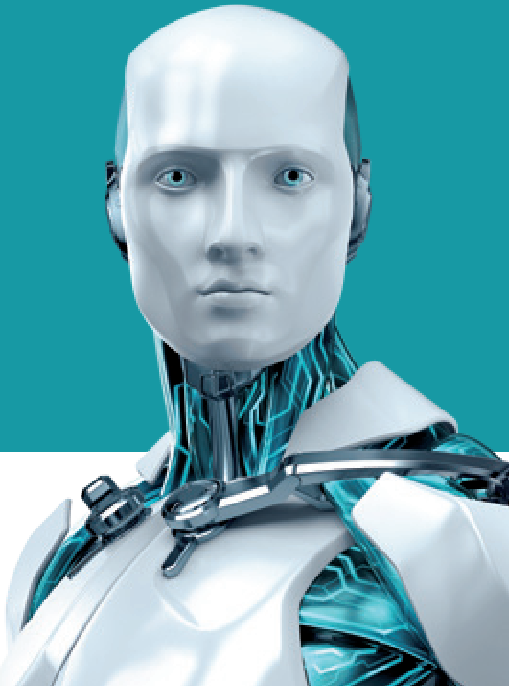
WINDOWS XP SECURITY

Author:
Aryeh Goretsky, MVP, ZCSE
Distinguished Researcher, ESET



ENJOY SAFER TECHNOLOGY™

CONTENTS

NOTE:

The goal of this white paper is to explain how to set up Microsoft Windows XP for use past Microsoft's April 8, 2014 End of Life (EOL) date, until such time that it can be replaced by a newer, more secure operating system.

This white paper explains how to make a new installation of Windows XP more secure, but such advice should not be construed as guidance on how to make it as secure as newer versions of Windows. There is no way to do this other than to install a newer version of Windows.

No third-party security software, no matter how effective, can take the place of regular security updates provided by a vendor for its operating systems and applications. The goal of this paper is to explain how to keep Windows XP as secure as possible <u>until it can be replaced</u>.

INTRODUCTION

Microsoft Windows XP is perhaps Microsoft's most-storied operating system. Released in 2001, just a year after the release of Microsoft Windows 2000, it was meant to fix Microsoft's cycle of releasing separate operating systems for consumers—based on Windows 95— and operating systems for enterprises—based on Windows NT—with a single unified operating system for use by everyone. Combining the reliability of the Windows NT kernel with the multimedia subsystem of Windows 9x, it would be equally usable whether at work or at play.

Figure 1: Windows XP booting up

So, how well did Microsoft execute on this vision from so long ago? In April 2014, Windows XP was installed on about 30% of our customers' desktop computers. As of March 2018, Windows XP accounts is installed on about 5,5% of those systems. While this may seem like a small percentage, it is 10 times the number of computers running Windows XP's successor, Windows Vista, which today accounts for a mere sub-1% of usage.

A Very Brief History of Windows XP Security

Given Windows XP's widespread adoption, it may be difficult to remember that it originally got off to a rocky start: when it first came out, there were many complaints about it, ranging from criticisms of its performance, to lack of hardware support, to complaints about the relative lack of new features compared to Windows 2000, to its cost ($200 and up in the United States, depending upon the edition). Yet, despite all these issues, Windows XP has gone on to enjoy a longevity on the desktop not seen since the days of Atari and Commodore, when ROM-based operating systems s were used, unaltered, for over a decade.

When Windows XP was introduced in 2001, it was billed by Microsoft as their most secure operating system ever. While that was true at the time, in the intervening years it had become Microsoft's most-patched operating system a consequence not only of its popularity, but of its longevity as well, in the attempt to maintain its original level of security. Microsoft's response to the deluge of vulnerabilities found in their flagship desktop operating system was two-fold, developing its Trustworthy Computing[1,2] (TwC) initiative to ensure safe computing, backed up by implementing a Security

[1] Charney, Scott. "Looking Forward: Trustworthy Computing." Microsoft Corp. https://cloudblogs.microsoft.com/microsoftsecure/2014/09/22/looking-forward-trustworthy-computing/.

[2] Microsoft. "10 Years of Trustworthy Computing." Microsoft Corp. http://www.microsoft.com/en-us/twc/twcnext/timeline.aspx.

Development Cycle[3] (SDL) to enforce the creation of secure code by its developers.

Efforts such as Microsoft's TwC, though, need to be followed up not merely *with* rapid responses to emerging threats, but with *correct* responses, and during the first few years it seemed the changes made by Microsoft were slow or incomplete. Two well-known examples:

- *Microsoft shipped Windows XP with a feature called AutoPlay[4, 5], which allowed the operating system to immediately identify when removable media, such as a CD-ROM, was inserted into the computer. This was coupled with a related feature called AutoRun[6], designed to begin running programs from the newly-available disk. Originally intended to allow a computer to automatically start running programs such as multimedia applications and games from CD-ROM, the feature never received much use by software developers. Or, at least, from legitimate developers: as the price of USB flash drives[7] went down, and availability skyrocketed, malware authors began making use of this technology to help spread their creations, such as the infamous Conficker worm[8, 9, 10]. Unfortunately, for all its misuse, Microsoft considered this to be a legitimate feature of the operating system and refused to change it until eight years later, in 2009[11, 12, 13] when they changed the functionality to disable this harmful behavior. And even then, they published wrong instructions the first time[14].*
- *In Service Pack 2, released in 2004, Microsoft changed the way in which TCP/IP Raw Sockets, which are a type of network communication, were handled[15, 16, 17]. This was done in response to widespread attacks from worms that generated so much network traffic that they degraded connectivity across the Internet as a whole, not to mention disrupting the networks of many of Microsoft's largest customers. The change, unfortunately, degraded the performance of peer-to-peer and network management applications that ran on Windows XP, which led some users to modify Windows networking*

[3] Microsoft. "Microsoft Security Development Lifecycle." Microsoft Corp. https://www.microsoft.com/security/sdl/default.aspx.

[4] Wikipedia. "AutoPlay." Wikimedia Foundation. https://en.wikipedia.org/wiki/AutoPlay.

[5] St-Michel, Stephane and Aust, Brian. "Autoplay in Windows XP: Automatically Detect and React to New Devices on a System." MSDN Magazine. http://msdn.microsoft.com/en-us/magazine/cc301341.aspx.

[6] Wikipedia, "AutoRun." Wikimedia Foundation. https://en.wikipedia.org/wiki/AutoPlay.

[7] Cobb, Stephen. "Are your USB flash drives an infectious malware delivery system?" WeLiveSecurity. http://www.welivesecurity.com/2012/12/11/are-your-usb-flash-drives-an-infectious-malware-delivery-system/.

[8] ESET. "Virus Radar Threat Encyclopedia - Win32/Conficker." http://www.virusradar.com/en/Win32_Conficker/detail.

[9] Goretsky. Aryeh. "1000 days of Conficker." WeLiveSecurity. http://www.welivesecurity.com/2011/08/17/1000-days-of-conficker/.

[10] Abrams, Randy. "Foil Conficker Get Rid of AutoRun." WeLiveSecurity. http://www.welivesecurity.com/2009/03/25/foil-conficker-get-rid-of-autorun/.

[11] Abrams, Randy. "Now You Can Fix AutoRun." WeLiveSecurity. http://www.welivesecurity.com/2009/08/25/now-you-can-fix-autorun/.

[12] Microsoft. "Microsoft Security Advisory (967940): Update for Windows Autorun." Microsoft Corp. http://technet.microsoft.com/en-us/security/advisory/967940.

[13] Microsoft. "How to disable the Autorun functionality in Windows." Microsoft Corp. http://support.microsoft.com/kb/967715/en-us.

[14] US-CERT. "Alert TA-09-020A: Microsoft Windows Does Not Disable AutoRun Properly." https://www.us-cert.gov/ncas/alerts/TA09-020A.

[15] Microsoft. "Microsoft Security Bulletin MS05-019 - Critical - Vulnerabilities in TCP/IP Could Allow Remove Code Execution and Denial of Service." Microsoft Corp. http://technet.microsoft.com/en-us/security/bulletin/ms05-019.

[16] Howard, Michael. "A little more info on raw sockets and Windows XP SP2." Microsoft Corp. http://blogs.msdn.com/b/michael_howard/archive/2004/08/12/213611.aspx.

[17] Windows Dev Center-Desktop. "TCP/IP Raw Sockets." Microsoft Corp. http://msdn.microsoft.com/en-us/library/windows/desktop/ms740548.

> *components in order to bypass the restrictions, a technique malware authors quickly adopted. It wasn't until four years later, in 2008, that Microsoft reversed these changes.*

While these actions by Microsoft did improve Windows XP's security posture, the operating system continued to be attacked, and it was arguably not until Windows Vista was released in 2007 that Microsoft was able to use the expertise gained from its TwC initiative and SDL lifecycle, along with over half-a-decade's worth of data on attack patterns, to implement major changes to the security of the Windows kernel. This work was further refined in 2009 with the release of Windows 7, and again in 2012 with the release of Windows 8.

The purpose of this paper is to explain the various methods by which users of Windows XP can bolster its security. However, the best method is simply to upgrade to a newer and more secure version of Windows[18]. While the measures outlined in the paper can improve Windows XP's security, they cannot fix underlying vulnerabilities in its code. April 8, 2014, the date on which Microsoft stopped creating new patches and hot-fixes for Windows XP to address security issues, is long-since past. While it is true that Microsoft has released ***two updates*** due to severe vulnerabilities which may have been exploited by nation states, such updates are not a normal practice and Windows XP's remaining users would be well-advised to upgrade.

If you are reading this paper, though, it is a good bet that you are not yet ready to say goodbye to Windows XP[19, 20]. It is still used somewhere in your computing environment, and continues to be used past the end of its extended support cycle from Microsoft. You may not have dedicated IT staff to help you secure those systems. With that in mind, let's look at some of the reasons you might be continuing to use Windows XP past its end of support date before we move on to how to secure it.

NOTE: For purposes of ease of use and brevity, we are going use the term Windows XP to refer to all of the editions of Microsoft *Windows XP* that were widely available to consumers and businesses:

Edition	Description
Windows XP Home Edition	*Version for home users, with limited management features*
Windows XP Media Center Edition	*Version for Home Theater PCs with TV tuners and DVD drives*
Windows XP Professional Edition	*Version for businesses, with manageability features.*
Windows XP Starter Edition	*Version for emerging markets on low-end hardware*
Windows XP Tablet PC Edition	*Version for notebooks with touch screens and digitizing styli*

Windows XP for Embedded Systems and *Windows XP Embedded* were special componentized builds of Windows XP available only to enterprises and device manufacturers, and should not be considered to be covered in this article unless specifically mentioned. Likewise, 64-bit editions of Windows XP, such as *Windows XP 64-Bit Edition for Intel® Itanium Processors* and *Windows XP Professional x64 Edition*, which are derived from *Microsoft Windows Server 2003*, are not meant to be considered when discussing Windows XP unless specifically mentioned.

[18] Goretsky, Aryeh. "Time to Move On From Windows XP." WeLiveSecurity. *http://www.welivesecurity.com/2014/03/25/time-to-move-on-from-windows-xp/*.

[19] Goretsky, Aryeh. "Goodbye, Windows XP!" WeLiveSecurity. *https://www.welivesecurity.com/2014/04/08/goodbye-windows-xp/*.

[20] Kubovič, Andrej. "Windows XP: The zombie OS 'lives' on." WeLiveSecurity. *https://www.welivesecurity.com/2016/04/08/windows-xp-zombie-os-lives/*.

WHY USE XP AFTER 2014?

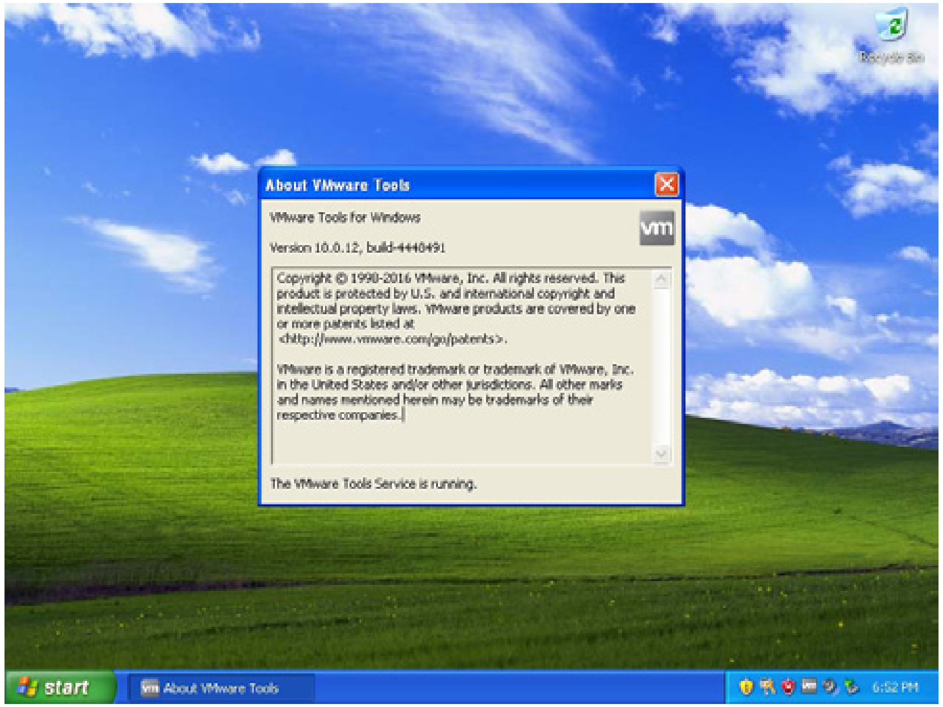
There are several reasons one might continue using Microsoft Windows XP long after its inception. Below is a list of three broad reasons why a business might still be using Windows XP today:

Description	Reason
Software	The computer is used to run (a) key application(s) that only works under Microsoft Windows XP. Upgrading is impractical because the developer may no longer be in business, the price of the upgrade may be cost-prohibitive, or the application may need to be replaced in its entirety by (a) brand new application(s).
Hardware	The computer is used to operate a piece of hardware that works only with Microsoft Windows XP. In some cases, industrial, medical or scientific equipment may use a PC running Windows XP as a kind of embedded controller, and the cost of upgrading the system to support newer versions of Microsoft Windows or replacing it may be cost-prohibitive or infeasible due to resource issues.
Familiarity	The computer is used to perform a specific set of functions, which employees are trained on, familiar with and comfortable using. While the computers and software it runs are capable of running newer versions of Microsoft Windows, upgrading to a newer version of Microsoft Windows incurs additional training costs and decreased productivity until employees come up to speed with the new operating system and application software.

While these three cases are different, they ultimately have the same underlying reason: *Cost*. While the examples above have concentrated on the financial impact for a business to upgrade to a newer operating system, these reasons are just as applicable to consumers as well. Familiarity may be even more of an issue for them, especially given the tendency to anthropomorphize computers.

WINDOWS XP, VIRTUALLY

If you need to continue to run Microsoft Windows XP, one possible solution might be for you to run it using virtual machine[21] software. As the name implies, a virtual machine (VM) is a program that emulates an entire computer in software. The emulation is so good that it can run another operating system inside of it, and that operating system and its programs will "see" the virtual machine as if they were running on a regular



About VMware Tools

VMware Tools for Windows

Version 10.0.12, build-4448491

Copyright © 1998-2016 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

The VMware Tools Service is running.

Figure 2: Windows XP running inside of a virtual machine

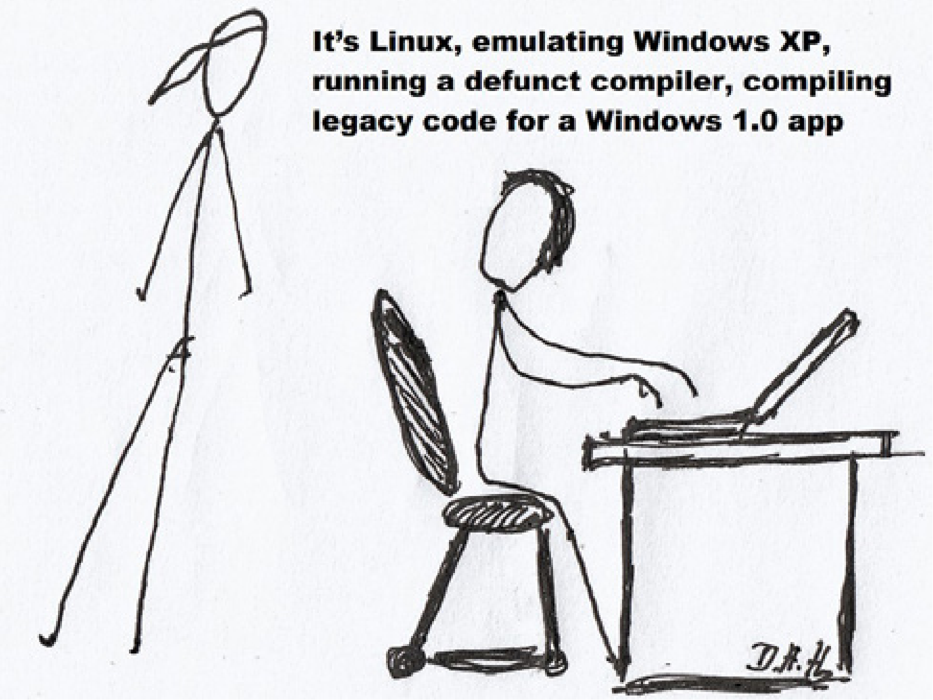
[21] Wikipedia. "Virtual Machine." Wikimedia Foundation. *https://en.wikipedia.org/wiki/Virtual_machine*.

computer. Using virtual machine technology, a computer running a more modern operating system such as Windows 7, Windows 8.1 or Windows 10, can run older versions of Windows or even entirely different operating systems, such as Linux and BSD.

