authority, p.124
[13] PC Authority, p.124
[14] Microsoft, http://www.microsoft.com/windowsxp/sp2/technologiesoverview.mspx
[15] Thurrott, http://winsupersite.com/reviews/windowsxp_sp2.asp

Outlook Express

SP2 makes a number of changes to improve security in OE including:

- Attachment Manager stops potentially dangerous attachments being saved or opened
- External graphics (used to gain valid user e-mail addresses for spam purposes when OE contacts the web server to download images) are blocked[16].

Do You Need SP2?

SP2 is not a critical update for all users. I hope all users who have an internet connection already run a software firewall (such as Norton Personal Firewall) and anti-virus program (such as Norton AntiVirus); or better still, run a security suite (such as Trend Micro Internet Security) to help provide even more security through ad blocking, URL blocking and privacy measures.

Installing SP2 may not be of any real benefit if you are confident you have the following security measures in place:

- Software firewall running (and firewall rules appropriately configured)
- Anti-virus program running (that is set to scan real-time and keep definitions up-to-date)
- Install all critical Windows XP patches from Windows Update[17]
- Are careful when surfing the web and opening e-mail attachments
- Use an alternative web browser to Internet Explorer (such as Opera or Mozilla Firefox).

However, even if you have all these security measures in place, consideration should still be given to installing SP2 for two reasons:

1. The Security Center consistently notifies you if you are not running a firewall, anti-virus software (and if you turn off real time scanning or do not update definitions), or Automatic Updates are not set to Microsoft guidelines. This notification can be useful if you disable/change settings on one of these applications and forget to turn it back on, or if a user on your PC disables/changes settings in these applications without you knowing
2. Microsoft may stop supporting Windows XP systems that are not running SP2[18].

Essential Actions to Take If You Do Not Want to Install SP2

If you believe the risk of installing SP2 outweighs the benefits, it is essential you have the following security measures in place to minimise the chance of a successful attack

[16] Microsoft, http://www.microsoft.com/windowsxp/sp2/technologiesoverview.mspx
[17] Finnie, p.2
[18] PC User, p.83

on your system:

- Run a third-party software firewall such as Norton Personal Firewall. A free firewall, ZoneAlarm, can be downloaded at www.zonelabs.com. Ensure you configure the firewall rules appropriately, regularly review the firewall rules, and are aware of applications running on your system which access the internet
- Run third-party anti-virus software such as Norton AntiVirus. A free anti-virus program, Nod32, can be downloaded at www.nod32.com. Ensure you have real-time scanning set and update virus definitions regularly
- Run a third-party program to scan for spyware. A free scanning tool, Ad-ware, can be downloaded at www.lavasoft.com
- Run an alternative web browser to Internet Explorer. Free, more secure web browsers with extra functionality (Opera and Mozilla Firefox) can be downloaded at www.opera.com and www.mozilla.org
- Run an alternative e-mail client to Outlook Express. Free, more secure e-mail clients (Opera Mail and Mozilla Thunderbird) can be downloaded at www.opera.com and www.mozilla.org
- Employ safe web surfing practices and be careful when opening e-mail attachments
- Visit Windows Update site regularly and download and install critical patches[19].

Installation Risk

If you decide to proceed with the SP2 update, there is a chance that you will encounter problems. The SANS Internet Storm Center has run a rating summary for users to post their SP2 experiences. As at 29th December 2004, over 60% of respondents did not have major problems when installing SP2 (38% no problems, 24% small problems). 25% of respondents had major problems (12% could not use or install SP2, 13% had to rebuild their system)[20]. In support of these figures, a Canadian asset-monitoring company, AssetMatrix, performed a study that showed around one in ten users will experience problems when installing SP2.[21] Therefore, other user experience shows that problems can occur; however the chances are not overly high.

SP2 Installation

Obtain Copy of SP2

Before you download and install SP2, there are some key points you should be aware of:

- SP2 is a free download
- SP2 is designed to work on Windows XP Professional and Home Edition

---

[19] PC User, p.84
[20] Internet Storm Center, http://isc.sans.org/xpsp2.php
[21] Keizer, p.1

- SP2 includes SP1[22]
- SP2 will not install on illegitimate copies of XP[23]
- System requirements – PC running Windows XP, 233 Mhz processor, 64MB RAM, 900MB of available disk space, and a CD-ROM drive is installing via CD[24].

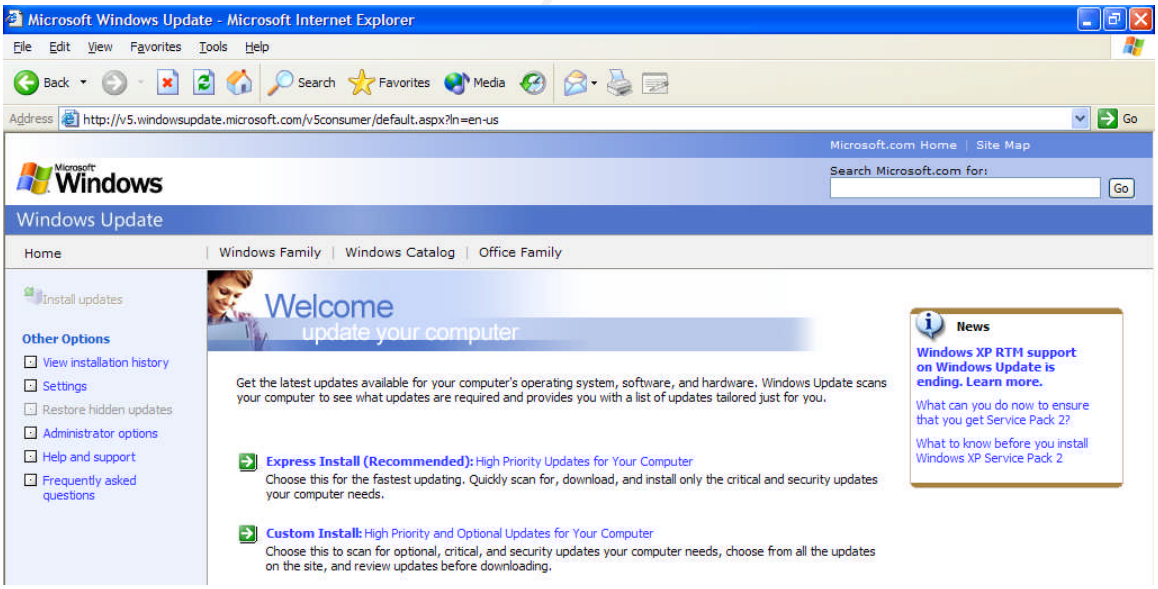
There are 2 ways you can obtain a copy of SP2:

1. Visit the Windows Update site – www.windowsupdate.com
2. Request SP2 on CD from the Microsoft site. Microsoft will post you the SP2 CD free of charge - visit the following site

http://www.microsoft.com/windowsxp/downloads/updates/sp2/cdorder/en_us/default.mspx

Note that cut down version (for home users) of SP2 is 75 megabytes in size (compared to 266 megabytes for the full version). If you on dial-up you may want to consider ordering the SP2 CD from Microsoft, as the download will take a considerable amount of time.

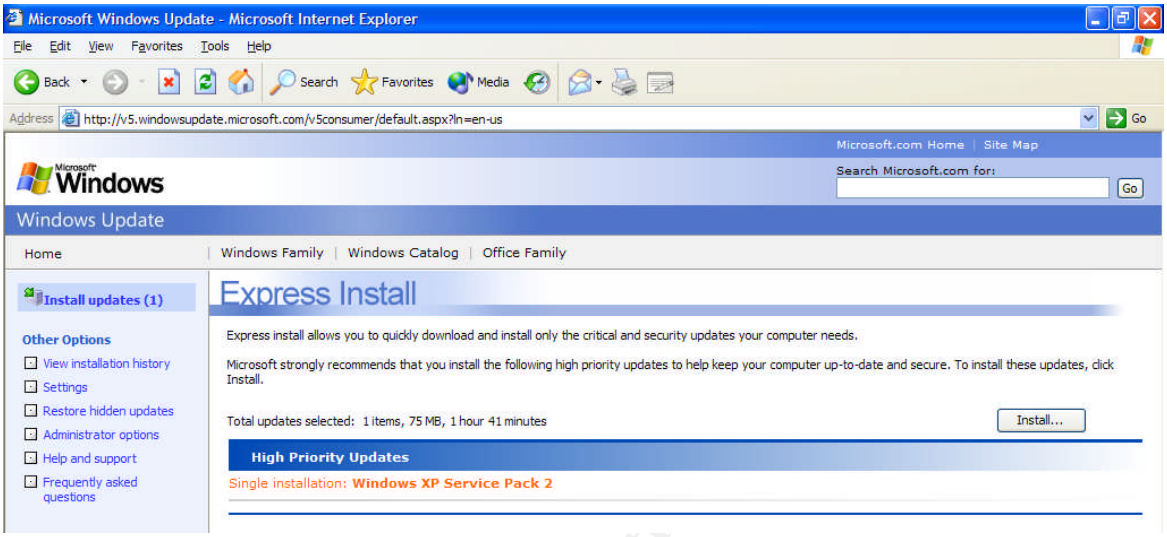
To download SP2 from the Windows Update site, please follow the steps below. Go to www.windowsupdate.com. Note that the Windows Update site will only open with the IE browser. If you have not visited the Windows Update site in a while, you will be asked to download Windows Update version five. This update is called the Background Intelligent Transfer Service (BITS), which controls the downloading of updates from the Windows Update site.