Virtual machine software comes in many forms, ranging from Open Source programs such as Oracle VirtualBox[22] to commercial offerings like VMware Workstation[23]. The business-focused editions of Windows 7 (Professional, Ultimate and Enterprise) even came with a virtual machine specifically for running Windows XP called Windows XP Mode[24, 25, 26]. Windows XP Mode is not available for Windows Vista or Windows 8.

Using a virtual machine may allow you to run only that last remaining application requiring Microsoft Windows XP, at least until it can be replaced. It is important to keep in mind that while running Windows XP inside of a virtual machine may *reduce* its attack surface, any underlying vulnerabilities facing Windows XP remain. It does, however, make the computer itself easier to manage, which can be important if relying on older hardware for which parts may be difficult to obtain. Also, running Windows XP inside a virtual machine on modern hardware may allow you to bypass compatibility issues with modern hard disk drives and solid-state drives, which will be discussed in further detail later in this white paper.

If there is any question about whether or not to use a virtual machine to keep running Microsoft Windows XP, that question should only be "*Can I?*" If you *can*, you **should** do so in order to get away from the costs associated with continuing to maintaining whatever old hardware is needed to run Windows XP. It may be, though, that your usage of Windows XP relies on some software or hardware that does not work successfully inside of a virtual machine. If that's the case, you will need to maintain the "native" hardware, an issue about which we will go into greater detail below.


It's Linux, emulating Windows XP, running a defunct compiler, compiling legacy code for a Windows 1.0 app
D.A.H.

[22] Oracle. "VirtualBox." Oracle. https://www.virtualbox.org/.

[23] VMware. "VMware Workstation." VMware, Inc. http://www.vmware.com/products/workstation/.

[24] Microsoft. "Windows XP Mode." Microsoft Corp. http://windows.microsoft.com/en-us/windows7/products/features/windows-xp-mode.

[25] Microsoft. "Install and use Windows XP Mode in Windows 7." Microsoft Corp. http://windows.microsoft.com/en-us/windows7/install-and-use-windows-xp-mode-in-windows-7.

[26] Microsoft. "Microsoft Download Center – Windows XP Mode." Microsoft Corp. http://www.microsoft.com/en-us/download/details.aspx?id=8002.

A NOTE ABOUT PIRACY

A related—and recurring—issue we came across during research into the reluctance of consumers to let go of Microsoft Windows XP was software piracy: A significant minority of people spoken with while researching this paper are running a pirated copy of the operating system, and sometimes pirated applications as well. In some cases, the computer originally came with a licensed version of Windows XP, but had been replaced at some point with a pirated copy during a hardware upgrade, or as a result of a disk crash, or due to a desire to avoid the bloatware installed by the computer manufacturer, or because of some other misadventure. Not only has this left them unable to upgrade legally to a newer operating system using inexpensive upgrade editions; it also means they often avoid installing security patches and updates, fearful that one of them will disable their pirated copies of Windows.

This paranoia was not helped by Microsoft's release of Windows Genuine Advantage[27] (WGA). WGA is a digital rights management (DRM) tool designed to block pirated copies of Windows from receiving non-critical updates, to disable the personalization features in the operating system, such as the ability to customize the wallpaper, and to display messages warning the user the operating system may be unlicensed. That Microsoft released WGA through the auspices of the Windows Update service, claiming it to be a critical security update, left many people with pirated copies of Windows operating systems hostile towards Microsoft as, in fact, it fixed no vulnerabilities in the operating system and collected information that could be used to identify computers running it uniquely. Many people were alienated by Microsoft's initial refusal to give any details about what the program did.

Regardless of their reasons for pirating Microsoft Windows XP, many users have responded to Microsoft's stance on software piracy by disabling Windows Update for fears of having their pirated copies deactivated or being spied upon by Microsoft. These computers, which are often missing years of patches, are far more vulnerable to exploitation than their legal and updated counterparts.

If any of the computers running Microsoft Windows XP for which you are responsible are in this situation, now would be a good time to get them out of that state. If you cannot install a newer version of Windows, then install the legally licensed version of Windows XP that came with the computer, using the correct recovery media for the computer combined with the product ID key on the Certificate of Authenticity label on the side or bottom of the unit.

If the hardware you are using did not come with a legal license for Windows XP, your next best option is to use a retail license for Microsoft Windows XP Professional from an unopened copy of the software still in its shrink-wrap, which can sometimes be found on online auction sites and at thrift stores. This will allow you to run the operating system on whatever hardware, virtual or physical, has been selected until the operating system can be replaced by a more modern and secure version.

[27] Microsoft. "Description of the Windows Genuine Advantage Notifications application." Microsoft Corp. https://windows.microsoft.com/en-US/windows/help/genuine/faq.

BACKUP STRATEGIES FOR WINDOWS XP

Regardless of the reasons for continuing to use Windows XP past its well-publicized expiration date[28, 29, 30], the most important thing for users of Windows XP to do is ensure their computers will continue to work reliably despite the long-expired April 8, 2014 deadline.

If your usage of Windows XP is routine, there is probably nothing additional you need to do with your installation, other than to download the final set of Windows Updates from Microsoft. Of course, other programs you run under the operating system may continue to receive updates as well, and those updates should be installed to keep those applications safe and secure from vulnerabilities that could lead to their exploitation. In particular, it would be a good idea to check for updates to Adobe Flash, Adobe Reader and Oracle (formerly Sun) Java, as these programs are frequented exploited by attackers.[31] More information about updating Windows and your applications can be found ***below***.

If, however, your intended use of Windows XP is for running some kind of business-critical application, then things can get a little trickier. For example, if the computer is used to run specific software, you will need to preserve the installation media for that proprietary software in case the computer needs to be replaced. If the software in question uses some sort of copy protection mechanism, you should make sure you have the ability to reactivate the software once it has been reinstalled—an issue that may be problematic if the company which made the software is no longer in business (or no longer supports it).

In this case, using disk imaging software may be the best method of keeping a "clone" of the working operating system around. However, keep in mind that cloning may require backing up and restoring an image of the computer's entire hard disk drive (HDD), so you may end up losing valuable data if you have to restore an older image of the system. We'll talk more about backups in a bit.

Backing Up Your Hardware: Issues with Interfaces

If the computer running Windows XP is used to control industrial or scientific equipment, it becomes even more important to keep backup copies not only of the software, but of the hardware as well. If the computer uses specialized hardware such as a serial, parallel or digital I/O controller card to communicate with the equipment, you should have at least one spare controller card to install in the PC, along with any cabling, software and device drivers needed for it to work.

This can become increasingly more difficult to manage if older hardware is required. Over the years, motherboards have used a variety of (for the most part, incompatible) expansion slots for cards, going from ISA[32] (1981)

[28] Microsoft. "Support for Windows XP is ending." (business messaging). Microsoft Corp. *https://www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx*.

[29] Microsoft. "Support for Windows XP is ending." (consumer messaging). Microsoft Corp. *https://windows.microsoft.com/en-us/windows/end-support-help*.

[30] Margel, Rob. "Download the Windows XP End Of Support Countdown Gadget." Microsoft Corp. *https://blogs.msdn.microsoft.com/robmar/2011/04/20/download-the-windows-xp-end-of-support-countdown-gadget/*.

[31] Selinger, Markus. "Adobe & Java Make Windows Insecure." AV-Test. *http://www.av-test.org/en/news/news-single-view/artikel/adobe-java-make-windows-insecure/*.

[32] Wikipedia. "Industry Standard Architecture." Wikimedia Foundation. *https://en.wikipedia.org/wiki/Industry_Standard_Architecture*.

to EISA[33] (1988) to VLB[34] (1992) to PCI[35, 36] (1993) to AGP[37] (1996) to PCIe[38,39] (2004). These days, it is difficult to find motherboards manufactured with PCI expansion slots, let alone the older interface technologies. If your use of Windows XP requires one of these legacy cards, you may end up spending a great deal of time and money trying to locate replacement parts to keep Windows XP running on worn-out hardware.

Backing Up Your Hardware: Issues with Disk Drives

Expansion cards and their interfaces are not the only technology to change over time. Even standard components like disk drives change. Over the years since Windows XP was released, hard disk drives have grown in capacity from megabytes to gigabytes to terabytes. While computer motherboards have adjusted over time to utilize greater disk drive capacities, older motherboards may only recognize hard disk drives up to certain sizes, such as 8GB or 137GB, depending upon how their BIOSes operate[40, 41]. Short for *Basic Input/Output System*, a BIOS is a small piece of software embedded in a chip on the motherboard that controls how hardware is enumerated (recognized and accessed) when the computer is booted.

In some cases, computer or motherboard manufacturers may have released updated BIOSes to allow older computers to use larger-capacity hard disk drives, but it may be difficult to locate such updates, especially if the manufacturer provides no support for older models or is no longer in business. Some hard disk drive manufacturers include a jumper switch which can be set on a hard disk drive so that it will report it is 8GB in size to the computer's BIOS, eliminating issues with the hard disk drive not being recognized. Of course, using this approach means that the remaining space on the hard disk drive goes to waste as it is no longer visible to the computer.

PATA versus SATA Hard Disk Drives

In 2001, it was standard to use an AT Attachment[42] (abbreviated as ATA, and also known as Enhanced Integrated Drive Electronics, or EIDE for short) disk drive in a PC, which would connect to the motherboard using a 40-pin (or later, 80-pin) ribbon cable. The reason for the large number of wires was that signals were transferred in parallel between the PC and disk drive. In 2003, the Serial ATA[43] (SATA) interface for disk drives was ratified, complete with different, non-compatible cabling that used fewer wires,

[33] Wikipedia. "Extended Industry Standard Architecture." Wikimedia Foundation. https://en.wikipedia.org/wiki/Extended_Industry_Standard_Architecture.

[34] Wikipedia. "VESA Local Bus." Wikimedia Foundation. https://en.wikipedia.org/wiki/VESA_Local_Bus.

[35] PCI-SIG. "Conventional PCI." http://www.pcisig.com/specifications/conventional/.

[36] Wikipedia. "Conventional PCI." Wikimedia Foundation. https://en.wikipedia.org/wiki/Conventional_PCI.

[37] Wikipedia. "Accelerated Graphics Port." Wikimedia Foundation. https://en.wikipedia.org/wiki/Accelerated_Graphics_Port.

[38] PCI-SIG. "PCI Express®." PCI-SIG Administration. http://www.pcisig.com/specifications/pciexpress/.

[39] Wikipedia. "PCI Express." Wikimedia Foundation. https://en.wikipedia.org/wiki/PCI_Express.

[40] DEW Associates Corp. "Hard Drive Size Limitations and Barriers In Depth." http://www.dewassoc.com/kbase/hard_drives/hard_drive_size_barriers.htm

[41] Torres, Gabriel. "Hard Disk Drives Capacity Limits." Hardware Secrets. http://www.hardwaresecrets.com/hard-disk-drives-capacity-limits/.

[42] Wikipedia. "Parallel ATA." Wikimedia Foundation. https://en.wikipedia.org/wiki/Parallel_ATA.

[43] Serial ATA International Organization. "Technical Overview." https://www.sata-io.org/technical-overview.

resulting in slimmer cabling being used. While it took another four years for SATA interfaces to become commonplace, their introduction did cause the immediate renaming of the original ATA standard to the Parallel ATA (PATA) standard.

Now, there's a reason for this disk drive history lesson, and it is very important to Windows XP: Microsoft never officially released a version of Microsoft Windows XP with native support for SATA disk drive interfaces included on the installation disc. Microsoft refers to such device driver[44] software as "inbox" when they are on the CDs (or DVDs) in the boxed version of Microsoft Windows sold in stores.

Microsoft, of course, worked with various manufacturers of disk drives, controller chips and computers to ensure that SATA worked in Windows XP, but for most people, the means of getting a copy of Windows XP with SATA support built in was to buy a new computer with Windows XP loaded onto it by the manufacturer, who would have added the SATA device drivers as part of the customizations they made to Windows XP for the computers they sold. It is possible for consumers to add SATA device drivers when they install a boxed version of Windows XP from scratch, but this required loading them off of floppy diskettes, an even older technology. Even at the beginning of the century, computers started to ship without floppy drives. IT departments could also create semi-customized versions of Windows XP with SATA device drivers "slipstreamed" into them. However, the process is not a consumer-friendly one. It was not until 2007, with the release of Windows Vista, that a person could buy a boxed copy of Windows off the shelf in a store and expect it install successfully on their SATA-equipped computers, at least without jumping through numerous hoops.

Issues with New Sector Sizes and Disk Partition Schemes

In addition to these changes to the connectors outside of hard disk drives, changes were occurring *inside* of hard disk drives as well: Since the early 1980s hard disk drive manufacturers have been manufacturing hard disk drives using sectors[45] that are 512 bytes (or characters) in length, as a sector is the smallest block of data that can be read or written from a disk. For example, if you created a file that was 100 bytes long, it would still occupy one 512-byte sector of a disk. If you created a file that was 513 bytes, it would occupy two sectors, and so forth. Individually accessing sectors, though, introduces a lot of I/O overhead in seeking, reading and writing data, so file systems map groups of sectors together into larger blocks called clusters, which may be up to 256KB (or 512 512-byte long sectors) long[46].

Keeping track of how files are stored on a disk drive is the job of the file system, but keeping track of how space is allocated (or the way in which a disk/volume is partitioned) for file systems on disk drives has been the job of the Master Boot Record (MBR)[47], a standard that dates back to 1983, and in its last implementation has a limit of 232 sectors [that's 4,294,967,295 sectors, or 2.199 terabytes (TB)]. When Windows XP was released in 2001, hard disk drives were just entering the gigabyte (GB) range, but today 8TB (and larger) hard disk drives are readily available to consumers.

[44] A device driver is a specialized small program that allows a particular piece of hardware to communicate with the operating system.

[45] Wikipedia. "Disk Sector." Wikimedia Foundation. https://en.wikipedia.org/wiki/Disk_sector.

[46] Microsoft. "Default cluster size for NTFS, FAT, and exFAT." Microsoft Corp. https://support.microsoft.com/en-us/help/140365/default-cluster-size-for-ntfs,-fat,-and-exfat.

[47] Wikipedia. "Master Boot Record." Wikimedia Foundation. https://en.wikipedia.org/wiki/Master_boot_record.

In order for computers to make use of these ever-growing hard disk drive capacities, several changes were introduced by operating system vendors and hard disk drive manufacturers:

- *A new standard for partitioning hard disk drives was introduced formally in 2010, called GUID Partition Table (GPT)[48]. GPT theoretically supports hard disk drives up to 9.4 zettabytes (9.4 billion terabytes). Windows XP does not recognize GPT-partitioned hard disk drives.*
- *Likewise, a new standard was introduced for sector sizes. Instead of continuing to use the almost thirty-year-old standard of 512 bytes per sector, disk drive manufacturers agreed to transition, starting in January 2011, to 4,096 byte (four kilobyte) sectors, a change referred to as Advanced Format (AF) technology[49, 50, 51]. Windows XP does not support Advanced Format (4KB) sectored disk drives natively, although more on that, below, for a workaround.*

These approaches are sensible, given the ever-increasing nature of storage capacities; however, they introduce additional problems for anyone using or maintaining Windows XP-era systems. Even if users never needs to utilize a disk partition larger than 2TB with their Windows XP installations, they still may end up using Advanced Format (4KB) sectored hard disk drives due to the unavailability of native 512-byte sector drives.

Unlike the GPT disk partitioning technology, Advanced Format disk drives that use 4KB sectors labeled as being "Advanced Format 512e" or simply "512e" disk drives[52] ***are*** backwards-compatible with older operating systems like Windows XP that use 512-byte long sectors. The conversion between 512-byte and 4,096-byte sectors is done by the disk drive itself. This introduces a small performance penalty from the overhead of having to emulating 512-byte sectors.

A Note About Solid-State Drives

Given that many current-day installations of Windows XP have modest storage requirements, it may be tempting to replace hard disk drives with solid-state drives (SSDs).