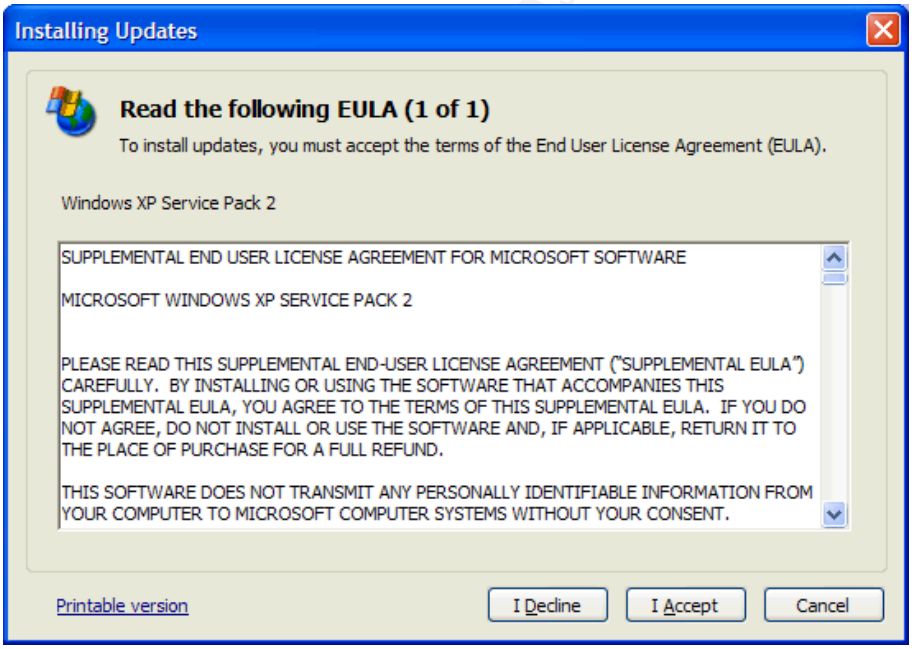
After you have downloaded and installed BITS, you will need to open Windows Update

[22] Microsoft, http://www.microsoft.com/windowsxp/sp2/overview.mspx
[23] PC Authority, p.7
[24] Microsoft, http://www.microsoft.com/windowsxp/sp2/overview.mspx

site and click on “Express Install”. The Windows Update site will scan your machine to identify any critical patches you do not have installed. Note that SP2 may not be immediately available for download. If your system is not fully patched with all critical updates, Windows Update will ask you to download a number of hotfixes. After you have installed these updates, click on “Express Install” again and the SP2 file will be available for download. Click on “Install” to download SP2.



Next you will be presented with a request to accept the End User License Agreement (EULA). Carefully read the terms and if you agree, click “I Accept”.



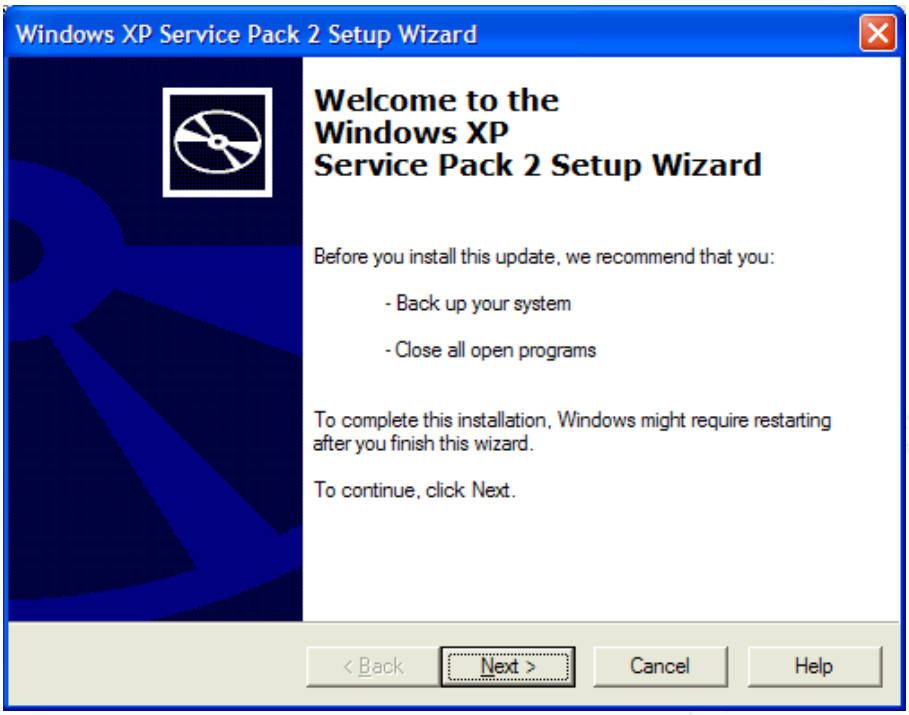
Install SP2

Before you install SP2, you should perform the following measures to reduce the impact of a failed installation:

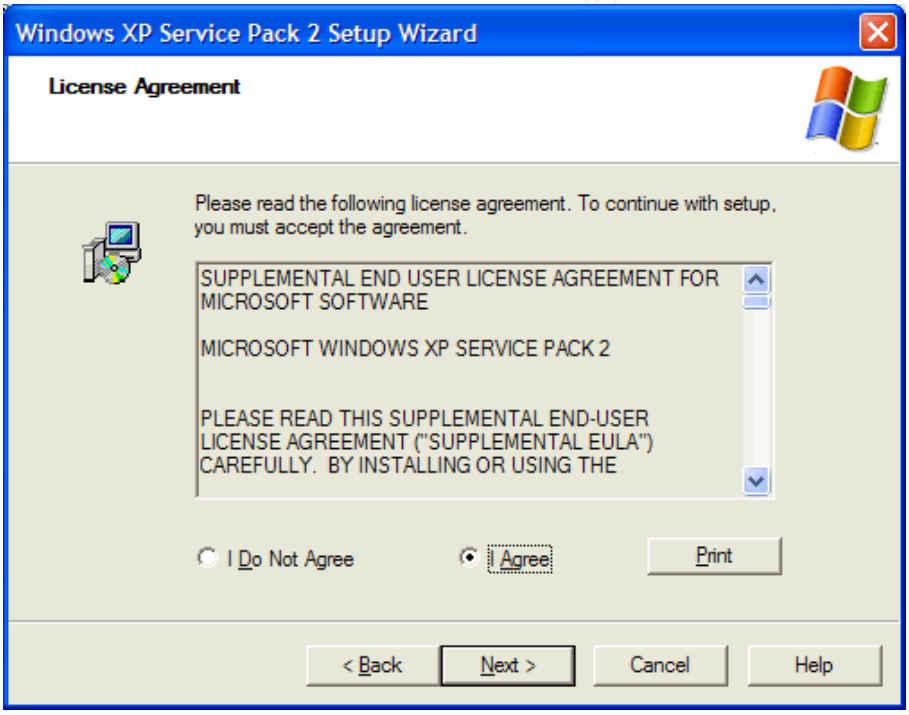
1. Backup all critical files and folders
2. Check your computer for spyware
3. Visit the homepages of your computer manufacturer and software applications you have running on your machine, and download any updates[25]. Many computers will need to update drivers before SP2 will run without breaking applications[26]
4. Temporarily disable or uninstall firewall and anti-virus software[27]. Failure to disable this software has resulted in a number of problems for users when installing SP2 (due to conflicts with changes SP2 is attempting to make). Make sure you do not have an active internet connection whilst you have this software temporarily disabled. After you have successfully installed SP2, remember to re-enable or re-install your firewall and anti-virus software before you connect to the internet.

After you are happy you have completed all the tasks mentioned above, you are now ready to install SP2. After the SP2 download is complete, you will be presented with the SP2 setup wizard. Click on “Next”.

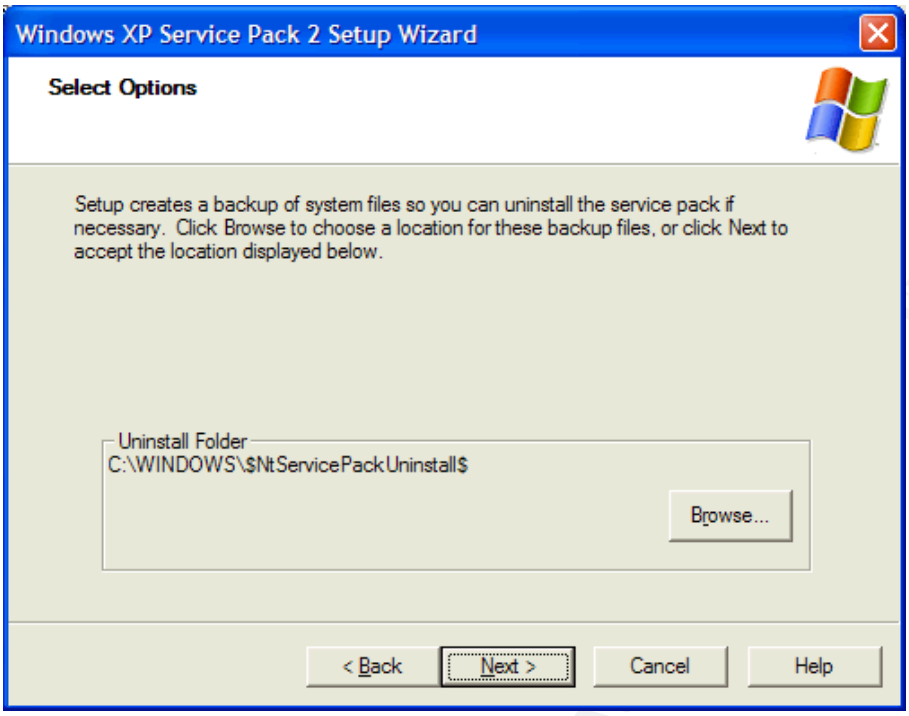
[25] Microsoft, http://www.microsoft.com/athome/security/protect/windowsxp/choose.aspx
[26] Rash, p.2
[27] Finnie, p.3



You will be presented with a request to accept for the Supplemental End User License Agreement. Carefully read the terms and if you agree, click “I Agree” and “Next”.



Next the setup process will check the current configuration of your system, archive current files and update files. Click “Next”. This took around 20 minutes when installing on my machine.



After this has completed, the setup process is finished. You will have to restart your machine for the changes to take affect, and hope that you have no issues. Click “Finish”.

If you experience problems, you can visit the Microsoft site at http://support.microsoft.com/search/?adv=0 and search for your problem in the Knowledge Base articles. Also, you can visit the SP2 community newsgroup where users have posted questions and answers they have experienced when installing SP2. You can find this newsgroup by searching for 'SP2' at http://communities2.microsoft.com/communities/newsgroups/en-us/default.aspx

One common SP2 installation problem faced by users has been a freeze during the setup process, resulting in a failed installation[28]. Microsoft has released a patch to fix this problem. If you encounter this problem, you can download the KB885894 patch at http://www.microsoft.com/downloads/details.aspx?familyid=36dd19df-bc5e-44b7-a339-6794d97994a2&displaylang=en

SP2 Configuration

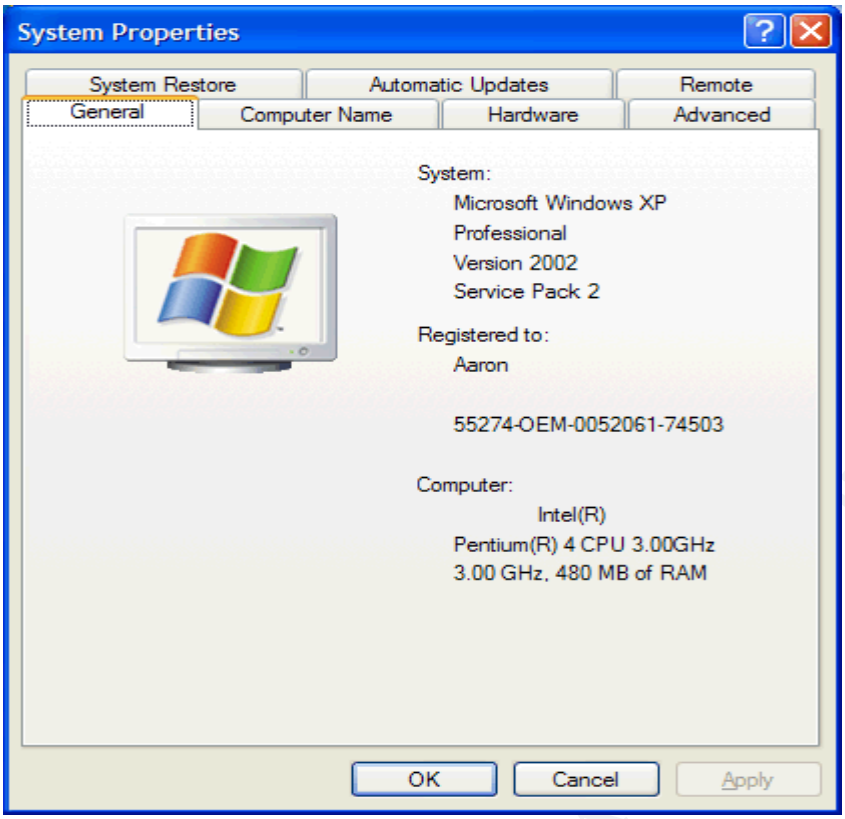
After resetting your computer, you will be presented with a screen that will ask you to turn on Automatic Updates. You are given two options:

1. Help protect my PC by turning on Automatic Updates
2. Not right now

I recommend you select on option one and click "Next". Windows will then open up as normal and you will be presented with the Security Center. If you have third-party firewall and anti-virus software, and have not already turned it back on, now is a good time. Note that the Security Center will say that the firewall is turned on (before you re-enable the third-party firewall). This is because the WF is turned on by default through the SP2 installation. If you decide to run a third-party firewall, disable the WF as the two firewalls may conflict (for information on how to do this, see the WF section below).

If you would like to ensure that SP2 is running on your machine, right click on My Computer, select Properties, go to the General tab, and you should see Service Pack 2 listed under the System details.

[28] Finnie, p.1



Security Center

To view the SC, go to start, Settings, Control Panel, Security Center.

To obtain more information about the Firewall, Automatic Updates, or Virus Protection, click on the down arrow of each section.

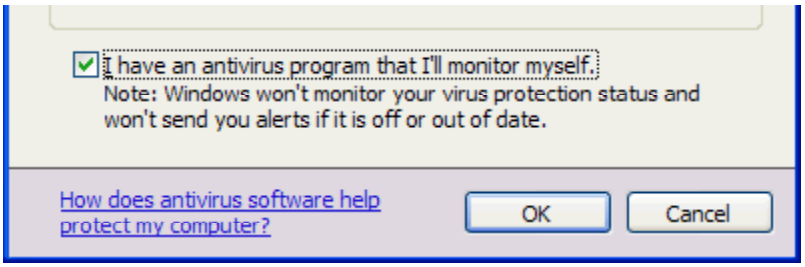
You can turn on Automatic Updates (to the Microsoft recommended guidelines) from the Security Center by clicking on “Turn on Automatic Updates”.

The Security Center checks for common firewall and anti-virus programs, however there is a chance that the Security Center may not identify the software you have installed on your system[29]. In this case, you can disable the notification to prevent the Security Center constantly notifying you to change your setup!

To disable the firewall notification, under the Security Center, click on the Firewall down arrow and click “Recommendations”. Select the “I have a firewall solution that I’ll monitor myself” check box and click “OK”.