Today, top-end SSDs can operate more than 45 times faster than hard disk drives, especially hard disks available at the same time as Windows XP. Hard disk drives also suffer a performance penalty from file *fragmentation*, caused by the hard disk drive having to read and write files scattered across different sectors of their internal platters (the actual disks inside a hard disk drive). In contrast, solid-state drives have no moving parts and access all sectors on them at the same speed, meaning file fragmentation has little to no effect on them.

Although solid-state drives do not suffer from file fragmentation, over time they can suffer comparable performance issues because they have to keep track of which sectors (called *blocks* in SSDs) are used inside of which clusters (called *pages* in SSDs). This is solved by allowing the solid-state drives to periodically identify exactly which pages are no longer in use and mark them as free space, which is a technique known more commonly to programmers as *garbage collection*. For SSDs, performing garbage collection is called *trimming*, and, unsurprisingly, is handled by the operating system,

[48] Wikipedia. "GUID Partition Table." Wikimedia Foundation. https://en.wikipedia.org/wiki/GUID_Partition_Table.

[49] International Disk Drive Equipment and Materials Association. "Advanced Format (AF) Technology." http://www.idema.org/?page_id=98.

[50] International Disk Drive Equipment and Materials Association. "The Advent of Advanced Format." http://www.idema.org/?page_id=2369.

[51] Coughlin, Thomas M. "Aligning with the Future of Storage." Coughlin Associates, Inc. https://tomcoughlin.com/Coughlin/Techpapers/2011_06%20Alignment%20White%20Paper%20(Coughlin%20Assoc.)%20final.pdf.

[52] Wikipedia. "Advanced Format." Wikimedia Foundation. https://en.wikipedia.org/wiki/Advanced_Format.

which issues a special TRIM command to the SSD[53]. Neither Windows XP (nor its much-maligned successor, Windows Vista) support issuing TRIM commands to solid-state drives, meaning that drive performance will slow down over time, even to speeds slower than those of hard disk drives.

TIP	The lack of a TRIM command only hampers Windows XP when installing it directly to a solid-state drive. You can run Windows XP as a "guest" (in a virtual machine) on modern hardware that supports TRIM, such as Windows 7 or newer, which allows the "host" operating system to manage TRIM operation.

Backing Up Your Hardware: Wrapping It Up

It is important to remember that the failure rate for any computer part is 100%… eventually. Even if your computer does not use any "special" expansion cards or other hardware, it is still a good idea to keep a stock of replacement parts such as disk drives and fans, which contain mechanical parts that wear out over time. Solid-state parts with no moving components like memory, motherboards and some power supplies can suffer from component failure as they age and go through cycles of thermal expansion and contraction during normal usage.

Even parts like hard disk drives, which one think might think of as remaining relatively unchanged over time, need to have a special supply kept for them, due to technological changes such as SATA interfaces and Advanced Format sectoring.

In cases like this, the best thing to do is to maintain not just an inventory of replaceable parts, but an entire computer (or two) that has been built and configured to run your business-critical application. That way, if that old Windows XP computer does fail, you can remove it, plug the new computer in, and be up and running in a matter of minutes after loading your latest backup or data files onto it. You could even swap the "in-use" computer with the "spare" computer two or three times a year, which allows you perform preventive maintenance such as cleaning out dust and replacing mechanical parts before a failure occurs. For purposes of reliability and longevity, spare parts and computers should be stored in a climate-controlled environment. Some components such as motherboards and some storage controllers have batteries on them. These should be disconnected and removed before entering long-term storage to avoid damage from battery leaks. A storeroom in your office should be fine for this purpose. A warehouse without any heating or air conditioning is not ideal, because exposure to excessive heat, cold, humidity and dryness can reduce the effective life of electronics, even when they are not powered on.

Backing Up Your Software

Now that you have an idea of the steps needed to keep the hardware going that keeps Windows XP up and running, let's take a look at the requirements for backing up the software-side of things. This discussion is going to be shorter than the section on hardware, above, not because it is simpler—it isn't—but because it is so complex. On the matter of backups, ESET has a white paper devoted exclusively to that subject, *Options for Backing Up Your Computer*[54]. As a result, in this white paper we will only go over the bare essentials for backing up your machine.

[53] Wikipedia. "Trim (computing)." Wikimedia Foundation. https://en.wikipedia.org/wiki/Trim_(computing)

[54] Goretsky, Aryeh. "Options for backing up your computer." ESET. http://www.eset.com/fileadmin/Images/US/Docs/Home/Staying_Secure/2205_19_0_EsetWP-OptionsBackingUpComputer.pdf.

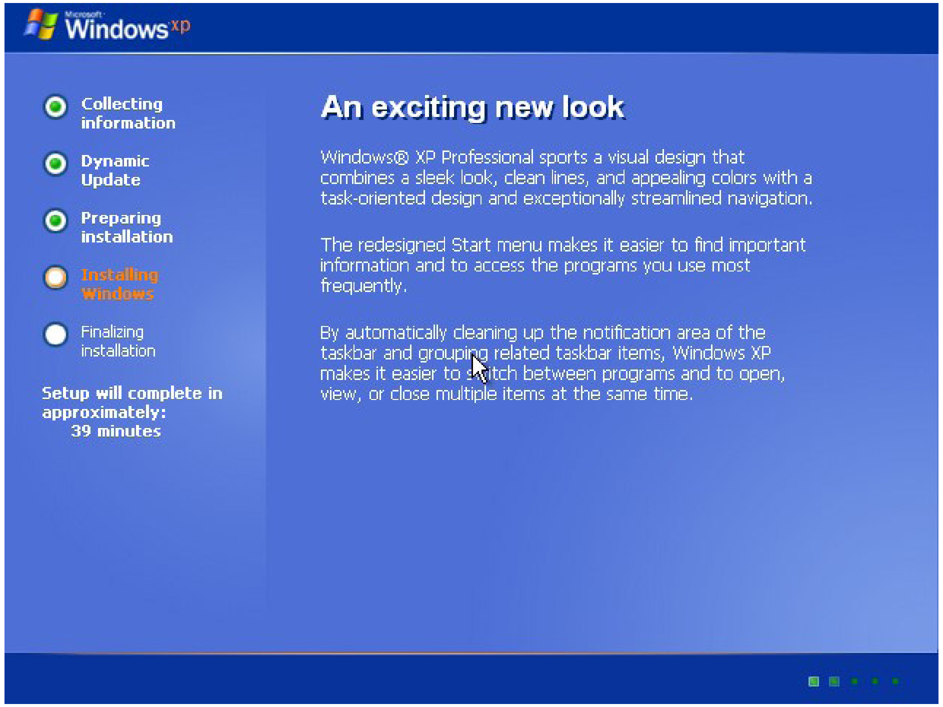
If you are looking to back up a computer running Microsoft Windows XP, there are two major kinds of backups that can be performed:

- *The first is a file backup, which basically means copying the files on the computer from one location to another. For example, from the computer's internal hard disk drive to a network share, an external hard disk drive plugged into a USB port, and so forth. The advantage of this approach is that the files are easily accessible and readily available by plugging the external hard disk drive into a new computer, connecting to the network share containing the files, etc.*
- *The second mechanism is a "blob" (binary object) backup. With this mechanism, files (or even the entire disk drive) are backed up in monolithic "blocks." These blocks may range in size from megabytes to gigabytes, in order to make them easier to save to optical media such as CDs and DVDs, or to tape. The most common implementation is* disk imaging, *where the contents of the entire hard disk drive, in use or not, are copied to another hard disk drive, tape drive or other storage medium with the same or greater capacity as the original hard disk drive.*

Again, for more detailed information, including the advantages and disadvantages of each mechanism, how to schedule backups, and, most importantly, how to test them, it is strongly recommended you read ESET's white paper on backups, ***Options for backing up your computer***.

SETTING UP XP FOR LONG-TERM USAGE

If you are planning on using Microsoft Windows XP for an extended period of time past the April 8, 2014 EOL date, we have a variety of recommendations for you.



Collecting information

Dynamic Update

Preparing installation

Installing Windows

Finalizing installation

Setup will complete in approximately:
39 minutes

An exciting new look

Windows® XP Professional sports a visual design that combines a sleek look, clean lines, and appealing colors with a task-oriented design and exceptionally streamlined navigation.

The redesigned Start menu makes it easier to find important information and to access the programs you use most frequently.

By automatically cleaning up the notification area of the taskbar and grouping related taskbar items, Windows XP makes it easier to switch between programs and to open, view, or close multiple items at the same time.

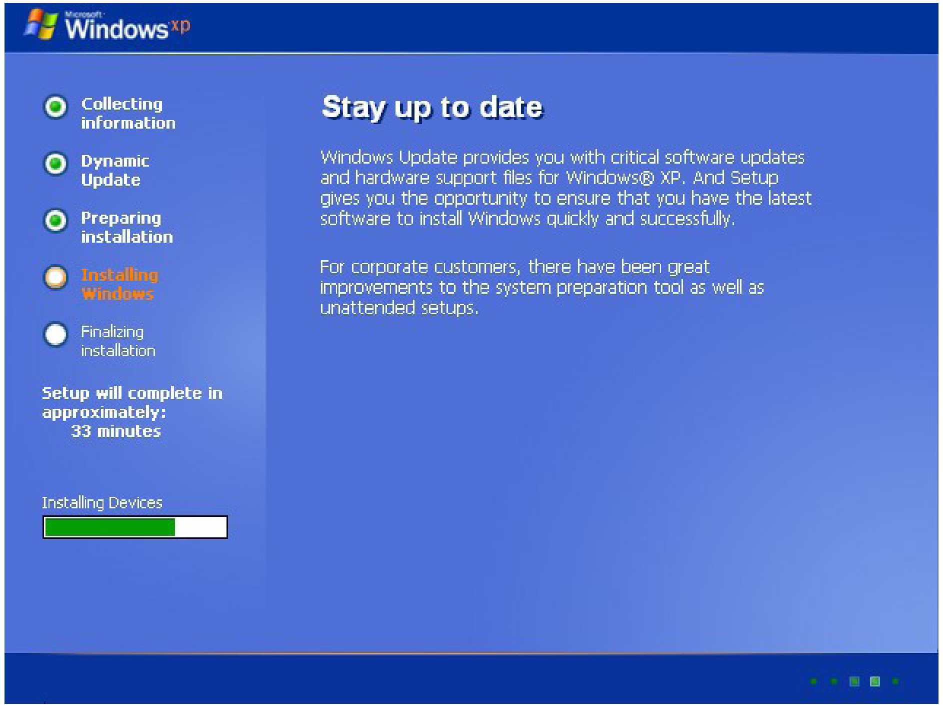
Figure 3: A Windows XP installation screen

First, get your PCs ready for long-term usage by starting with a clean installation of Windows XP. If the current installation of Windows XP is more than a few years old, chances are it is littered with the detritus and debris that befall any old installations of Windows, such as missing-or-outdated device drivers, incompletely-uninstalled programs, programs that are obsolete or otherwise no longer used but still present, broken shortcuts, incorrectly associated file associations and so forth. Because having a mishmash of software and operating system errors is likely to affect the long-term reliability, stability and performance of your installation of Windows XP, starting anew with a fresh installation of this old operating system is an important step in preparing it for use now it is no longer supported by Microsoft.

As a reminder, do not use the computer to access the Internet while installing all of Windows XP's service packs, patches, hot fixes and other updates. Windows XP is vulnerable to attack and the computer should remain behind a firewall to prevent its as-yet unfixed vulnerabilities from being exploited. It is best to download Windows XP's updates on a computer with a secure, modern operating system and then transfer them to the computer running Windows XP. This also applies to security software, as well.

Installing XP Anew

If possible, start with a blank, unformatted hard disk drive—or at least one that you can erase prior to the installation. Using a blank hard disk drive helps ensure there are no file system or software problems to start with, as there might be if using an existing installation of Windows XP. We have mentioned the steps above needed to ensure a hard disk drive is compatible with Windows XP. If the hard disk drive uses a SATA interface, make sure your installation media for Windows either have the device drivers already added, or you have them available to install via floppy diskette as Windows XP's installer does not recognize USB or network connections. Support for additional optical drives may be limited, making floppy diskettes the best way to install device drivers if they are not present on the installation media. Once Windows XP is finished installing, you will be able to access these other types of devices.



Stay up to date

Windows Update provides you with critical software updates and hardware support files for Windows® XP. And Setup gives you the opportunity to ensure that you have the latest software to install Windows quickly and successfully.

For corporate customers, there have been great improvements to the system preparation tool as well as unattended setups.

Setup will complete in approximately:
33 minutes

Figure 4: Another Windows XP installation screen

In order to connect to any networks, including the Internet, you may also need to install device drivers for the computer's network interface card. These may have been bundled into the computer manufacturer's version of Windows XP that you are installing. If not, they may be on a CD or DVD that came with the computer. Failing that, you may need to download them from the manufacturer's support web site on another computer, copy them to a CD, DVD or USB flash drive, and bring them over for installation on the "new" computer running Windows XP.

Installing Windows XP's Service Packs

Chances are there are several years' worth of updates to apply, including one or more of Microsoft's Service Packs for Windows XP. A Service Pack bundles not only hundreds of existing updates into a single package, but also changes to Windows XP's default settings from when it was released. Service Packs also contain newer versions of existing older updates, and allow them to be applied to the operating system together instead of individually.

To find out which Service Pack, if any, is installed with your Microsoft Windows XP, click on the Start button, type in "`winver.exe`" and press Enter. The version of Windows will be displayed along with the Service Pack level. If no Service Pack information is displayed, then the original Release To Manufacturing (RTM) version of Windows XP is installed.

If you are lucky, your installation media for Windows XP includes Service Pack 3—the last Service Pack released for Windows XP—and your downloading will be limited to whatever post-SP3 updates are required. That is still several hundred megabytes worth of updates, but not an insurmountable quantity, especially on a fast Internet connection. Note that Service Pack 3 is for 32-bit versions of Windows XP only; the latest Service Pack for the 64-bit edition of Windows XP is Service Pack 2.

The following table gives an overview of the major changes each Service Pack brought to Microsoft Windows XP, along with links to the pages on Microsoft's web site from which each Service Pack can be downloaded:

Service Pack	Release Date	Notable Features and Improvements / Download Links
1	September, 2002	300+ minor bug fixes; USB 2.0 support; Microsoft Java* and .NET Framework support; Set Program Access and Defaults Control Panel Applet **Download:** http://www.download.windowsupdate.com/msdownload/update/v3-19990518/cabpool/xpsp1a_8441053935adbfc760b966e5e413d3415a753213.exe
2	August, 2004	820+ bug fixes; improvements to Wi-Fi and Bluetooth; native Wi-Fi Protected Access support, pop-up ad blocker in Internet Explorer 6; Data Execution Prevention; removal of raw sockets; Windows Security Center; Windows Firewall improvements **Download:** http://www.microsoft.com/en-us/download/details.aspx?id=28
3	May, 2008	1,700+ bug fixes; improvements to BITS, Data Execution Prevention, Group Policy, IPSec, MMC, RDP, Windows Imaging, Windows Installer, Windows Script and X.509 certificate handling; Wi-Fi Protected Access 2 support; Network Access Protection client for enterprises. **Download:** https://www.microsoft.com/en-us/download/details.aspx?id=55245

**In February 2003, Microsoft Java Support was removed from SP1 due to a lawsuit with Sun Microsystems and the service pack re-released as SP1a.*

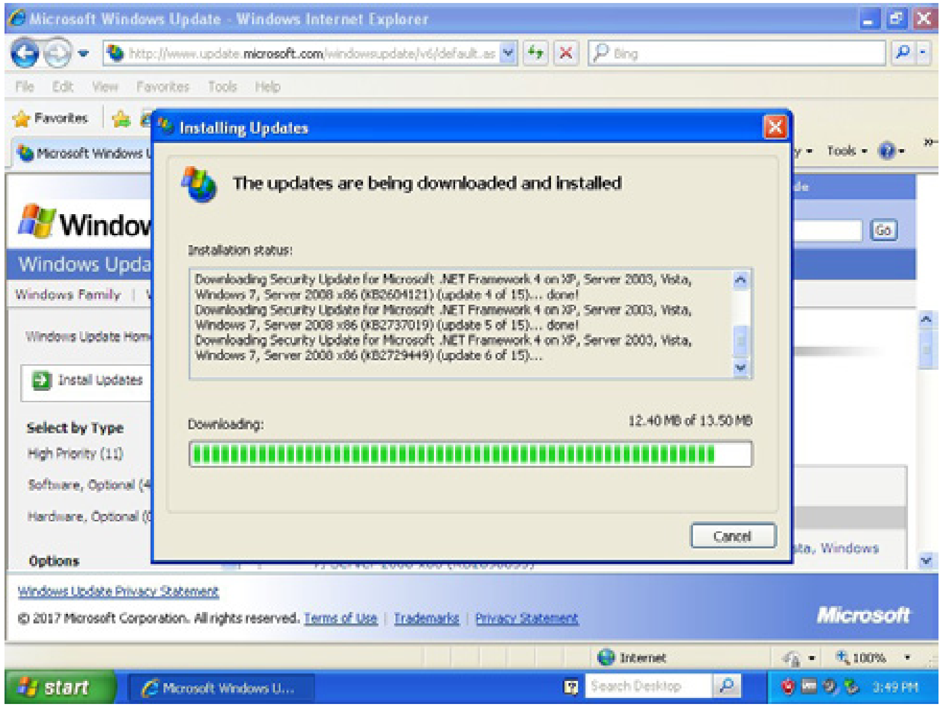
We are providing links to the download pages for each of Windows XP's Service Packs in case you wish to download and install them separately before beginning the Windows Update process. These download locations may change in the future, so it is good practice to save important operating system updates such as these in an easy-to-remember location so they may be installed in the future without having to download them again.