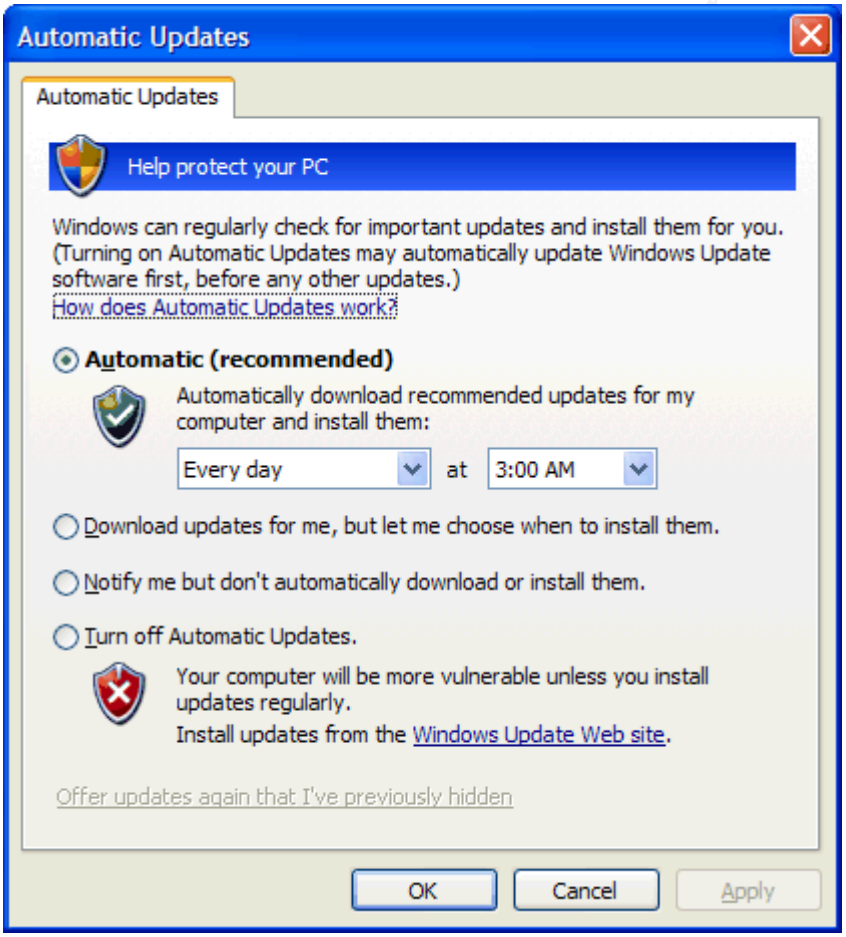
[29] Microsoft, http://www.microsoft.com/windowsxp/using/security/internet/sp2_wscintro.mspx

To disable the anti-virus notification, under the Security Center, click on the Virus Protection down arrow and click “Recommendations”. Select the “I have an antivirus program that I’ll monitor myself” check box and click “OK”.



Automatic Updates

To view Automatic Updates, go to start, Settings, Control Panel, Automatic Updates.



When configuring Automatic Updates, there are four options:

1. **Automatic (recommended)** – updates are downloaded and installed automatically at the time set. Your computer stays updated without the need for your intervention
2. **Download updates for me, but let me choose when to install them** – updates are downloaded automatically, however you choose when to proceed with the installation
3. **Notify me but don't automatically download or install them** – you are notified when updates become available. It is your responsibility to visit the Windows Update site and download and install updates
4. **Turn off Automatic Updates** – you are not notified when updates are available, therefore updates will not be downloaded and installed and you will not be aware when updates are available.

I recommend you set Automatic Updates to option 1 (as does Microsoft), have it set to check every day, and at a time when you will be online (there is no point having Automatic Updates check at a time you will not be online as you will never receive any updates).

However despite this, I would like to put forward an alternative view to the recommendation above. Option 2 may be more applicable to some users, as the installation of the update is at the discretion of the user. Some users may not want to install updates until they have been able to research the update and ensure that it will not cause damage to their system. Therefore, by setting Automatic Updates to option 2 allows users to be comfortable with the update before they choose to install. Note though that this places responsibility back on the user to remember to install the update. The Security Center does however continually notify that there are updates that have been downloaded and are ready to be installed.

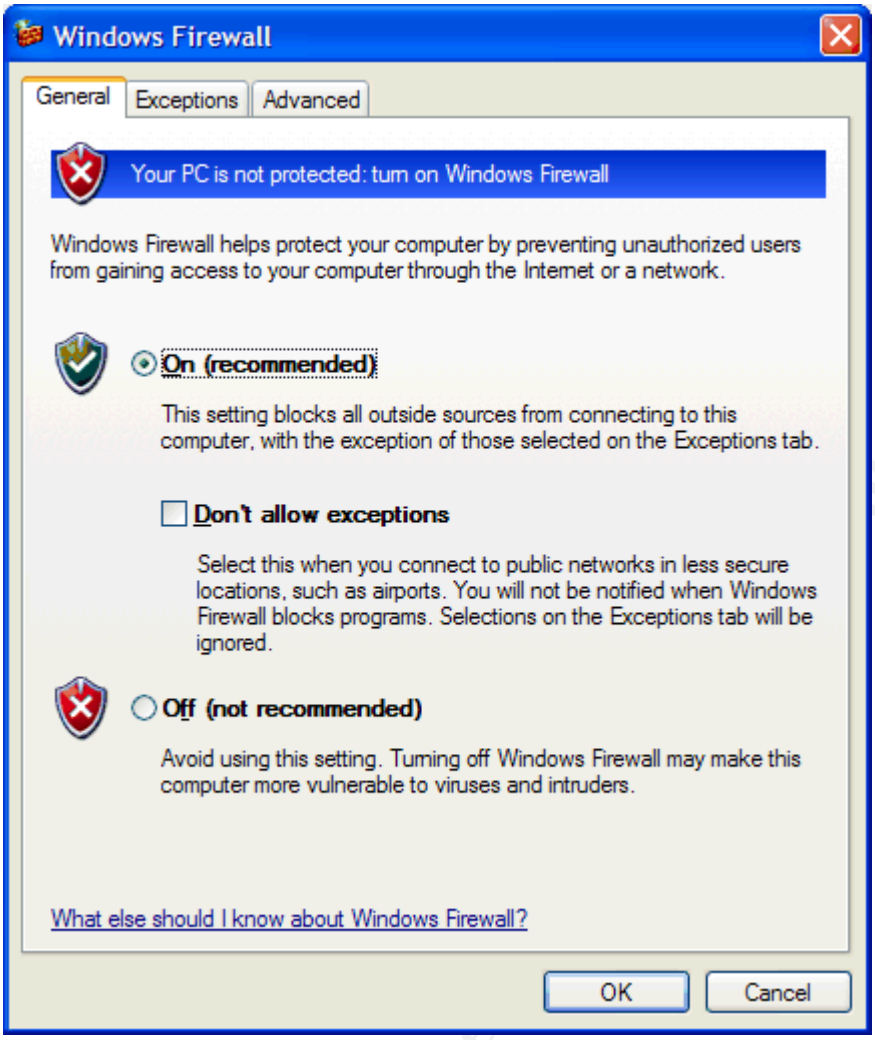
Windows Firewall

To view WF, go to start, Settings, Control Panel, Windows Firewall.

When configuring WF, there are three options:

1. **On (recommended) –** WF is turned on and blocks all outside sources connecting to your computer except for those in the exception rules
2. **On (recommended) without exceptions –** WF is turned on, however no exceptions are allowed (Microsoft recommends to set this option when accessing the internet in a public location)
3. **Off (not recommended)** – WF is turned off.

On (recommended) is set by default. I recommend that you have a third-party software firewall running on your machine (so that outbound traffic is restricted as well). If so, set option 3 so that the WF does not conflict with your third-party software firewall. If you do not have a third-party software firewall running, I recommend you set option 1 (and appropriately configure firewall rules as shown below).