TIP	In order to speed up the process of updating Microsoft Windows XP, download whichever Service Pack(s) you need and install them separately ***before*** running Windows Update. This minimizes the amount of time spent downloading updates for Windows XP, as only post-Service Pack 3 updates will be displayed.

Windows XP's Service Pack updates are, in theory, *cumulative*. This means that Service Pack 2 contains all of the updates from Service Pack 1, and that Service Pack 3 contains all of the updates from Service Pack 2 and Service Pack 1. In practice, Microsoft does not recommend installing Service Pack 3 on computers running the original RTM or SP1 versions of Windows XP, so install Service Pack 2 first to update the operating system from RTM or SP1, reboot, and install Service Pack 3.

Windows Updates

Even if you are performing a fresh installation of Microsoft Windows XP with the latest service pack, you will still have several years' worth of post-Service Pack 3 updates to install after making any changes necessary to gain network access, such as installing device drivers for a network interface card.



Installing Updates

The updates are being downloaded and installed

Installation status:

Downloading Security Update for Microsoft .NET Framework 4 on XP, Server 2003, Vista, Windows 7, Server 2008 x86 (KB2604121) (update 4 of 15)... done!
Downloading Security Update for Microsoft .NET Framework 4 on XP, Server 2003, Vista, Windows 7, Server 2008 x86 (KB2737019) (update 5 of 15)... done!
Downloading Security Update for Microsoft .NET Framework 4 on XP, Server 2003, Vista, Windows 7, Server 2008 x86 (KB2729449) (update 6 of 15)...

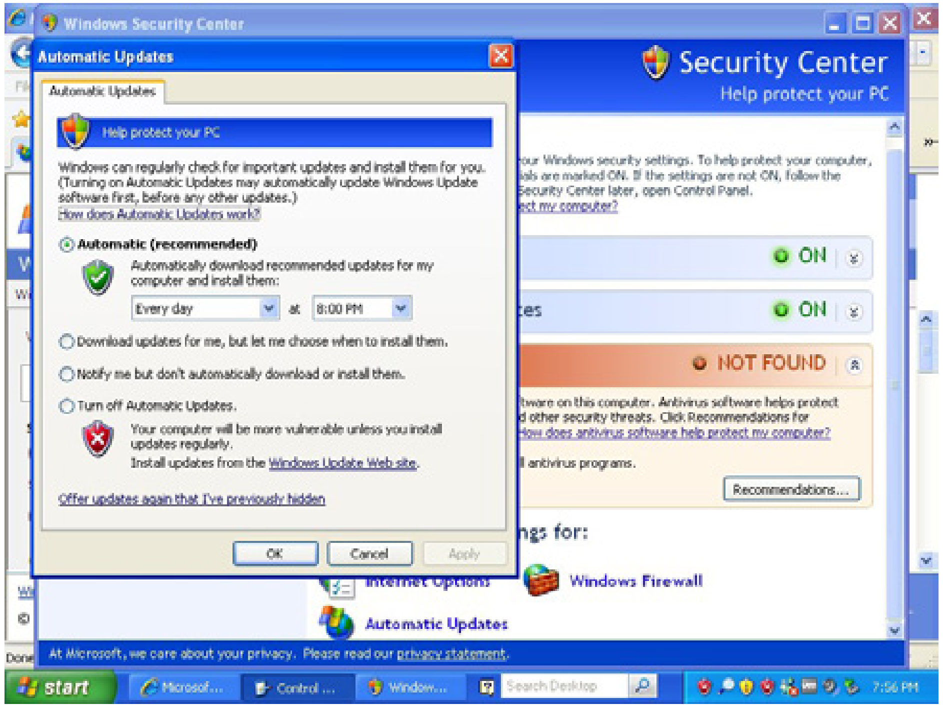
Downloading: 12.40 MB of 13.50 MB

Microsoft Windows Update - Windows Internet Explorer
http://www.update.microsoft.com/windowsupdate/v6/default.as
Bing
File Edit View Favorites Tools Help
Favorites
Microsoft Windows U
Tools
Windows Update
Windows Family
Windows Update Home
Install Updates
Select by Type
High Priority (11)
Software, Optional (4
Hardware, Optional (
Options
Go
Cancel
Windows Update Privacy Statement
© 2017 Microsoft Corporation. All rights reserved. Terms of Use | Trademarks | Privacy Statement
Microsoft
Internet
100%
start
Microsoft Windows U...
Search Desktop
3:49 PM

Figure 5: Windows Update runs via web browser in Windows XP

Once Windows XP has network access, the next step is to let Windows XP's Automatic Updates run, so the operating system will download and install all the patches, hotfixes and service packs that have been released since the Windows XP installation media was created.

Depending upon the age of your Windows XP installation, the operating system may be so old that it needs an update to the Windows Update mechanism itself before it can download any further updates. This can be done by opening the **Control Panel**, opening the **Security Center** by clicking on it, selecting the *Automatic Updates* option at the bottom of the window, and making sure that Automatic Updates are set to *Automatic (recommended)*.



Automatic Updates

Help protect your PC

Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)
How does Automatic Updates work?

● Automatic (recommended)
Automatically download recommended updates for my computer and install them:
Every day at 8:00 PM

○ Download updates for me, but let me choose when to install them.

○ Notify me but don't automatically download or install them.

○ Turn off Automatic Updates.
Your computer will be more vulnerable unless you install updates regularly.
Install updates from the Windows Update Web site.

Offer updates again that I've previously hidden

Figure 6: Enabling Automatic Updates via the Windows Security Center

This will allow Windows XP to download critical updates to the operating system's updating mechanism, after which a reboot will be required. Once rebooted, allow *Automatic Updates* to proceed to install any remaining critical updates. After *Automatic Updates* has installed these, you can install the remaining security updates and bug fixes by launching **Windows Update** from the Start Menu. If the Windows Update shortcut is not available, open Internet Explorer and go to `http://update.microsoft.com/` to begin the process of downloading and installing updates. Unlike later versions of Windows, which have a dedicated application for installing Windows Updates, Windows XP installs them through the Internet Explorer web browser.

WARNING

Depending upon when your installation media discs for Windows XP were originally created, they may be five, ten or even more years out-of-date. As a result, Windows XP will be **highly insecure** not just until it is completely patched (a process that may take a few hours depending upon the speed of your Internet connection and require several reboots) but also until you are done securing it even further against attacks.

To help protect Windows XP while it is being installed, it is important to follow these two instructions:

1. If possible, do **not** connect the computer directly to the Internet using a modem, as a direct connection means that attackers will have easy access to the unprotected computer. Instead, make sure your computer is connected to a router (a residential gateway broadband router for home and SOHO use, or a more advanced network router if in an office) which, as the name implies, breaks the direct connection the computer has to the Internet, and vice-versa, making it a tougher target for attackers.

   Most Internet connections use a router these days, but direct connections are still available in many parts of the world. Contact your Internet service provider if you are unsure of what sort of Internet connection they provide.

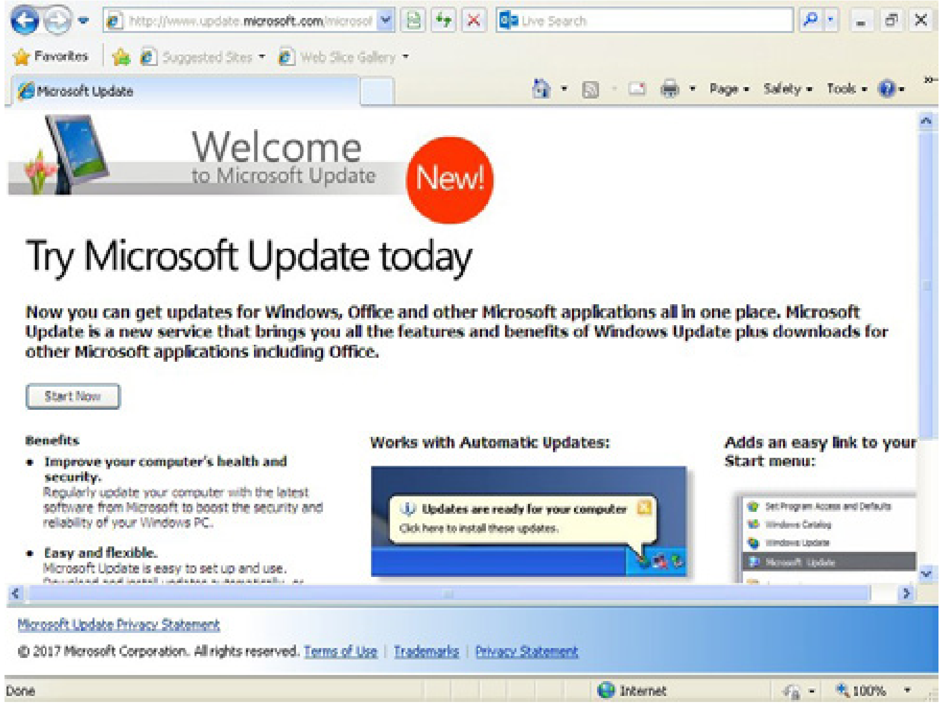
2. Do not visit any web sites, download any programs or run any software that connects to the Internet until Windows XP is completely finished with its updates and you have taken further steps to secure it. Using Windows XP makes a computer a large target, and you should not use it on the Internet until you have minimized that threat as much as possible.

   As with Windows Updates and device drivers, download security software for Windows XP on an already-secured computer, and bring it to the computer for installation. If offered a choice between a "web installer" and an "offline installer," choose the offline installer so that the entire program can be installed. It will still need to download some updates once installation is finished, but the full program will be installed and able to offer some protection.

On the *Optional* tab for Windows Updates, you may see an option to install Microsoft Security Essentials (MSE), Microsoft's free anti-malware (aka anti-virus) program for use in homes and small business with under ten PCs[55, 56]. If you are planning on using anti-malware software from a different vendor (including ESET) you should not install MSE onto the computer. We will discuss anti-malware software in greater depth, below.

Windows Updates versus Microsoft Updates

During the installation of Windows updates through the Internet Explorer web browser, you may be prompted to install ***Microsoft Update*** as well.



Welcome to Microsoft Update

Try Microsoft Update today

Now you can get updates for Windows, Office and other Microsoft applications all in one place. Microsoft Update is a new service that brings you all the features and benefits of Windows Update plus downloads for other Microsoft applications including Office.

Benefits

- Improve your computer's health and security.
  Regularly update your computer with the latest software from Microsoft to boost the security and reliability of your Windows PC.
- Easy and flexible.
  Microsoft Update is easy to set up and use.

Works with Automatic Updates:

Updates are ready for your computer
Click here to install these updates.

Adds an easy link to your Start menu:

Microsoft Update Privacy Statement

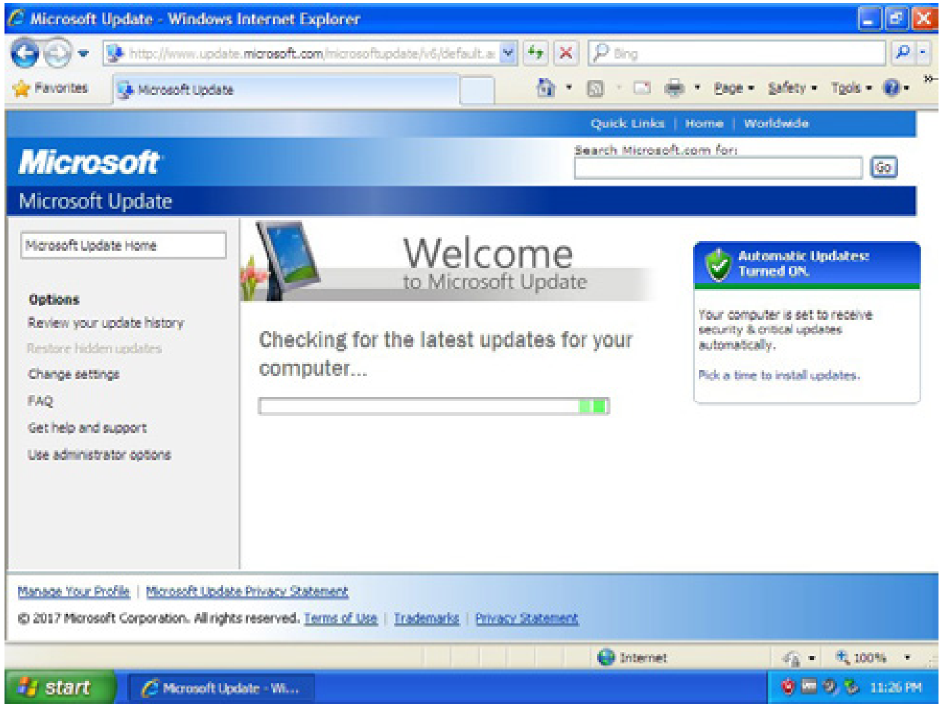
© 2017 Microsoft Corporation. All rights reserved. Terms of Use | Trademarks | Privacy Statement

Figure 7: Windows Update prompts for Microsoft Update

While Windows Update provides updates to the operating system core files, it does not provide any updates to applications, such as Microsoft Live Essentials, Office, Skype and Silverlight.

[55] Microsoft. "Microsoft Security Essentials – Protect Your PC." http://windows.microsoft.com/en-US/windows/security-essentials-download.

[56] Microsoft "Microsoft Safety & Security Center: Get free virus protection with Microsoft Security Essentials." http://www.microsoft.com/security/pc-security/microsoft-security-essentials.aspx.


Microsoft Update - Windows Internet Explorer
http://www.update.microsoft.com/microsoftupdate/v6/default.a
Bing
Favorites
Microsoft Update
Page
Safety
Tools
Quick Links | Home | Worldwide
Microsoft
Search Microsoft.com for:
Go
Microsoft Update
Microsoft Update Home
Options
Review your update history
Restore hidden updates
Change settings
FAQ
Get help and support
Use administrator options
Welcome
to Microsoft Update
Automatic Updates: Turned ON.
Manage Your Profile | Microsoft Update Privacy Statement
Terms of Use | Trademarks | Privacy Statement
Internet
100%
start
Microsoft Update - Wi...
11:26 PM

Checking for the latest updates for your computer...

Your computer is set to receive security & critical updates automatically.

Pick a time to install updates.

© 2017 Microsoft Corporation. All rights reserved.

Figure 8: Microsoft Update checking for updates

We recommend that you enable Microsoft Update in order to obtain updates for these programs.

In order to update Microsoft Windows XP fully, you may need to run Windows Update or Microsoft Update multiple times, as some of the initial updates that are downloaded may require further updating themselves. Keep running these updaters manually until all updates are installed and no further updates are offered.

TIP	Windows Update and Microsoft Update display each available update as a single line with a check box in front of it in Internet Explorer. When you check (select) an update, it expands downward to show several lines of descriptive text. To minimize the amount of scrolling needed to go through the list, start from the bottom and work your way up to the top.

Device Driver Installation

During the Windows Update process, you will likely be asked to install missing or updated device driver software to allow Microsoft Windows XP to work best with the computer's hardware. In the past, Windows Update has had some problems with identifying and providing the correct device drivers, causing some computers to behave poorly or even lock up. This has led some people to recommend going to either the hardware manufacturer's support web site to download them, or to try to identify the actual chip manufacturer, go to their support web site and download the drivers from there.

Microsoft has gone through a great deal of effort to improve the correct detection of hardware and downloading of the right device drivers through Windows Update in the past few years and has largely alleviated such issues. However, that does not always mean that Windows Update will provide the *latest* device drivers for a computer's hardware, just the ones that have been submitted to it by the manufacturer of the computer or the chips inside of it. Some computer manufacturers provide a program that automatically identifies missing and outdated drivers and installs them automatically[57, 58, 59]. If yours does, you may want to consider using it to download device drivers if you have concerns about Windows Update.

To ensure that you have the latest Microsoft Windows XP device drivers for your computer, we recommend visiting the manufacturer's support web sites from a computer with an up-to-date, *supported* operating system and with current security software installed, downloading them, and then transferring them via CD, DVD or USB flash drive for installation on the computer running Windows XP.

Computer manufacturers are not likely to support Microsoft Windows XP indefinitely with device driver updates, and some may even go out of business and thus discontinue support. For this reason, we recommend that after downloading any necessary device drivers, you save them to an easy-to-remember location as well as store a separate copy in a safe archival location.

Here is a short (and, of, necessity, incomplete) checklist for device drivers you may want to make use of when identifying the device drivers that are needed to install Windows XP on the computer:

Required? / Downloaded?	Description	Common Vendors
□/□	audio drivers for sound card Version: ____________	Analog Devices, AMD (formerly ATI), C-Media, Creative Labs, IDT, M-Audio, Realtek, SigmaTel, Turtle Beach, VIA
□/□	chipset drivers for motherboard Version: ____________	AMD (formerly ATI), Intel, nVidia, SIS, ULI (formerly ALI), VIA, Winbond
□/□	computer-specific *(for mouse and keyboard, power management, special features of motherboards, expansion cards and so forth)* Version: ____________	Acer (formerly Gateway), AMD (formerly ATI), ASRock, Asus, Clevo, Dell, ECS, EVGA, Foxconn, Fujitsu, Gigabyte, Hewlett-Packard (formerly Compaq), Intel, Lenovo (formerly IBM), MSI, Packard Bell, PNY, Samsung, Shuttle, SONY, Supermicro, Toshiba, Tyan, VIA, XFX, ZOTAC
□/□	network drivers for wired network connections *(Ethernet, Fiber, Token-Ring)* Version: ____________	ASIX, Atheros, Broadcom, Cisco, Hewlett-Packard (formerly 3Com), Intel, Marvell, nVidia, Ralink, Realtek, SIS, SMC, US Robotics, VIA, Winbond
□/□	network drivers for wireless network connections *(Bluetooth, Wi-Fi)* Version: ____________	Agere, Atheros, Broadcom, CSR, Intel, Ralink, Realtek, TDK, Toshiba, VIA
□/□	PATA, SATA or SCSI drivers for disk drive controllers Version: ____________	3ware, ALI, Adaptec, AMD (formerly ATI), Areca, Avago, High Point, Intel, ITE, JMicron, LSI, Marvell, nVidia, Promise, Silicon Image, SIS, VIA
□/□	printer drivers for printer Version: ____________	Brother, Canon, Citizen, Dell, EPSON, Hewlett-Packard, Lexmark, Kodak, Konica, Kyocera, OKI, Panasonic, Ricoh, Xerox
□/□	video drivers for video card Version: ____________	AMD (formerly ATI), Hauppauge, Intel, Matrox, nVidia, S3, SIS, VIA

[57] Dell. "Dell Driver Download Manager FAQs." http://support.dell.com/support/topics/global.aspx/support/downloads/en/downloads_faq.

[58] "HP Customer Support – Software and Driver Downloads." https://support.hp.com/us-en/drivers.

[59] Lenovo. "ThinkVantage System Update." http://support.lenovo.com/en_US/detail.page?LegacyDocID=TVSU-UPDATE.

It is always a good idea to download device drivers ***directly*** from the silicon chip or manufacturer's web site, just as you should any other software. Avoid visiting third-party websites, as there is no guarantee about the safety or reliability of their files. In some cases, this may be unavoidable; however, be sure to check the files carefully with your security software before using them.

In addition to device drivers to control a computer's hardware, updates may be available for the hardware itself in the form of new BIOS firmware (software that is stored in a chip and run when the computer initializes at power-up). Motherboards, and some expansion cards, often have a programmable chip on them that contains instructions on how to communicate with the various devices that connect to them. Manufacturers periodically update these to add compatibility for newer devices, improve performance and, yes, even fix bugs (it *is* software, after all). Check with the device manufacturer to determine if a BIOS firmware update is available—and needed—for your hardware.

After installing the latest device drivers for the computer's hardware, you should now have not only a fully-updated version of Microsoft Windows XP, but an installation that has the latest device drivers for hardware support as well. Although no third-party application or utility software has yet been installed, this would be a good time to create one (or more) backups of the computer's hard disk drive. An image-based backup here provides an advantage in that it can be more quickly restored if the operating system is in a non-functioning state. This can save the time and effort required to rebuild Windows XP from scratch should a problem arise and the sole backup is damaged or missing.

This disk image provides a "zero-point" or "baseline" image that can quickly be reloaded in case of a problem encountered when installing the specialized software that only runs under Microsoft Windows XP.

TIP	Backups should always be stored in a safe, easy-to-remember location. That way, you will easily be able to access them should you need to perform a restore operation. As a matter of fact, now is an excellent time to verify that the backup is working by performing a restore of it to a blank, spare disk drive from your parts inventory (*q.v.*). This will allow you to verify that the backup is working before an emergency situation arises where you actually might need it, only to find out it isn't working. Remember: The best time to fix problems is **before** they turn into a full-scale emergency that causes your business lost productivity and revenue.

Preparing for Use

Now that your baseline installation of Microsoft Windows XP is installed, updated with the latest Service Pack and hot fixes, and has all device drivers necessary for operation, it is time to begin loading whatever software it is that can only be run under Windows XP.

It is important to keep in mind that you should not be installing *all* of the software you typically use on a computer; the goal of this activity is, after all, to create a system running Microsoft Windows XP that can be used for as long as it needs to be used before being replaced with a more modern and secure version of Windows. Every additional program added to the computer means another piece of software with its own vulnerabilities that an attacker can exploit. Keeping the amount of installed software to a minimum reduces the "size" of the computer's "attack surface," *i.e.*, the amount of risk.

Framework Dependencies

If the software you are installing depends on a particular framework, such as Microsoft's .NET Framework, Microsoft Silverlight, Adobe Flash, Adobe Reader or Oracle Java, install the latest version compatible with Windows XP. If the developer continues to update it in the future, download and install these updates as well since vulnerabilities in the software or framework can be exploited by an attacker. If the software requires an older, insecure version of a framework, or the framework no longer supports Windows XP, install the most recent version and check with its developer to see if they have additional recommendations on how to secure it.

Web Browsers

While Microsoft's Internet Explorer 8.0[60] web browser is no longer a major target, there are still threats that can exploit it, and since it is no longer being updated for Windows XP, it is a good idea to use a newer web browser that receives security updates.

Google Chrome and Mozilla Firefox are the two most-widely-used web browsers; however, Google Chrome stopped supporting Windows XP and Windows Vista in April 2016 in its Version 49 release[61]. While this makes it a better candidate for browsing modern web sites than Internet Explorer, it is still a poor choice from a safety, privacy and security perspective. The Mozilla Foundation announced that Firefox will be supported on Windows XP and Vista until June 2018, at which point the non-profit will reassess whether to continue support for Windows XP[62]. This leaves Mozilla Firefox as the sole remaining mainstream web browser to use with Windows XP, albeit one with a clock ticking downwards towards expiry.

Since Google Chrome is based on Chromium, an open source project, and Mozilla Firefox is also released as an open source project, it is possible that there may be forks of theses web browsers' code bases that will allow for continued support of Windows XP. If you choose to use such a browser, be sure to test it thoroughly for compatibility.

PDF Readers

As was mentioned earlier, to avoid increasing the system's attack surface, you should avoid installing any additional software beyond what is absolutely needed under Windows XP. Software that views or prints PDF files may, however, be a requirement. Adobe Acrobat Reader is the most common PDF reader, and Adobe Acrobat Reader XI (aka v11.0) is supported on Windows XP through mid-October, 2017, which is almost two years longer than Windows Vista had support[63].

The PDF document specification allows JavaScript to be used for forms and workflow automation, and these are commonly used as an attack vectors because they can contain malicious code. It is important to keep Adobe Acrobat Reader up to date to protect against vulnerabilities. If you must use Adobe Acrobat Reader, verify that Adobe Reader Protected Mode, Protected View, and Enhanced Security are enabled, and disable

[60] Wikipedia. "Internet Explorer 8." Wikimedia Foundation. http://en.wikipedia.org/wiki/Internet_Explorer_8.

[61] Pawliger, Marc. "Update to Chrome platform support." Google, Inc. https://chrome.googleblog.com/2015/11/updates-to-chrome-platform-support.html.

[62] Mozilla. "Update on Firefox Support for Windows XP and Vista." Mozilla Blog. https://blog.mozilla.org/futurereleases/2017/10/04/firefox-support-for-windows-xp-and-vista/.

[63] Wikipedia. "Adobe Acrobat version history." Wikimedia Foundation. https://en.wikipedia.org/wiki/Adobe_Acrobat_version_history#Adobe_Acrobat_and_Reader.

JavaScript[64, 65]. If you are unable to disable JavaScript, lock it down as much as possible following Adobe's instructions[66, 67].

If your use of PDF files does not require forms or workflow automation, consider using another PDF reader that still supports Windows XP but does not contain support for JavaScript, such as Evince or Sumatra PDF, for a default PDF reader[68, 69].

Reminder: Make a Backup

At this point, the computer is configured for use, but is essentially insecure. In the next section, we will explain how to make Microsoft Windows XP *more* secure through the use of both Microsoft tools and practices, as well as third-party software that you can install.

Aside from being less secure then newer versions of Microsoft Windows, Windows XP is less resilient in recovering from problems caused by incompatible software. This being the case, there is always a slim possibility that some of the security recommendations in this paper may not work with your installation of Windows XP, or the software running on top of it.

Because of this, we recommend making another backup of the computer now, before you begin to secure it. That way, if a problem does occur due to one of the steps outlined, you will be able to restore the computer quickly to a known, good working state.

For more information about backups, see the previous section, ***Backing Up Your Software***.

SECURING WINDOWS XP FOR LONG TERM USAGE

Now that the computer running Microsoft Windows XP is up-to-date and configured with whatever software it is that cannot be run under a newer version of Microsoft Windows, it is time to begin making it more secure.

Over the intervening years, Microsoft has made numerous investments in Microsoft Windows XP's security, and the fully-patched and updated

[64] Arkin, Brad. "Introducing Adobe Reader Protected Mode." Adobe Systems, Inc. http://blogs.adobe.com/security/2010/07/introducing-adobe-reader-protected-mode.html.

[65] Adobe. "Application Security Overview." Adobe Systems, Inc. http://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/index.html.

[66] Adobe. "JavaScripts in PDFS as a security risk." Adobe Systems, Inc. https://helpx.adobe.com/acrobat/using/javascripts-pdfs-security-risk.html.

[67] Adobe. "JavaScript Controls" Adobe Systems, Inc. https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/javascript.html.

[68] Evince. "Evince." The GNOME Project. https://wiki.gnome.org/Apps/Evince.

[69] Kowalczyk, Krzyystof. "Sumatra PDF." https://www.sumatrapdfreader.org/.

version of Windows XP as it exists after April 8, 2014 is much more secure than the version of Windows XP available on October 25, 2001, but the need for backwards compatibility with a wide variety of hardware and software, plus practical limitations about how much an operating system can be changed during its lifecycle, mean that some of Windows XP's default options make it unsafe for use in today's world.

In the following sections, we will look at what steps can be taken to make Windows XP more secure using Microsoft's own tools, some of which are built into Microsoft Windows XP, and others that you may have to download. Then, we'll look at what sorts of additional defenses can be added with third-party tools. But, before we begin those two steps, I would first like to address a "step zero," if you will, that does not often get mentioned on the context of securing an operating system: Physical security.

NOTE:

The following instructions have been specifically written for home users and small businesses that may not have access to dedicated IT staff to manage their computers.

Many of the instructions in the rest of this paper explain how to secure a standalone computer running Microsoft Windows XP that is not connected to an Active Directory domain.

Computers connected to an Active Directory domain are managed by IT staff who should determine the appropriate level of security for them.

Physical Security

If the computer running Microsoft Windows XP is going to be in a publicly-accessible (or semi-accessible) location, it's worth taking a moment to consider how to secure it from potential attackers. This includes not just physical theft of the computer, but unauthorized access as well.

If the software the computer is running does not use them, disconnecting the keyboard and mouse – thus limiting access to its input devices – is a good idea, to reduce the risk of the computer being misused. Keep in mind that the round, barrel-shaped PS/2 connectors used by older keyboards and mice are **not** hot-pluggable. The computer will need to be powered down before they are connected or removed. USB-based keyboards and mice are hot-pluggable, and can be connected and removed while the computer is running.

There is a variety of physical anti-theft solutions available to lock a computer down so it cannot be easily stolen, or opened up or modified. The exact mechanisms will vary based on the size, type and location of the computer (as well as your budget), but could be as simple as a cable-lock to prevent the computer from being taken, to the use of anti-theft screws to make the chassis more difficult to open, to metal enclosures that block access to the computer's ports.

While the theft of a computer is quite noticeable, it is likely that far more damage would be caused by an attacker who is able to access the computer for the purposes of installing software, altering its information, copying files from it, and so forth. For this reason, it is important to limit access to a computer's input and output devices to just those that are needed for business purposes. This includes not just expansion ports like USB ports, but access to the power switch, keyboard and mouse, floppy diskette drive, CD and DVD drives, or other parts of the computer.

In some instances, a physical enclosure may not restrict access to these devices, but it may still be possible to install physical covers on devices to block access to unused ports. If this is not possible, you may still be able to disable them in the computer's BIOS settings and then password-protect access to the BIOS. As a last resort, it may be necessary to open the computer up and disconnect the cabling for them.

Controlling physical access to the computer's ports may be less important if the computer is in an area not accessible to the public and only available for use by trusted staff; however, it is still a good idea to think about how to protect it not just from theft, but also against loss from fire, flood or other forms of damage.

Securing Windows XP with Microsoft's built-in tools

As mentioned above, the Microsoft Windows XP of 2014 is very different from the version that shipped in 2001. While a large number of changes to Windows XP's security were made in 2007 with the release of Service Pack 2, there were still limits to how much could be changed without breaking compatibility with then-existing software applications[70]. Fortunately, because you are in charge of this final deployment of Windows XP, you have the opportunity to tighten up all the security settings beyond what Microsoft could do *en masse*.

Configuring accounts as User for more security

If you have just created a new installation of Microsoft Windows XP for long-term usage, then it is likely your account has Administrator privileges. Accounts with Administrator privileges have the ability to make changes that affect all users on the computer, as well as to the operating system. While this might not sound especially dangerous, it actually is one of the largest security issues—if not *the* largest—that has faced Windows XP since it was introduced.

While creating new users accounts with Administrator privileges made it easier for users to install new hardware and software and configure their systems, and may have seemed like a good idea when Windows XP was introduced in 2001, it also meant that if a user accidentally executed a virus, worm, trojan horse or other malicious program, that the malware would effectively have complete access to the computer without having to trick the user into granting them through social engineering or via sophisticated techniques to escalate its privileges. From then on, the malware—not the user—had effective control of the computer.

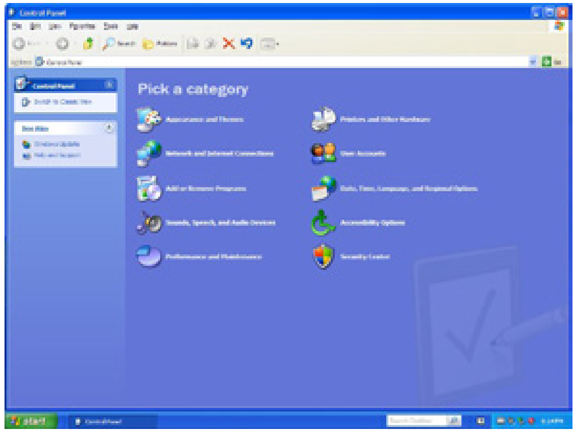
With this in mind, one of the most important steps you can take to secure a computer is to remove Administrator privileges from the accounts that will regularly access the computer and change them to have only User privileges.

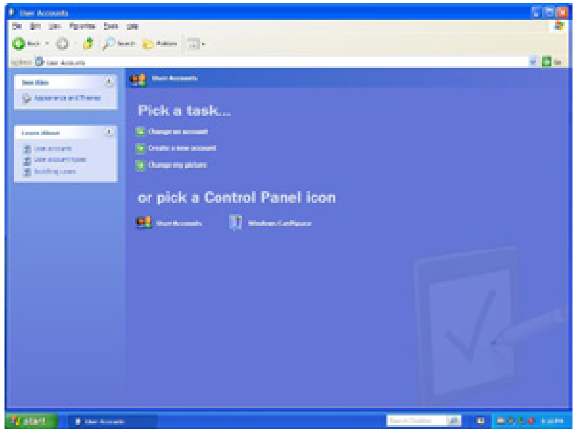
WARNING	Your computer probably has an account named Administrator, which has Administrator privileges. Do not change the privileges on this account. There should be at least one account on the computer with Administrator privileges, in order to allow you to install (or update) software, connect to a network, perform backups and other administrative functions. However, you should avoid using accounts with administrator privileges for routine computer use.

[70] Microsoft. "Release notes for Windows XP Service Pack 2." Microsoft Corp. http://support.microsoft.com/kb/835935.