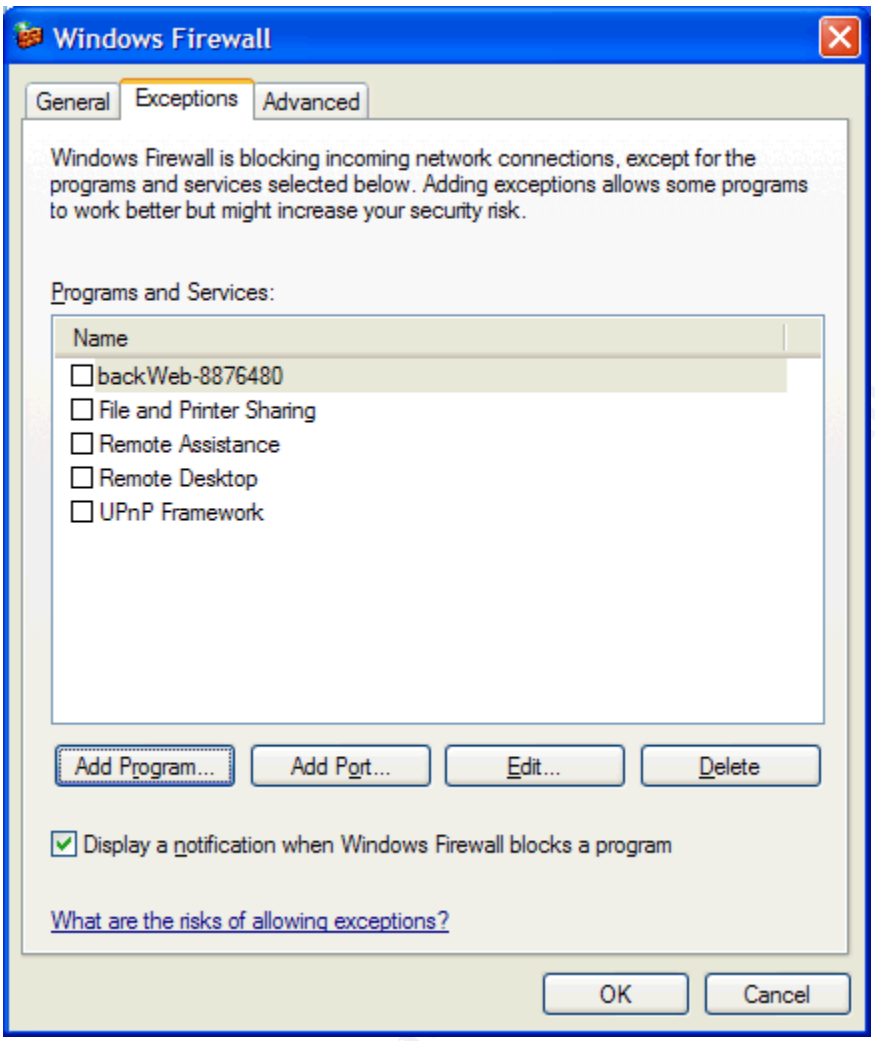
If you set the WF on, you will most likely need to configure exceptions to allow incoming network connections for certain programs (such as games). In the WF, click on the "Exceptions" tab.

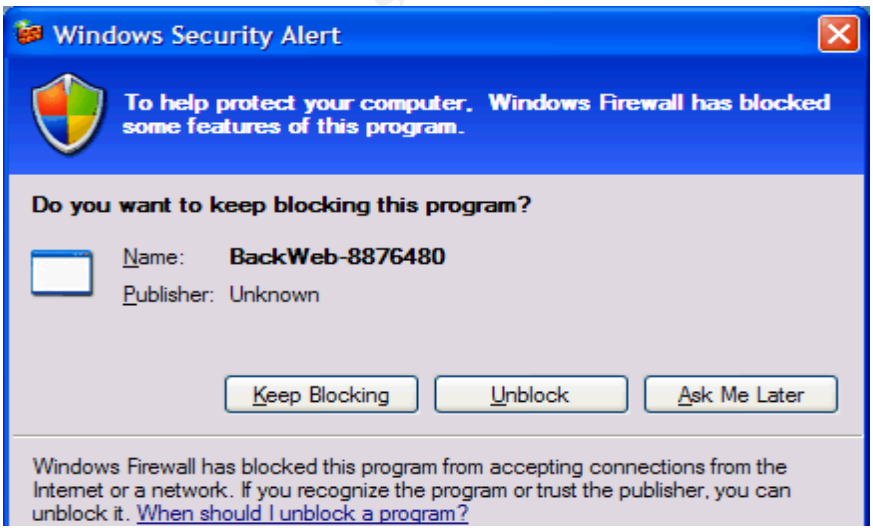
You can set exceptions in two ways:

1. **Add Program** – Allows a program to receive incoming network connections
2. **Add Port** – Allows incoming network connections to pass through a certain port number

Be careful when allowing programs or ports incoming network connections to your computer. Only allow necessary programs or ports, as creating these exceptions allows a hacker a potential opening to your computer.

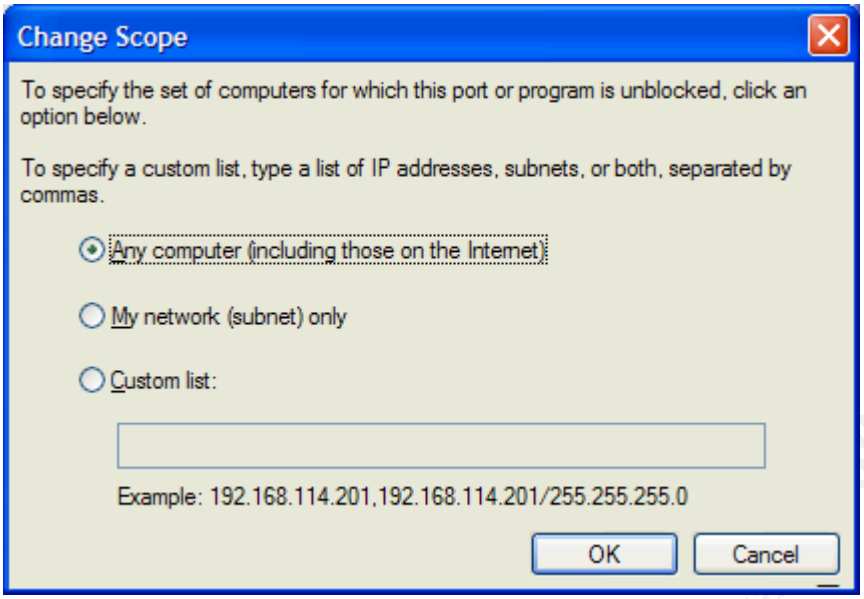
You can also set the firewall to notify you when it blocks a program. This can be useful, as you will be alerted when a program is attempting to receive an incoming network connection. This notification is set by default under the "Display a notification when Windows Firewall blocks a program".



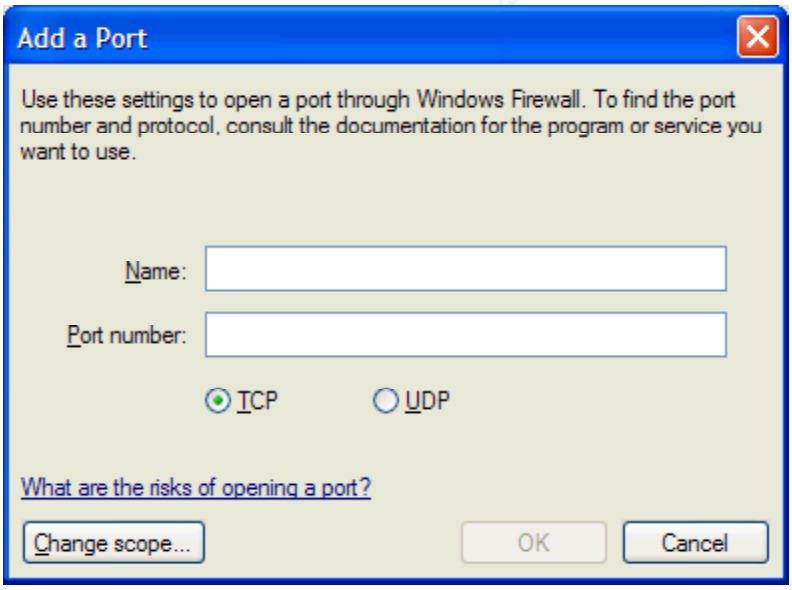


If you want to add a program to the exception list, click on “Add Program” under the “Exceptions” tab. Search through the list of programs listed (these are programs that Windows detects running on your computer) and select the program you wish to add to the exception rules. Click “OK”. If you can not find the program you are looking for, click on “Browse” to locate the program. Adding a program is useful when you do not know the port number a program uses, or it uses dynamic ports.

You can further restrict the program exception down to a specific subnet or computer that can access your machine through the program exception. Select the program exception under the “Exceptions” tab, click “Edit”, and click on “Change Scope”. If you would like to restrict access to computers on your network only select “My network (subnet) only”. If you would like to restrict access to an external subnet or individual computer, select “Custom list” and enter in the relevant subnets and IP addresses.

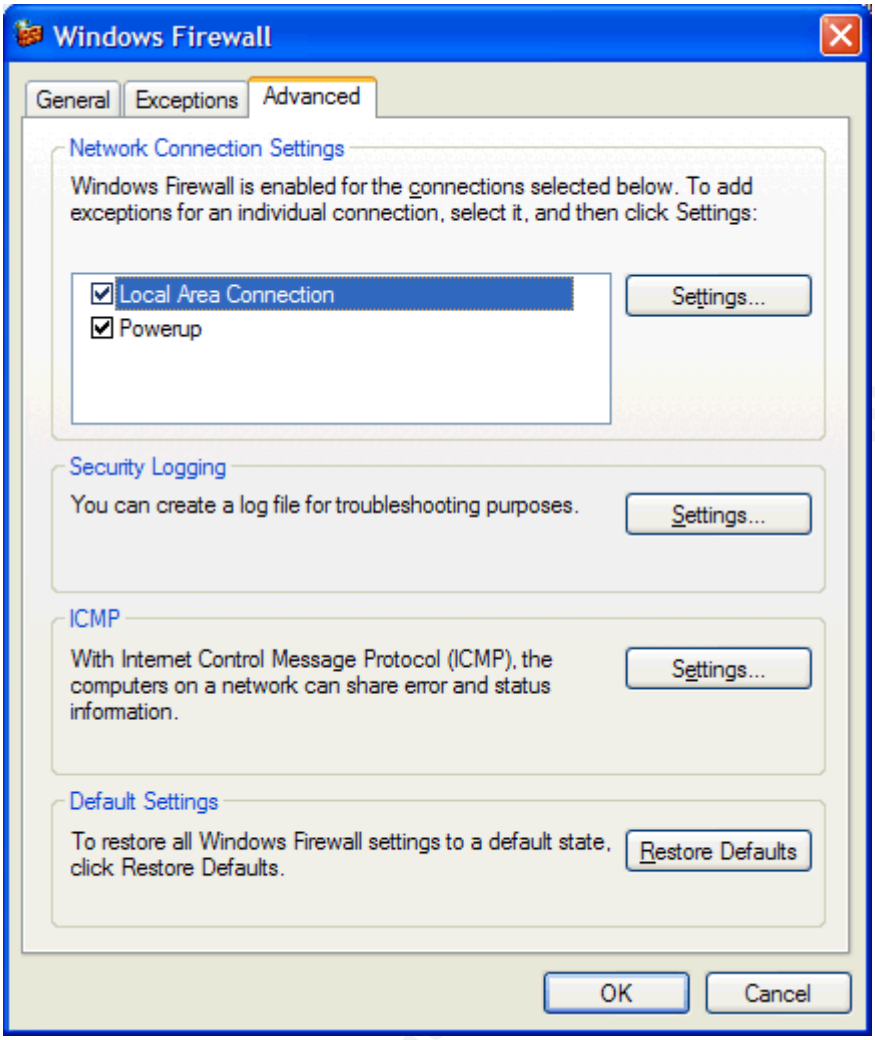


If you want to add a port, click on “Add Port” under the “Exceptions” tab. You can allow incoming network connections to access your computer through both TCP and UPD port numbers. To open a certain port, type in a name you would like to call the exception in the “Name” field (eg. Microsoft Messenger), enter the port number in the “Port number” field (eg. 1863) and select the IP transport protocol (ie. TCP or UDP). Note that unless you are confident in your knowledge of port numbers and the services that run on each, I would recommend against opening up ports as malicious users (not just the specific program traffic) can access your computer through an open port.



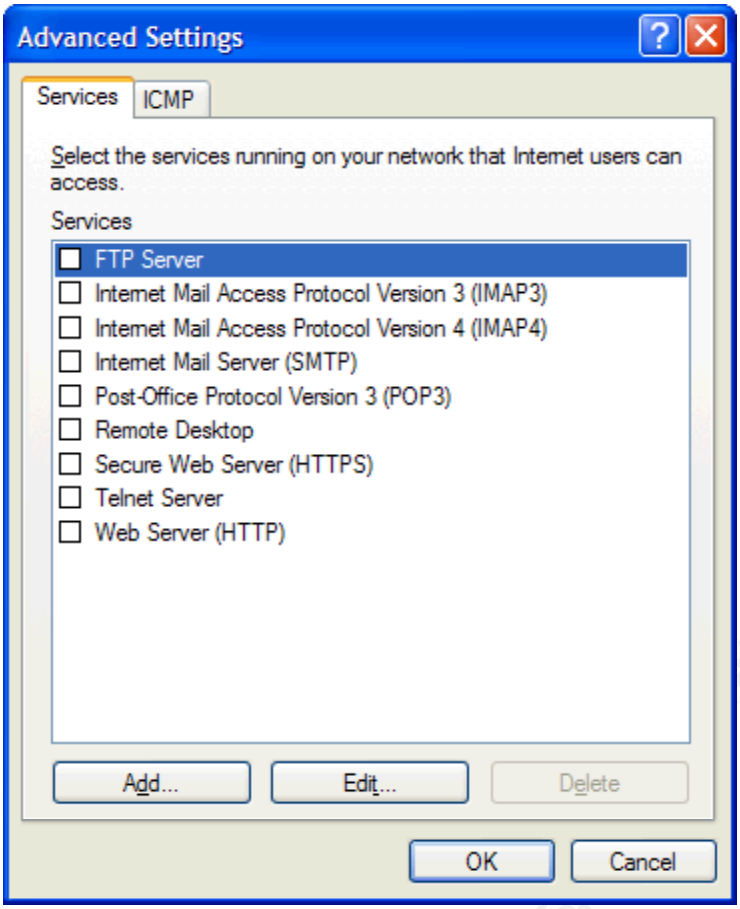
You can further restrict the port number exception down to a specific subnet or computer that can access your machine through the port exception (as previously discussed). Select the port exception under the “Exceptions” tab, click “Edit”, click on

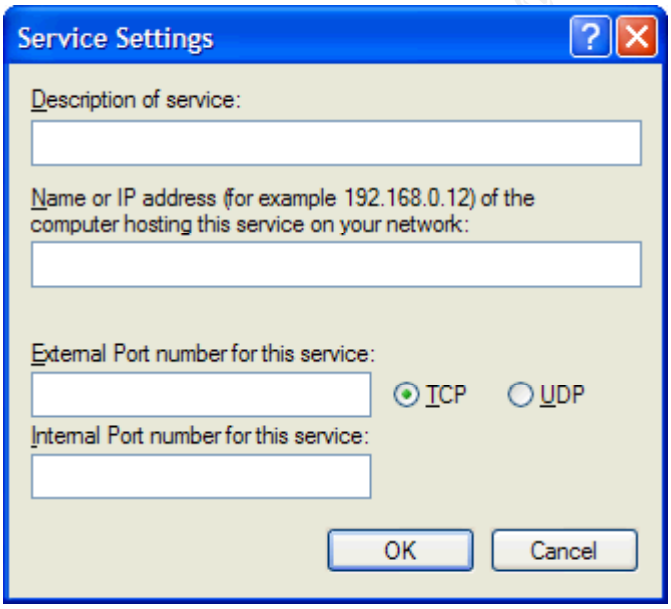
“Change scope” and follow the instructions above.



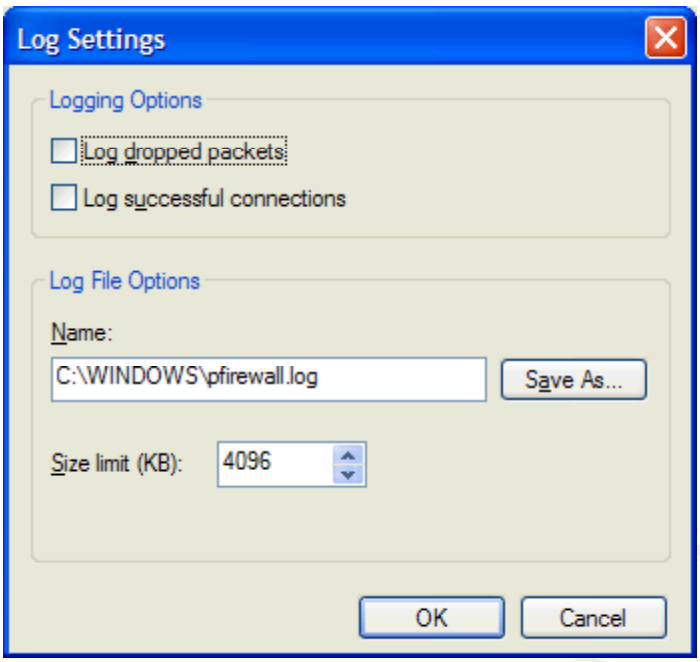
You can apply different sets of exception rules to different connections (eg. LAN and broadband). To set firewall exceptions for a specific connection, click on the “Advanced” tab, select the connection, and click “Settings” under the Network Connection Settings section.

If the service you want to exclude for a connection is already listed, place a tick in the box beside the service. Otherwise, to select the service that will be excluded click on “Add”. Enter in the name of the service under “Description of service”, name or IP address of the computer hosting the service under “Name or IP address of the computer hosting this service on your network”, input the external and internal port number under “External port number of this service” and “Internal port number for this service”, and select the IP transport protocol (ie. TCP or UDP).





If you want to keep a log of network traffic, WF allows you to log dropped packets and successful connections. Under the “Advanced” tab, click on “Settings” in the “Security Logging” section. You can select if you want to log dropped packets and/or successful connections, where the log will be saved, and the size limit.



Internet Explorer

To open IE, go to start, Programs, Internet Explorer. To view IE security settings, go Tools, Internet Options.