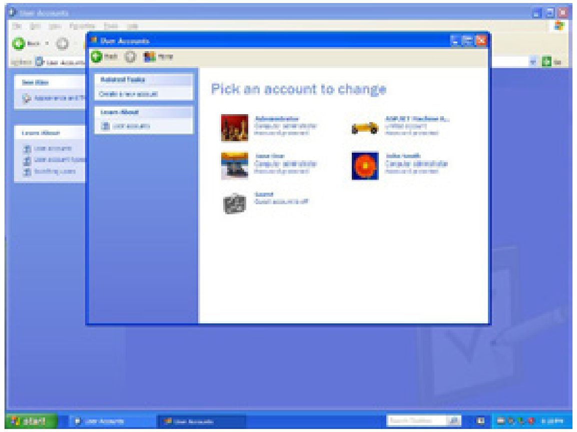
We will go over how change an account from Administrator to User privileges, step-by-step, below:

1. Open the **Control Panel** from the Start Menu, and select the *User Accounts* category. The ***User Accounts Control*** Panel applet (filename: `LUSRMGR.CPL`) will start.

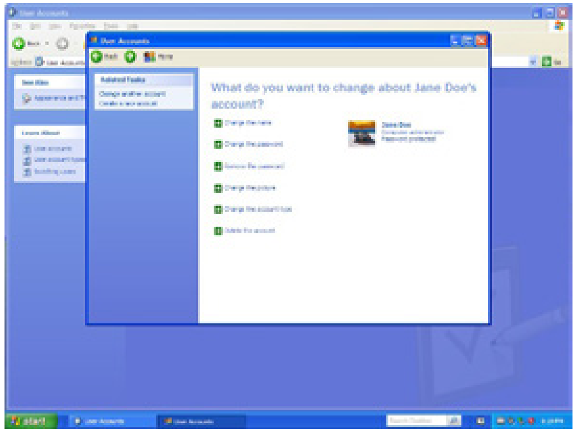

Control Panel
Pick a category
Appearance and Themes
Printers and Other Hardware
Network and Internet Connections
User Accounts
Add or Remove Programs
Date, Time, Language, and Regional Options
Sounds, Speech, and Audio Devices
Accessibility Options
Performance and Maintenance
Security Center
start



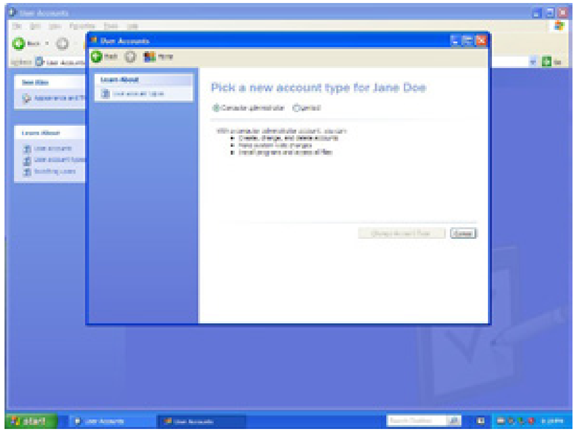
2. In the **User Accounts** applet, select *Change an account*. The *Pick an account to change* window will appear.



3. In the *Pick an account to change* window, select the account to change. The *What do you want to change about* Username's *account* window will appear.



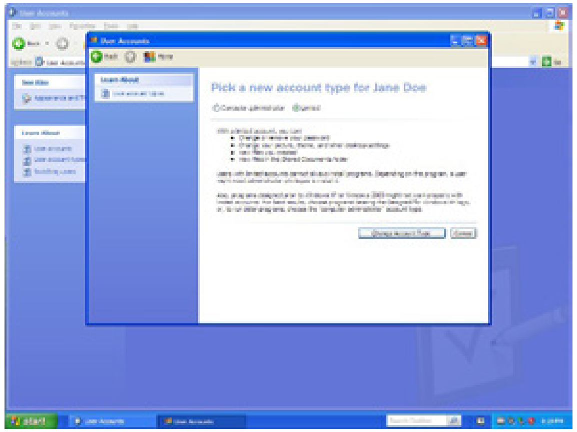
4. In the *What do you want to change about* Username's *account* window, select the *Change the account type* option. The *Pick a new account type for User* window will appear.



Pick a new account type for Jane Doe

● Computer administrator ○ Limited

5. In the Pick a new account type for User window, select "Limited" and click on the ***Change Account Type*** button to make the change.



Pick a new account type for Jane Doe

○ Computer administrator ● Limited

In this example, the account has now been changed from an "Administrator" account to a "User" account

TIP	If you are running a Professional or Tablet PC edition of Microsoft Windows XP, you can use the **Local User and Groups** MMC snapin (filename: `LUSRMGR.MSC`) to perform these steps, instead. This will probably be quicker, especially if there are multiple accounts that need to have their privileges changed.

Applications that are properly written for Microsoft Windows XP should not normally require that the account running them have Administrator privileges. It is possible that an application may need to perform an action that *does* require Administrative privileges, or it may be that the application is not properly written. In either case, if you do find yourself needing Administrative privileges in order to run whatever legacy application you need Windows XP for, consider the following two options:

1. *Create a dedicated Administrator-privilege account to log into when the application needs to be run. This works best if the application only needs to be run periodically, such as at the end of the business day or work week, due to the aforementioned security issues with being logged in using Administrator privileges.*
   While it is a best practice to rename the Administrator account to something other than Administrator, the application may require the account to have this name and fail to work if the account is renamed or attempts are made to run the program using an Administrator-privilege account with a different name. If this is the case, allow the program to use the account, but create another Administrator-privilege account for performing all other activities requiring Administrator privileges.

2. *Consider using the Microsoft Windows **RunAs** command to start the application with Administrator privileges[71, 72, 73]. The user will be prompted to enter credentials with Administrator privileges in order to run the application.*

WARNING Although Administrator privilege credentials can be saved with **RunAs** under Microsoft Windows XP to bypass the prompting for credentials, this is not recommended because once enabled, it allows ***any other program*** to be run with Administrator privileges—a major security issue[74].

Disabling AutoRun

As mentioned above in the section *A Very Brief Overview of Windows XP's Security History*, Microsoft Windows XP's AutoRun feature met with the Law of Unintended Consequences when it was adopted not only by educational software and game developers but also by malware authors. While for some time before Microsoft Windows XP was released, computer worms had been seen attacking Windows in various forms (malicious programs running on the operating system, macros for Microsoft Office and even as self-replicating instructions to database servers), they relied on network connections to spread.

The changes made to AutoRun in Windows XP gave malware authors an additional mechanism for spreading their creations, by writing worms that could spread from computer to computer by using USB flash drives as their infection vector[75, 76]. While network connections continued to be used to spread worms, AutoRun functionality provides worms an additional mechanism for spreading—and often re-infecting—groups of computers, regardless of whether they are directly networked to each other.

How does AutoRun work?

To understand why this was so problematic, it's important to have an understanding of how AutoRun originally worked under Microsoft Windows XP:

When removable media, such as a CD-ROM, DVD or USB flash drive, was inserted into a computer running Windows XP, the operating system checked to see if there was a file named `AUTORUN.INF` in the root directory of the removable drive[77, 78].

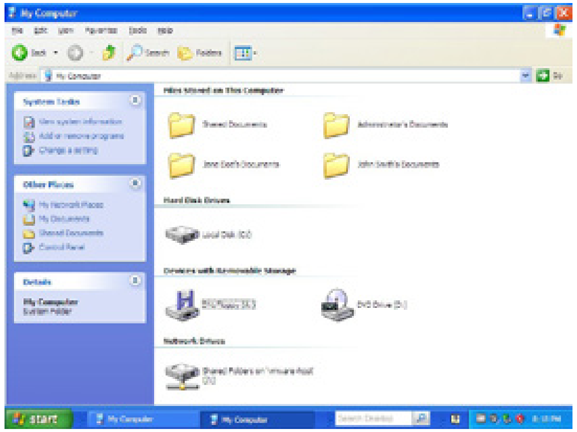


Figure 9: Example of a CD inserted into PC without an AUTORUN.INF file.

[71] Microsoft. "Runas." Microsoft TechNet. http://technet.microsoft.com/en-us/library/cc771525.aspx.

[72] Microsoft. "Runas." Windows XP Command Line Reference A-Z. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-xp/bb490994(v=technet.10).

[73] Wikipedia. "Runas." http://en.wikipedia.org/wiki/Runas.

[74] Barizien, Stephane. "RUNAS /SAVECRED is a huge security hole." NTBUGTRAQ mailing list. https://marc.info/?l=ntbugtraq&m=105949766325326&w=2.

[75] Abrams, Randy. "Foil Conficker Get Rid of AutoRun." WeLiveSecurity. https://www.welivesecurity.com/2009/03/25/foil-conficker-get-rid-of-autorun/

[76] Cobb, Stephen. "My Little Pronny: Autorun worms continue to turn." WeLiveSecurity. http://www.welivesecurity.com/2012/12/07/autorun-worm-continues-to-turn/.

[77] Microsoft. "Autorun.inf Entries." Windows Dev Center. http://msdn.microsoft.com/en-us/library/windows/desktop/cc144200%28v=vs.85%29.aspx.

[78] Wikipedia. "Autorun.inf." Wikimedia Foundation. https://en.wikipedia.org/wiki/Autorun.inf.

AUTORUN.INF files are just plain ASCII text files that can be created in an application like Notepad, but they contain instructions that the operating system follows automatically.

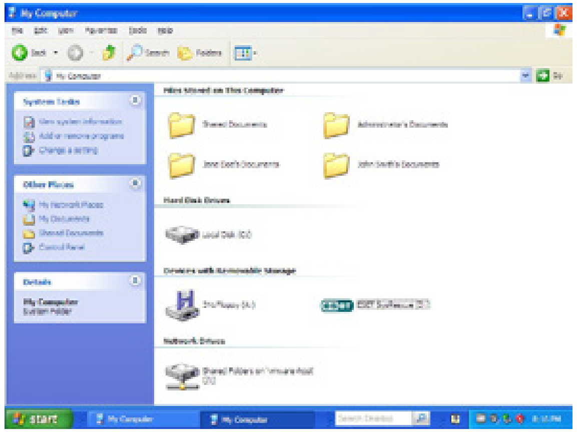


Figure 10: Example of a CD inserted into PC with an AUTORUN.INF file.

The actions controlled through the AUTORUN.INF file can vary from displaying a custom icon for the removable media to helping install device driver software, but the command most favored by malware authors was to run a program automatically[79].

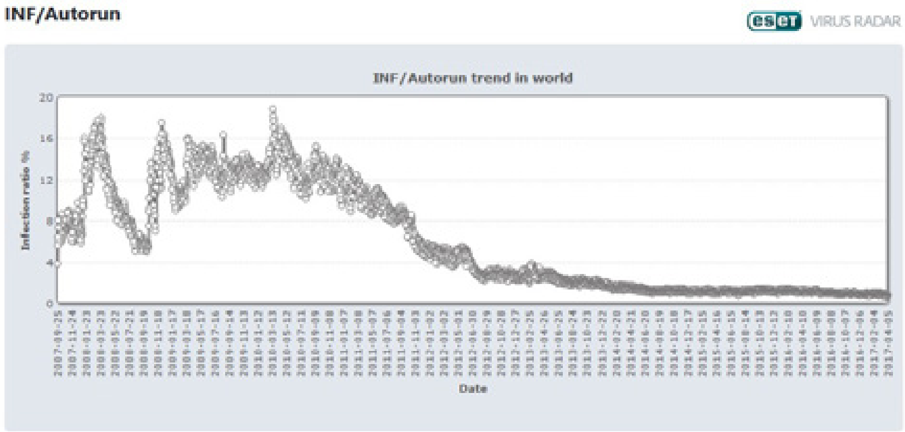


Figure 11: Ten years of detections of Autorun malware

This simple action gave malware authors the foothold they needed to spread their creations, and they took advantage of it. ESET identifies malware using AUTORUN.INF files as **[INF/Autorun](http://virusradar.com/en/INF_Autorun/detail)**[80]. Looking at detections from the past decade using ESET's VirusRadar®, it became the most-reported infection in 2007 and spiked in 2008 as the infection technique was used by Conficker and other worms[81]. It was not until 2010 that it began to decrease, due not only to the rapid adoption of Microsoft Windows 7, but also to the release of patches by Microsoft that, by default,

[79] Windows Dev Center. "Autorun.inf Entries." Microsoft Corp. https://msdn.microsoft.com/en-us/library/windows/desktop/cc144200.aspx.

[80] VirusRadar Threat Encyclopaedia. "INF/Autorun." ESET, spol. s r.o. http://virusradar.com/en/INF_Autorun/detail.

[81] Abrams, Randy. "Foil Conficker Get Rid of AutoRun." WeLiveSecurity. https://www.welivesecurity.com/2009/03/25/foil-conficker-get-rid-of-autorun/.

disabled AutoRun for removable media in Windows Vista and Windows XP[82, 83, 84, 85].

To disable the AutoRun functionality in Microsoft Windows XP, download and install the *Update to the AutoPlay functionality in Windows* update released by Microsoft from:

https://support.microsoft.com/?kbid=971029

This web page contains patches not just for all editions of Windows XP, but also for Windows Vista, Windows Server 2003 and Windows Server 2008. As with many patches, a reboot may be required in order for the changes made to the operating system to take effect.

Enabling Data Execution Prevention

With the release of Windows XP Service Pack 2 in 2004, Microsoft introduced a feature called Data Execution Prevention (DEP)[86, 87, 88]. DEP allows the computer to mark whether a block of memory, called a *page*, holds executable program code, or non-executable data, and only allows code to be run from memory pages marked as executable. Before the introduction of DEP, attackers could load code into a page of memory intended for data and then trigger its execution. Implementing DEP in the computer's hardware and software can prevent these kinds of attacks from succeeding[89].

There are several components to DEP under Windows:

- *A compatible processor must be installed which supports using a "No eXecute" (NX) bit[90]. The NX bit is used to flag whether a memory page contains code or data. Originally developed by chip maker AMD for its Athlon 64 line of processors in 2003, the technology was licensed to other CPU manufacturers including Intel, who added it to their Pentium 4 line in 2004. Chip manufacturers refer to the NX bit in slightly different ways: Intel calls it the XD bit (eXecute Disable) bit, while AMD calls it the Enhanced Virus Protection (EVP) bit. If you are trying to determine if a particular processor supports the NX bit but does not mention it by that name, check to see if XD or EVP are mentioned, instead.*
- *An operating system that supports the NX bit must be installed. In the case of Microsoft Windows XP, this means installing Service Pack 2 or Service Pack 3. Beginning with Windows Vista, DEP support is a standard feature of the operating system.*

By default, Microsoft enabled DEP only for core parts of Windows XP, and used an opt-in model for the rest of the computer's programs. This was done out of concern for compatibility issues with third-party programs,

[82] Riley, Steve. "Autorun: good for you?" Microsoft TechNet. *https://blogs.technet.microsoft.com/steriley/2007/09/23/autorun-good-for-you/*.

[83] Abrams, Randy. "Auto-Infect." WeLiveSecurity. *https://www.welivesecurity.com/2007/12/18/auto-infect/*.

[84] Microsoft. "Update to the AutoPlay functionality in Windows." Microsoft Corp. *https://support.microsoft.com/en-us/help/971029/update-to-the-autoplay-functionality-in-windows*.

[85] Harley, David. "Autorun and Conficker note dead yet: Threat Trends Report." WeLiveSecurity. *https://www.welivesecurity.com/2012/01/10/autorun-and-conficker-not-dead-yet-threat-trends-report/*.

[86] Windows Dev Center. "Data Execution Prevention." Microsoft Corp. *https://msdn.microsoft.com/en-us/library/windows/desktop/aa366553*

[87] Wikipedia. "Executable space protection." WikiMedia Foundation. *https://en.wikipedia.org/wiki/Executable_space_protection*

[88] Microsoft. "A detailed description of the Data Execution Prevention (DEP) feature in Windows XP Service Pack 2, Windows XP Tablet PC Edition 2005, and Windows Server 2003." Microsoft Corp. *https://support.microsoft.com/en-us/help/875352/a-detailed-description-of-the-data-execution-prevention-dep-feature-in-windows-xp-service-pack-2-windows-xp-tablet-pc-edition-2005-and-windows-server-2003*.

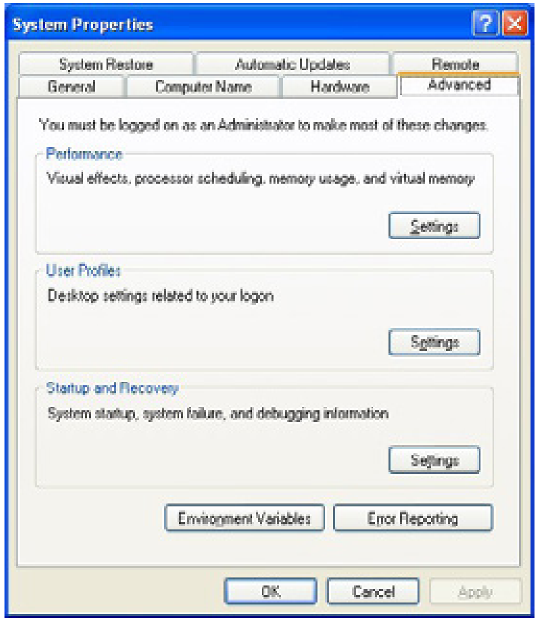
[89] Hensing, Robert. "Understanding DEP as a mitigation technology part 1." Microsoft TechNet. *https://blogs.technet.microsoft.com/srd/2009/06/12/understanding-dep-as-a-mitigation-technology-part-1/*.