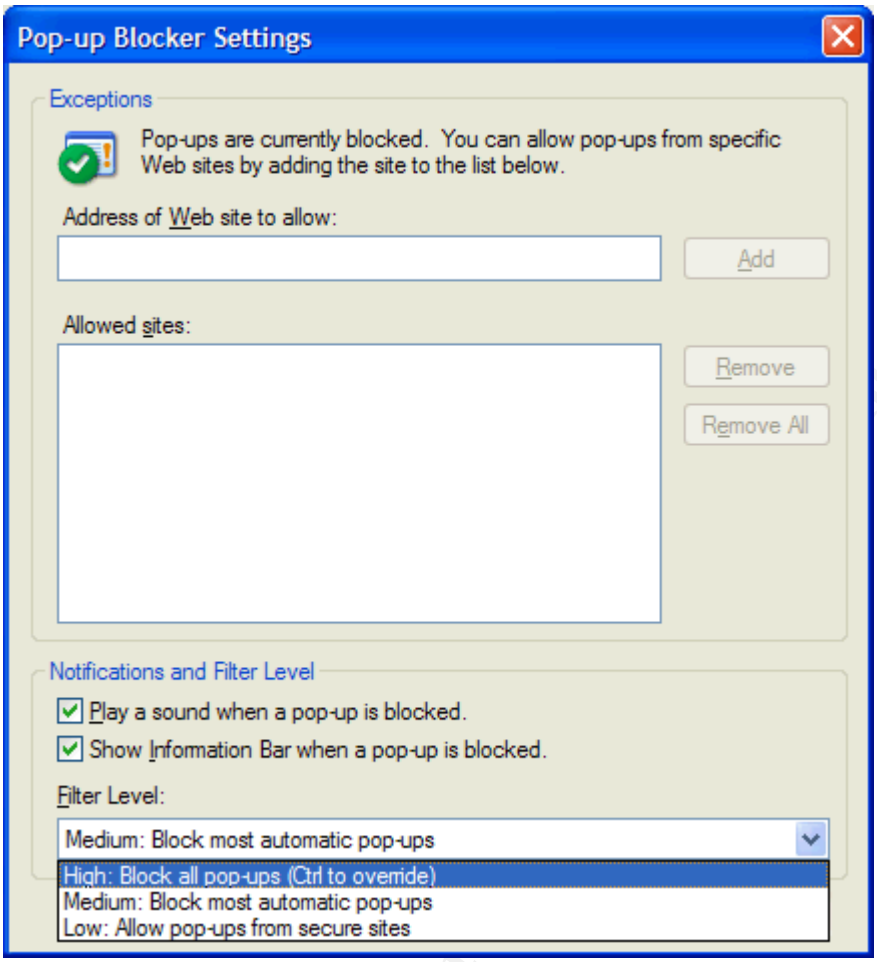
To set the Pop-up Blocker, select the “Privacy” tab under Internet Options. The Pop-up Blocker is turned on by default. I recommend you keep the Pop-up Blocker turned on. If you need to turn the Pop-up Blocker on/off, tick the “Block pop-ups” option under the Pop-up Blocker section.

There are a number of settings in the Pop-up Blocker that allow you to have more control over pop-ups rather than just a straight block. To view these settings, click on “Settings” in the Pop-up Blocker section.

If you want to allow pop-ups from a specific site (hopefully a secure site), you can add the URL to an exception list. To do this, type in the URL in the “Address of Web site to allow” area and click “Add”.

The Information Bar is a useful feature that allows you to temporarily allow pop-ups from the site you are visiting, or always allow pop-ups from the site you are visiting. I recommend you have the Information Bar enabled. The Information Bar is set by default under the "Notifications and Filter Level" section under the Pop-up Blocker settings. If you need to turn the Information Bar on/off, tick the "Show Information Bar when a pop-up is blocked".

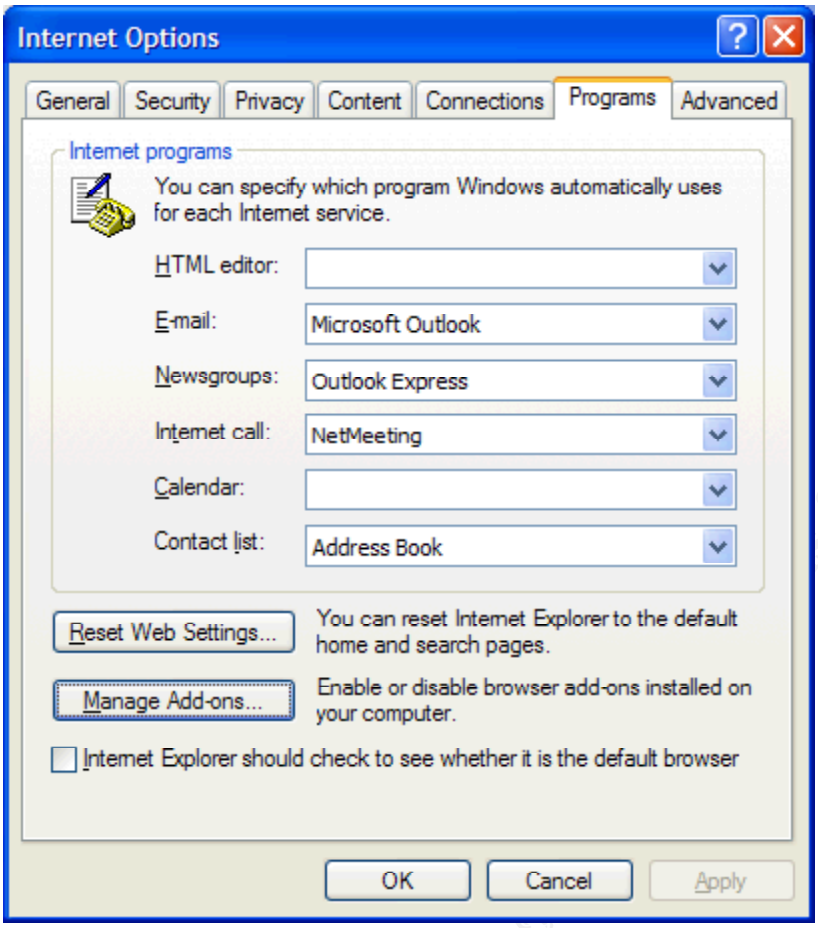
If you visit a web site that attempts to launch a pop-up, the Pop-up Blocker will block the pop-up and just underneath the address bar, the Information Bar will notify you a pop-up has been blocked, with a bar that says "Pop-up blocked. To see the pop-up or additional options click here". If you want to view the pop-up or allow pop-ups on this site, click on the Information Bar and select the appropriate option.



You can also select what filter level the Pop-up Blocker operates at. There are three options:

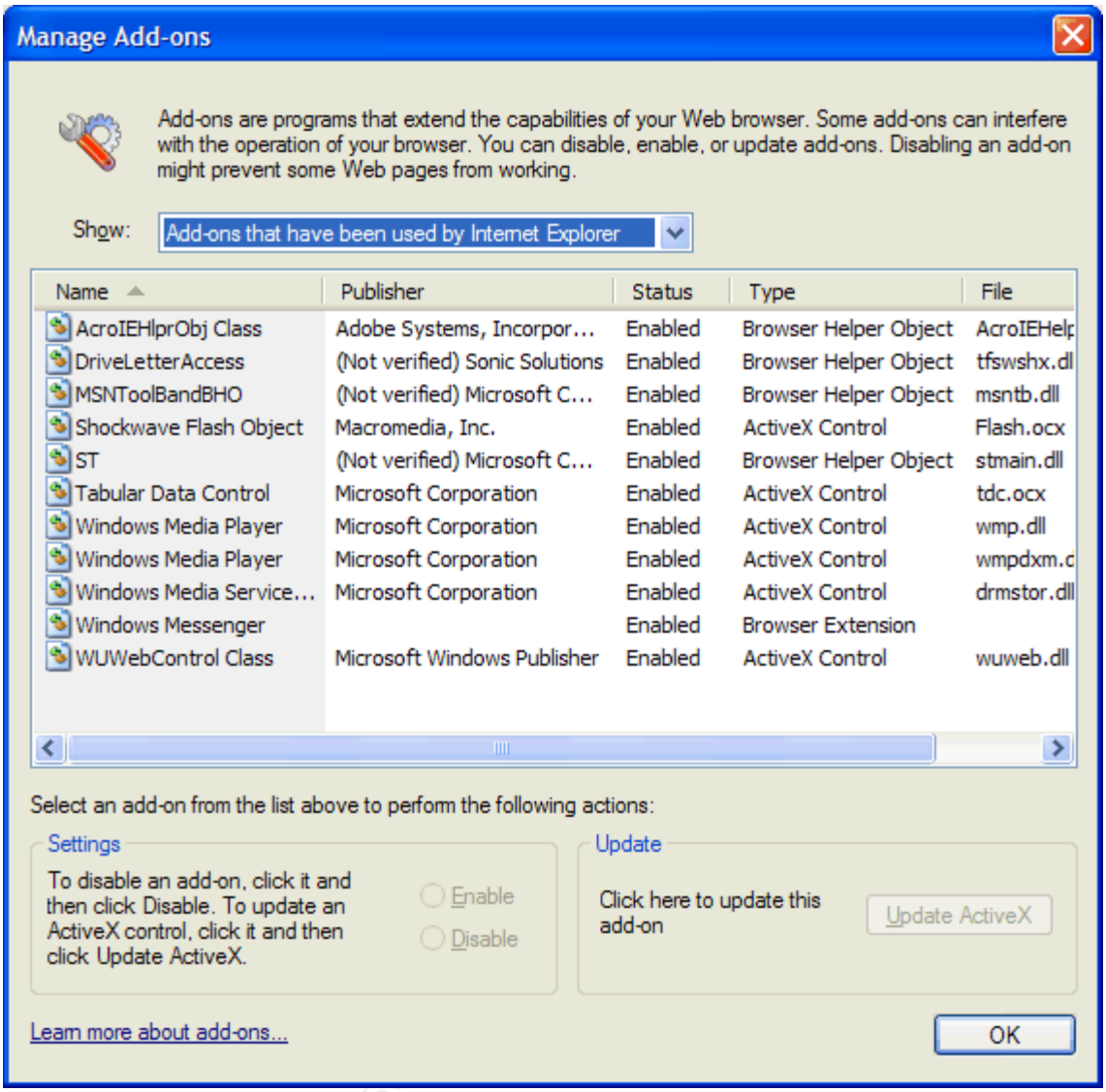
1. **High: Block all pop-ups (Ctrl to override)** – all pop-ups are blocked. If you want to launch a pop-up, you have to hold down the Ctrl key
2. **Medium: Block most automatic pop-ups** – most pop-ups are blocked, except for pop-ups that you have clicked a link to launch, such as confirmation details. This option is set by default
3. **Low: Allow pop-ups from secure sites** – only pop-ups from secure sites are launched.

I recommend keeping the filter level set to option 2, as option 1 would be impractical, and option 3 may still allow unnecessary pop-ups.



As most users would have been using IE for a number of years, users may have a number of add-ons installed (some of which may be harmful to your computer). The Add-on Manager allows you to view the add-ons installed on your computer and to remove any suspicious add-ons. To set the Add-on Manager, click the “Programs” tab under Internet Options, and click on “Manage Add-ons”.

In the Show section, select “Add-ons that have been used by Internet Explorer” so you can see all add-ons installed on your machine. Review the list and if there are any add-ons you want to disable, select the add-on, and in the Settings section select “Disable”.

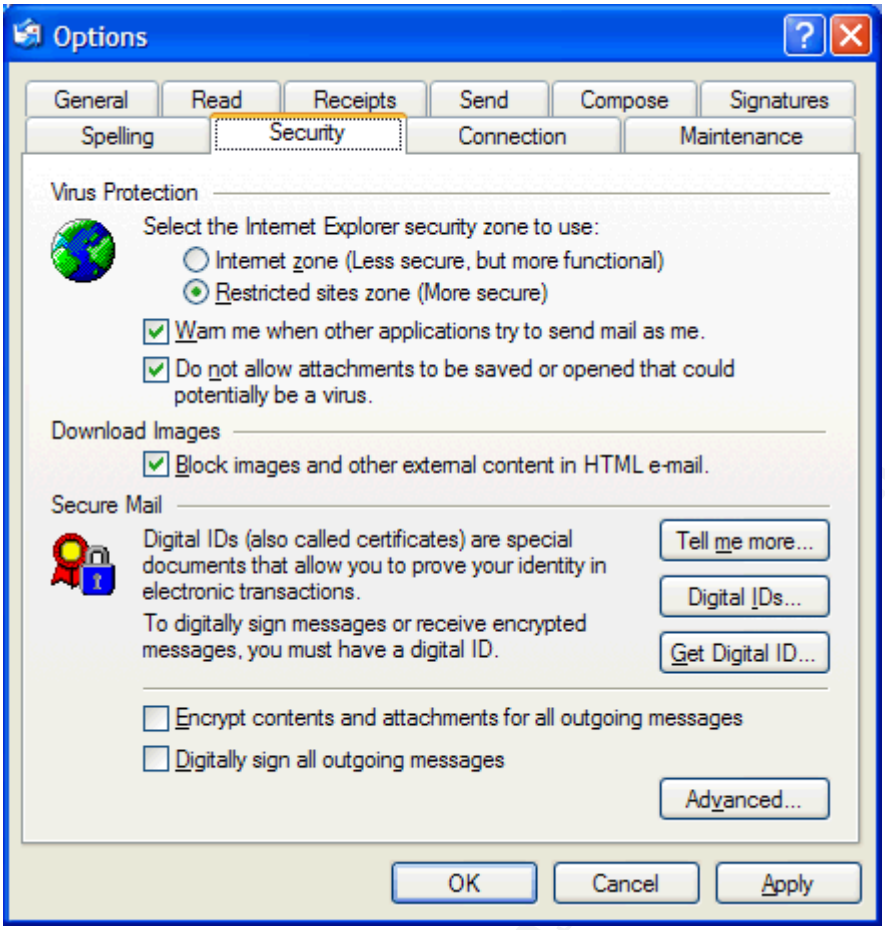


Outlook Express

To open OE, go to start, Programs, Outlook Express. To view OE security settings, go Tools, Options.

To set the graphics blocker, click the “Security” tab. The graphics blocker is set by default. If you need to turn the graphics blocker on/off, tick “Block images and other external content in HTML e-mail” under the “Download Images” section.

If you have had problems with OE blocking legitimate attachments in the past, this has now been addressed through Attachment Manager. To ensure dangerous attachments can not be saved or opened, tick “Do not allow attachments to be saved or opened that could potentially be a virus” under the “Virus Protection” section.



You now have completed the secure configuration of SP2. Safe surfing!

Conclusion

SP2, despite the well-documented installation problems, is a useful update that can help improve computer security. Microsoft has had a solid attempt at improving security within Windows XP, and in today's networked environment, SP2 is an extra layer of security that can help protect sensitive data. Despite their current set up, all users should seriously consider installing SP2. It may not be hacker proof, but it does help plug the security holes of Windows XP SP1.

References

Australian IT. “XP service pack hits 100m.” Australian IT Newspaper. Oct. 21 2004. 29 Dec. 2004 <http://australianit.news.com.au/articles/0%2C7204%2C11137838^15321^^nbv^15306%2C00.html>

Finnie, S. “Windows XP Service Pack 2: Is It Time Yet?” Information Week. Oct. 19 2004. 29 Dec. 2004. <http://informationweek.com/story/showArticle.jhtml?articleID=50500860&pgno=2>

Internet Storm Center. 29 Dec 2004. <http://isc.sans.org/xpsp2.php>

Keizer, G. “Windows XP Service Pack 2: The 10% Problem.” Information Week. Aug. 31 2004. 29 Dec 2004 <http://www.informationweek.com/story/showArticle.jhtml;jsessionid=PGBNQG4NK3P2QQSNDBCSKHSCJUMEKJVN?articleID=46200368>

Microsoft. 29 Dec 2004 <http://www.microsoft.com/windowsxp/sp2/technologiesoverview.mspx>

Microsoft. 29 Dec 2004 <http://www.microsoft.com/windowsxp/sp2/overview.mspx>

Microsoft. 29 Dec 2004 <http://www.microsoft.com/athome/security/protect/windowsxp/choose.aspx>

Microsoft. 29 Dec 2004 <http://www.microsoft.com/windowsxp/using/security/internet/sp2_wscintro.mspx>

PC Authority. “XP Service Pack 2 Install Guide.” PC Authority. Oct. 2004: 8-124.

PC User. “Stay safe without SP2.” PC User. Oct. 2004: 83-84.

Rash, W. “Windows XP SP2: A bandage but not a panacea.” IT Manager’s Journal. Nov. 12 2004. 29 Dec. 2004 <http://productguide.itmanagersjournal.com/article.pl?sid=04/11/13/1331243>

Spanbauer, S. “Is XP’s Fix Safe?” PC World. Nov. 2004. 29 Dec. 2004 <http://www.pcworld.com/news/article/0,aid,117990,00.asp>

Thurott’s, Paul. 29 Dec 2004 <http://winsupersite.com/reviews/windowsxp_sp2.asp>