[90] Wikipedia. "NX bit." Wikimedia Foundation. *https://en.wikipedia.org/wiki/NX_bit*.

services and device drivers. However, with DEP being a standard feature of Windows XP since 2004, it is recommended that you enable DEP for **all** programs and then exclude any applications which are incompatible, should there be any[91, 92].

Here are step-by-step instructions for enabling Data Execution Prevention for all programs in Windows XP:

1. Open the **System Properties** applet (filename: `SYSDM.CPL`) in the Control Panel. The *System Properties* window will appear.



You must be logged on as an Administrator to make most of these changes.

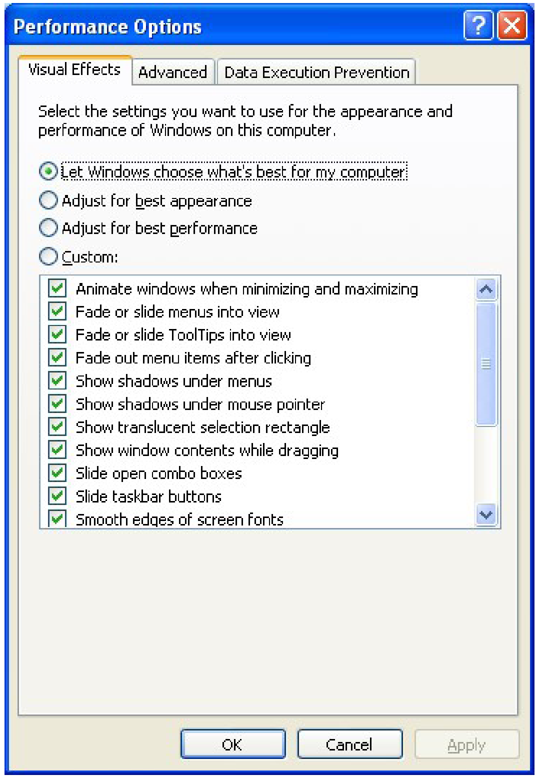
Performance
Visual effects, processor scheduling, memory usage, and virtual memory

User Profiles
Desktop settings related to your logon

Startup and Recovery
System startup, system failure, and debugging information

2. Click on the ***Advanced*** tab to view the advanced settings for the system.

3. In the *Performance* section at the top of the ***Advanced*** tab, click on the *Settings* button. The *Performance Options* window will appear.



Select the settings you want to use for the appearance and performance of Windows on this computer.

● Let Windows choose what's best for my computer
○ Adjust for best appearance
○ Adjust for best performance
○ Custom:

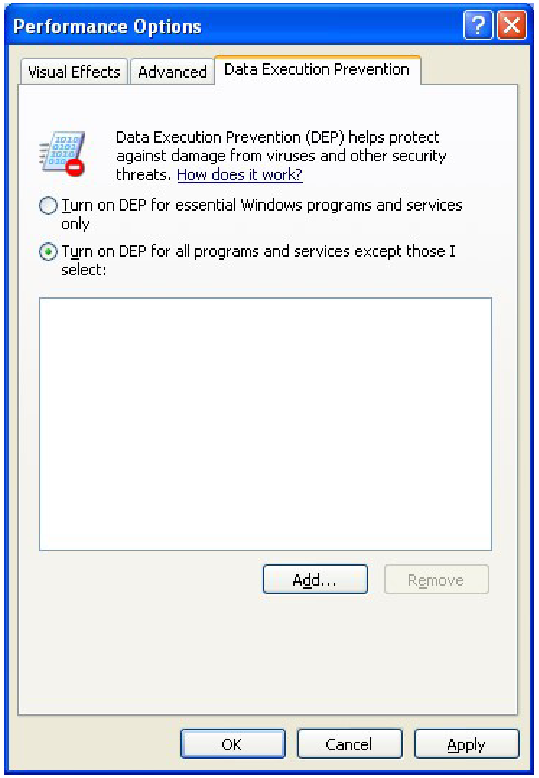
☑ Animate windows when minimizing and maximizing
☑ Fade or slide menus into view
☑ Fade or slide ToolTips into view
☑ Fade out menu items after clicking
☑ Show shadows under menus
☑ Show shadows under mouse pointer
☑ Show translucent selection rectangle
☑ Show window contents while dragging
☑ Slide open combo boxes
☑ Slide taskbar buttons
☑ Smooth edges of screen fonts

4. In the *Performance Options* window, click on the ***Data Execution Prevention*** tab to view the settings for DEP.

[91] Microsoft. "You receive a "Data Execution Prevention" error message in Windows XP Service Pack 2 or in Windows XP Tablet PC Edition 2005." Microsoft Corp. *https://support.microsoft.com/en-us/help/875351/you-receive-a-data-execution-prevention-error-message-in-windows-xp-se*

[92] Hameed, C.C. "To DEP or not to DEP." Microsoft Ask the Performance Team Blog. *https://blogs.technet.microsoft.com/askperf/2008/06/17/to-dep-or-not-to-dep/*

5. Select *Turn on DEP for all programs and services except those I select:*. If you have any programs that are incompatible with DEP, click on the ***Add*** button and add them to the exclusion list. Click on the ***OK*** button when finished to make the changes to the system.



Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?

○ Turn on DEP for essential Windows programs and services only

● Turn on DEP for all programs and services except those I select:

A reboot will be required for these changes made to Windows XP to take effect.

Before we move on, it should be noted that Data Execution Prevention is not infallible. Several vulnerabilities have been discovered that allowed DEP to be bypassed, causing Microsoft to issue patches to fix these vulnerabilities[93, 94, 95, 96]. This does not mean that it should be disabled, though, just because it isn't 100% effective. Enabling Data Execution Prevention provides an additional layer of security, and when using an unsupported operating system such as Windows XP, it is important to take as many defensive steps as are practical.

Configuring Windows File Explorer to show file extensions

Microsoft has made many changes to Windows over the years, from the first release of Windows 1.0 in 1985 to Windows 10 in 2015. Some of the biggest changes occurred to the user interface when switching from Windows for Workgroups 3.11 to Windows 95, which introduced users to the Start Menu and Windows Desktop metaphor, which were tweaked from version to version, but remained largely unchanged until Windows 8 was released in 2012.

In some cases, decisions were made to make Windows more user-friendly at the expense of reducing its security. There is always a trade-off involving ease-of-use over security, and such choices were likely to be fueled in part because attack vectors were not clearly understood when these decisions

[93] Ness, Jonathan. "Additional information about DEP and the Internet Explorer 0day vulnerability." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2010/01/18/additional-information-about-dep-and-the-internet-explorer-0day-vulnerability/.

[94] Roths, Andrew; et al. "DEP, EMET protect against attacks on the latest Internet Explorer vulnerability." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2010/11/03/dep-emet-protect-against-attacks-on-the-latest-internet-explorer-vulnerability/.

[95] Miller, Matt. "On the effectiveness of DEP and ASLR." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2010/12/08/on-the-effectiveness-of-dep-and-aslr/.

[96] Miller, Matt; Peteroy, William. "Mitigating the LdrHotPatchRoutine DEP/ASLR bypass with MS13-063." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2013/08/12/mitigating-the-ldrhotpatchroutine-depaslr-bypass-with-ms13-063/.

were made. One example of this is the AutoRun feature in Microsoft Windows XP discussed above. Another example is **Windows Explorer**'s (filename: `EXPLORER.EXE`) default settings for viewing files.

In Windows 3.x, the **File Manager** (filename: `WINFILE.EXE`) was used to view directories and launch programs[97]. It showed the files in a directory including their names, file extensions and small icons giving an indication of their file type handler, *e.g.*, the type program used to open the file, as applicable.

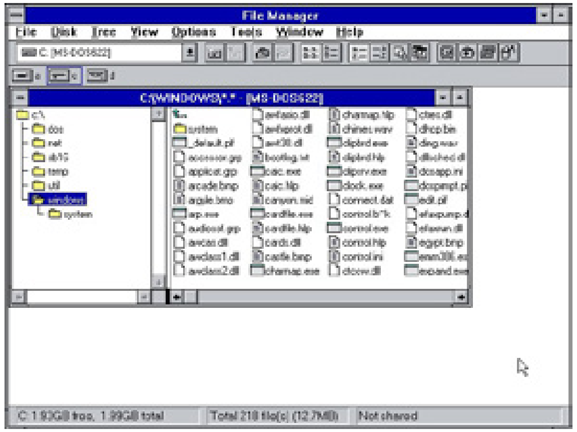

File Manager
File Disk Tree View Options Tools Window Help
C: [MS-DOS622]
C:\WINDOWS\*.* - [MS-DOS622]
c:\
dos
net
qb45
temp
util
windows
system
C: 1.93GB free, 1.99GB total
Total 218 file(s) (12.7MB)
Not shared

Figure 12: Windows for Workgroups 3.11 File Manager

While this made a good amount of sense for the business-oriented world of Windows 3.*x*, it was seen as being a less-friendly way of viewing files than that used by the Apple Macintosh, which made use of information stored inside of files to determine which icons were displayed and which applications opened them[98], [99], [100], [101]. In an attempt to make Windows 95 appeal to consumers by looking more friendly and to copy the Macintosh's simplicity, Microsoft made the decision to not display file extensions by default when viewed in Windows Explorer, the successor to Windows 3.x's File Manager. Explorer does, however, still display an icon based on either the file's extension, or an icon embedded as a resource within the file. Showing files in this fashion has been the default behavior for Windows and has remained unchanged for over twenty years, since Microsoft's release of Windows 95 in 1995.

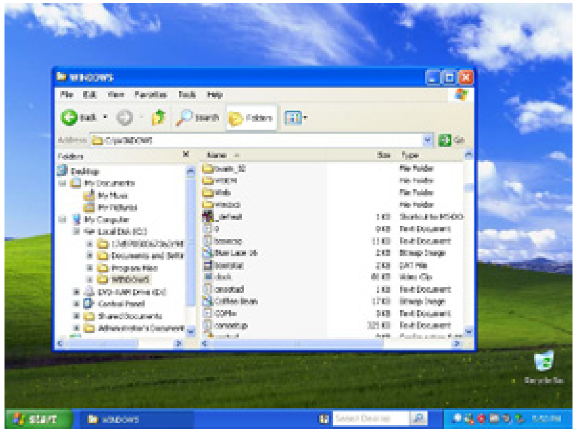


Figure 13: Microsoft Windows XP's Explorer

[97] Wikipedia. "File Manager (Windows)." Wikimedia Foundation. https://en.wikipedia.org/wiki/File_Manager_(Windows).

[98] Sanford, Glen D. "apple-history." Apple History. http://www.apple-history.com/.

[99] Mac 512, The. "System Showcase." The Mac 512. http://www.mac512.com/macwebpages/system.htm

[100] Wikipedia. "Macintosh." Wikimedia Foundation. https://en.wikipedia.org/wiki/Macintosh.

[101] Wikipedia. "Classic Mac OS." Wikimedia Foundation. https://en.wikipedia.org/wiki/Classic_Mac_OS.

Why is hiding file extensions such a problematic security issue, you might ask? The reason is that it is easy to create files with a doubled file extension—a “fake” extension followed by the real file extension—and as a result of this default setting, Explorer shows only the fake file extension.

As an example, creating a file with the name “`My Notes.txt`” means that it contains text, and is opened by Windows’ default text file editor, **Notepad** (filename: `NOTEPAD.EXE`). With Explorer’s default view set to not show extensions, the file just shows as up as “`My Notes`” on the computer. Creating a file with a doubled file extension such as “`My Notes.txt.exe`” means the **`.txt`** portion will be displayed in Explorer, while the **`.exe`** portion remains hidden.

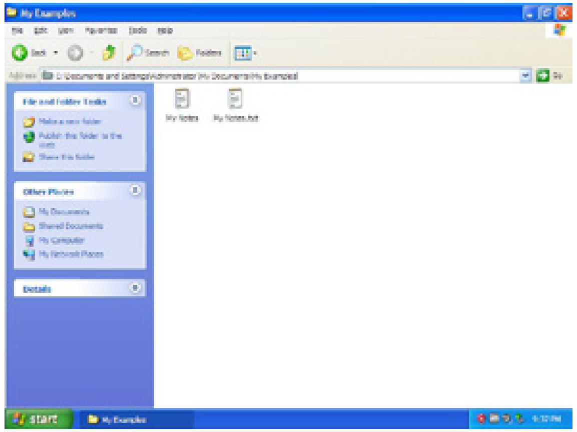
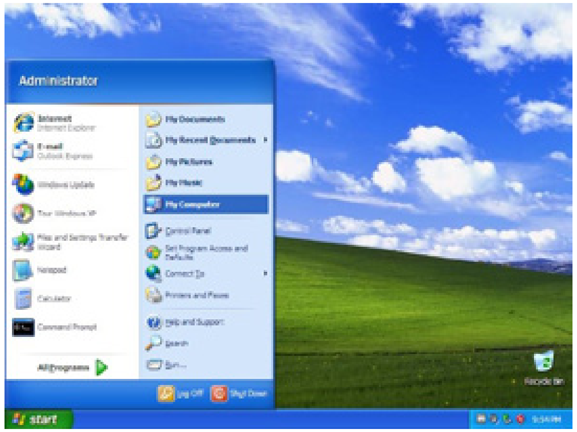


Figure 14: Showing seemingly identical files in Explorer

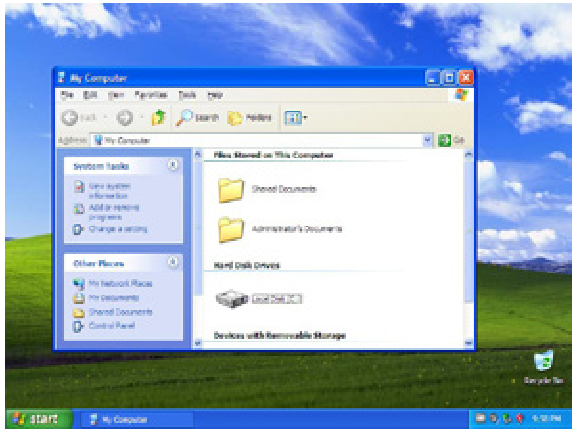
Over the years, this default setting, originally meant to make Microsoft Windows XP more friendly, has tricked hundreds of millions of people into accidentally running malicious programs, infecting their computers, and causing economic loss so high as to be nigh incalculable.

There is a simple solution to this security vulnerability, and that is to turn on the display of file extensions in Windows Explorer. Here are step-by-step instructions for doing so:

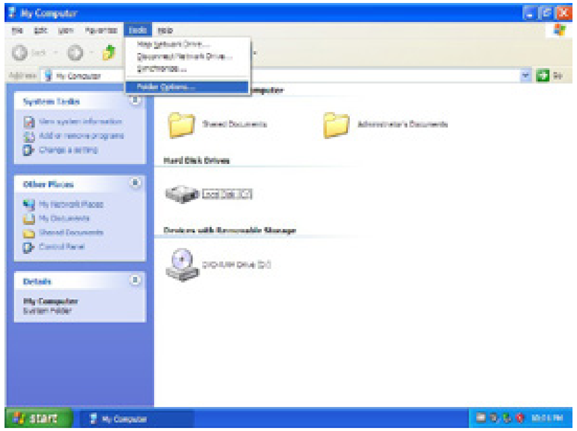
1. Click on the **Start** button and select ***My Computer*** to open Windows Explorer.



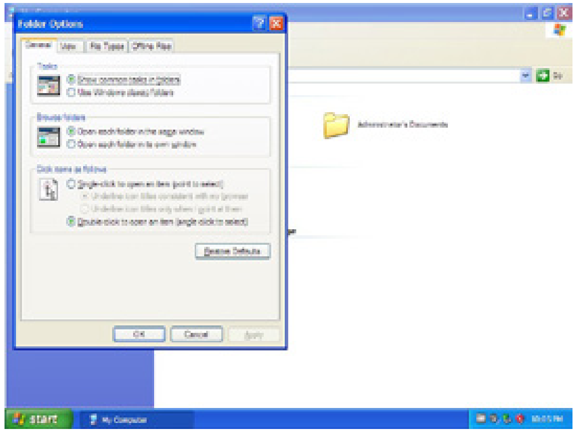
Windows Explorer will appear:


My Computer
System Tasks
Other Places
Files Stored on This Computer
Shared Documents
Administrator's Documents
Hard Disk Drives
Devices with Removable Storage
start

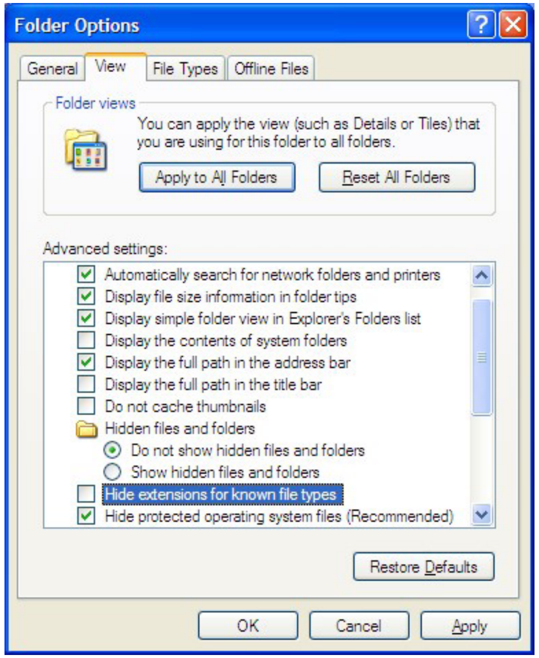
2. Select *Tools* → *Folder Options* from the main menu bar.



The ***Folder Options*** properties pane will appear.


Folder Options
General View File Types Offline Files
Tasks
Show common tasks in folders
Use Windows classic folders
Browse folders
Open each folder in the same window
Open each folder in its own window
Click items as follows
Single-click to open an item (point to select)
Double-click to open an item (single-click to select)
Restore Defaults
OK Cancel Apply
Administrator's Documents
start
My Computer

3. In the ***Folder Options*** properties pane, de-select (uncheck) the *Hide extensions for known file types* option.



You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

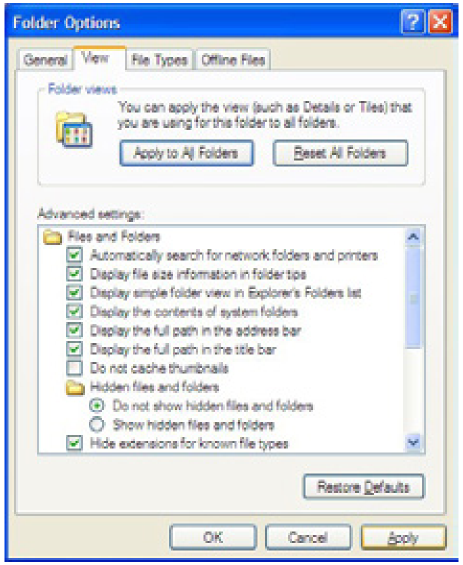
☑ Automatically search for network folders and printers
☑ Display file size information in folder tips
☑ Display simple folder view in Explorer's Folders list
□ Display the contents of system folders
☑ Display the full path in the address bar
□ Display the full path in the title bar
□ Do not cache thumbnails
Hidden files and folders
● Do not show hidden files and folders
○ Show hidden files and folders
□ Hide extensions for known file types
☑ Hide protected operating system files (Recommended)

We strongly recommend that you change the following settings as well:

- *select (check) Display the contents of system folders*
- *select (check) Display the full path in the title bar*
- *select the Show hidden files and folders radio button (beneath Hidden files and Folders)*
- *de-select (uncheck) Hide protected operating system files (Recommended)*

NOTE: You may want to make other changes as well for reasons of productivity or convenience.

4. When finished making changes, click on the ***Apply*** button to make the change to how the **current** folder is viewed, then the ***Apply to All Folders*** button to make the change to how **all** folders are viewed by the user. Click on the ***OK*** button when done.



Folder Options

General | View | File Types | Offline Files

Folder views

You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

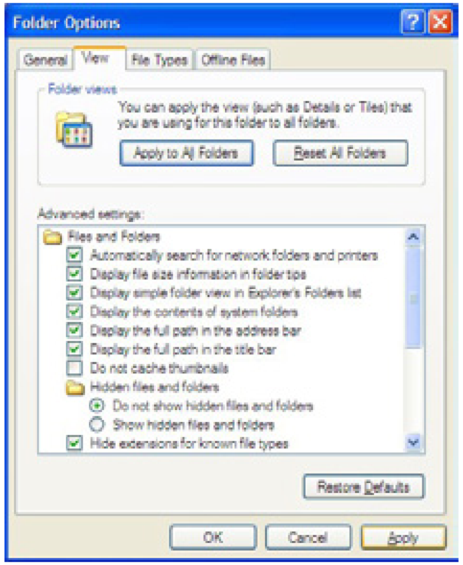
Apply to All Folders | Reset All Folders

Advanced settings:

- Files and Folders
  - ☑ Automatically search for network folders and printers
  - ☑ Display file size information in folder tips
  - ☑ Display simple folder view in Explorer's Folders list
  - ☑ Display the contents of system folders
  - ☑ Display the full path in the address bar
  - ☑ Display the full path in the title bar
  - □ Do not cache thumbnails
  - Hidden files and folders
    - ● Do not show hidden files and folders
    - ○ Show hidden files and folders
  - ☑ Hide extensions for known file types

Restore Defaults

OK | Cancel | Apply



Folder Options

General | View | File Types | Offline Files

Folder views

You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Apply to All Folders | Reset All Folders

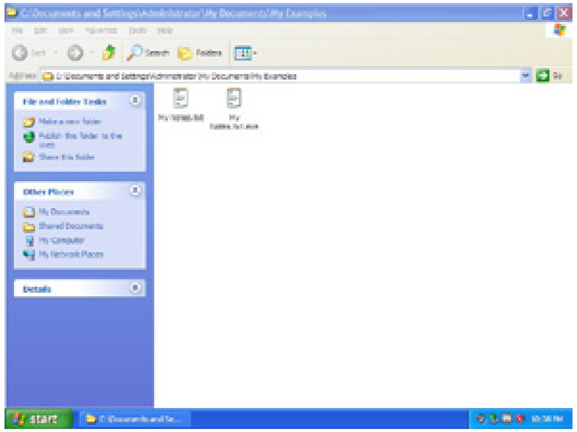
Advanced settings:

- Files and Folders
  - ☑ Automatically search for network folders and printers
  - ☑ Display file size information in folder tips
  - ☑ Display simple folder view in Explorer's Folders list
  - ☑ Display the contents of system folders
  - ☑ Display the full path in the address bar
  - ☑ Display the full path in the title bar
  - □ Do not cache thumbnails
  - Hidden files and folders
    - ● Do not show hidden files and folders
    - ○ Show hidden files and folders
  - ☑ Hide extensions for known file types

Restore Defaults

OK | Cancel | Apply

If you now view a folder in Windows Explorer, files will now be shown with their extensions. Here is the same folder shown in Figure 16 once the changes listed above have been made:



C:\Documents and Settings\Administrator\My Documents\My Examples

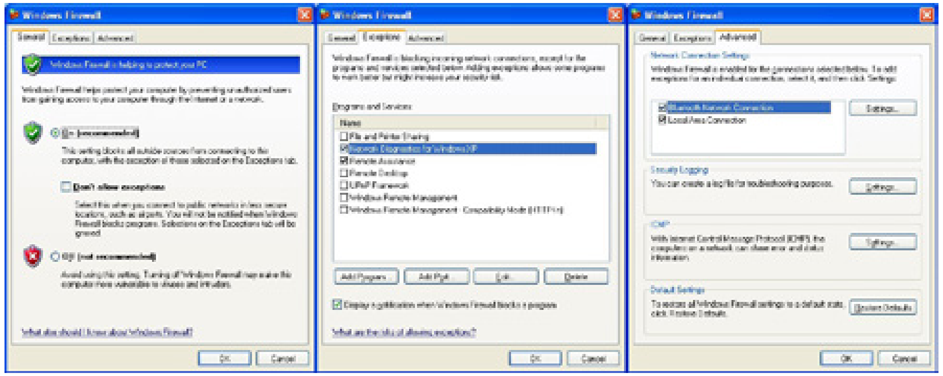
Figure 15: Showing file extensions helps identify files

As is typical with changes to the operating system under Windows XP, a reboot may be required for the changes to take effect.

TIP	Advanced users comfortable with editing the Windows system registry can make this change by using **REG.EXE** to enter the following single line from a Command Prompt: `REG.EXE ADD HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v "HideFileExt" /t REG_DWORD /d "0" /f` Use "/d" to set the DWORD value of `HideFileExt` to **1** to hide file extensions, or to **0** to show file extensions.

Windows Firewall

Under Windows XP, the Windows Firewall (also known as the Internet Connection Firewall before being renamed in Service Pack 2) provides basic protection, allowing incoming network connections to be blocked. This differs from newer versions of Microsoft Windows, where the Windows Firewall is *bidirectional* and can block both incoming **and** outgoing network connections. The Windows Firewall can be accessed by opening the **Control Panel**, opening the **Security Center** by clicking on it, going to the *Manage Security Settings For*: section at the bottom of the window, and selecting *Windows Firewall*. The ***Windows Firewall*** Control Panel applet (filename: `FIREWALL.CPL`) will then start.



○ On (recommended)

□ Don't allow exceptions

○ Off (not recommended)

Programs and Services

□ File and Printer Sharing
☑ Network Diagnostics for Windows XP
☑ Remote Assistance
□ Remote Desktop
□ UPnP Framework
□ Windows Remote Management
□ Windows Remote Management - Compatibility Mode (HTTP:80)

☑ Display a notification when Windows Firewall blocks a program

Network Connection Settings

☑ Bluetooth Network Connection
☑ Local Area Connection

Security Logging

ICMP

Default Settings

Figure 16: Windows Firewall's General, Exceptions and Advanced tabs

Although no computer running Microsoft Windows XP should ever have direct access to the Internet for its own safety and security, access to a local network may still be required for sharing data. The Windows Firewall should be enabled in order to restrict accidental network communications. On the ***General*** tab, selecting *Don't allow exceptions* will block all incoming network connections, except those initiated by the computer.

NOTE: The Windows Firewall under Windows XP is a basic software firewall and is only capable of blocking incoming network connections, not outgoing ones.

Unlike the previous sections where prescriptive guidance was provided, it is not possible to provide such guidance with the Windows Firewall. The firewall's configuration will depend on what sort of network access is needed by the computer in order to perform its specific function (or functions). Review all information for that function to determine which programs require Internet access, and to which servers and on which ports. This information can usually be found in documentation and knowledgebase articles.

If a bidirectional firewall is required, or you are unsure of what servers need to be accessed (and on what ports), use a third-party software firewall, instead. Most third-party software firewalls can be run in an interactive mode that prompts for connections in order to allow you to build the firewall's set of rules for allowing and denying Internet access. Once you have set up the necessary access rules, disable interactivity and place the firewall into a strict mode where only the connections you have set up policies or rules for will be allowed, and all other connections are to be dropped.

NOTE: Software firewalls for computers and hardware firewalls for networks perform different functions. They complement and do not replace each other.

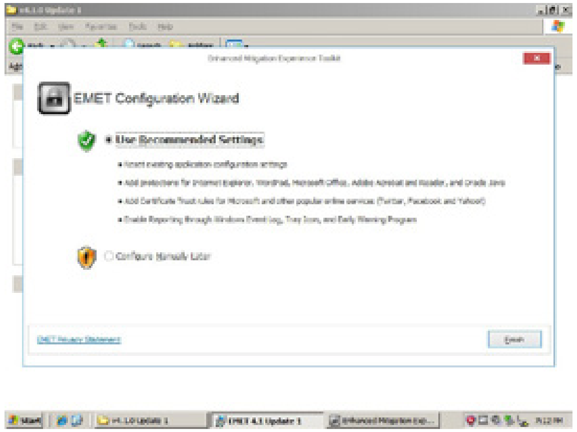
Additional Tools from Microsoft for Securing Windows XP

For any operating system as popular as Microsoft Windows XP was, it was inevitable that a large number of tools would be created to secure it. Some of these were strictly for the enterprise and required specialized training and ongoing maintenance to administer; some of them were specifically for individual home users with a single computer connected directly to the Internet. And some of these tools fell somewhere in between the two.

While we certainly cannot go over every security tool developed for Windows XP during its thirteen-year lifecycle, we can go over a few of the ones that are going to be most useful to mend and defend an unmanaged PC in a small office/home office environment.

Microsoft's Enhanced Mitigation Experience Toolkit

In 2009, Microsoft released the Enhanced Mitigation Experience Toolkit (EMET), a tool to provide an extra layer of prevention against malware[102]. EMET is not an anti-malware program *per se*; it works by applying mitigations to programs for vulnerabilities that otherwise would require them to be recompiled and distributed again[103]. This is particularly useful for programs that have vulnerabilities mitigated by EMET but for which no newer version exists. For these reasons, we recommend using EMET.



Enhanced Mitigation Experience Toolkit

EMET Configuration Wizard

● Use Recommended Settings

- Import existing application configuration settings
- Add protections for Internet Explorer, WordPad, Microsoft Office, Adobe Acrobat and Reader, and Oracle Java
- Add Certificate Trust rules for Microsoft and other popular online services (Twitter, Facebook and Yahoo!)
- Enable Reporting through Windows Event Log, Tray Icon, and Early Warning Program

○ Configure Manually Later

EMET Privacy Statement

Finish

Figure 17: Installing EMET 4.1.0 Update 1 on Windows XP

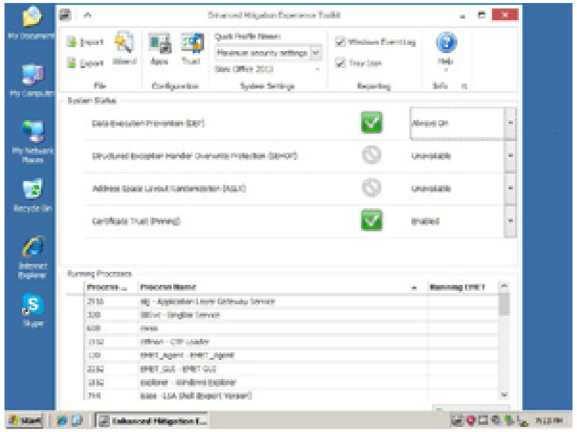
The initial release of EMET supported four mitigations for Windows XP. Each of these counters an exploitation technique, but to explain these techniques in detail is outside the scope of this paper. Here is a list of those exploits, along with links to Microsoft explaining how they operate:

Name	More Information
SEHOP	*Preventing the Exploitation of Structured Exception Handler (SEH) Overwrites with SEHOP*
Dynamic DEP	*Understanding DEP as a mitigation technology part 1*, *Understanding DEP as a mitigation technology part 2*
NULL page allocation	*Null page mitigation*
Heap spray allocation	*Nozzle: Counteracting Memory Exploits*

[102] Serna, Fermin J.; Roths, Andrew. "Announcing the release of the Enhanced Mitigation Tookit." Microsoft TechNet. *https://blogs.technet.microsoft.com/srd/2009/10/27/announcing-the-release-of-the-enhanced-mitigation-evaluation-toolkit/*.

[103] Microsoft. "Enhanced Mitigation Experience Toolkit." Microsoft TechNet. *https://technet.microsoft.com/en-us/security/jj653751*.

In April 2014, Microsoft released the last version of EMET officially compatible with Windows XP, Version 4.1.0 Update 1. In that release, Microsoft had increased the number of mitigations for Windows XP to ten[104, 105].



System Status

Data Execution Prevention (DEP) — Always On

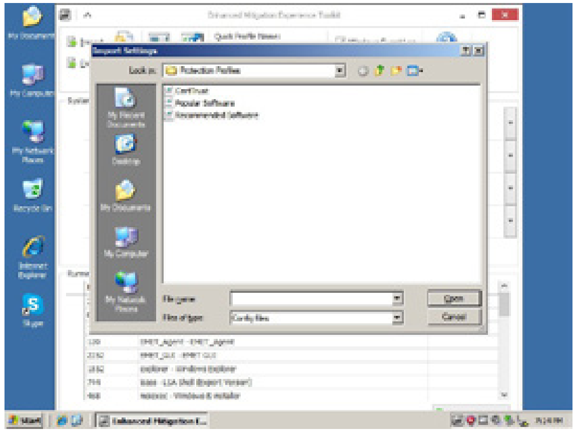
Structured Exception Handler Overwrite Protection (SEHOP) — Unavailable

Address Space Layout Randomization (ASLR) — Unavailable

Certificate Trust (Pinning) — Enabled

Figure 18: Enabling features in EMET

While this is fewer than the number of mitigations available to Windows Vista and newer operating systems, it still provides an additional layer of security to harden Windows XP against attacks.



Import Settings

Look in: Protection Profiles

CertTrust
Popular Software
Recommended Software

Files of type: Config files

Figure 19: Importing Protection Profiles into EMET

When installing EMET, we strongly suggest using Microsoft's recommended default settings, to enable all available features such as *Data Execution Prevention (DEP)* and *Certificate Pinning*, and to import all protection profiles provided by Microsoft. This will ensure that EMET is configured with the highest degree of security possible under Microsoft Windows XP.

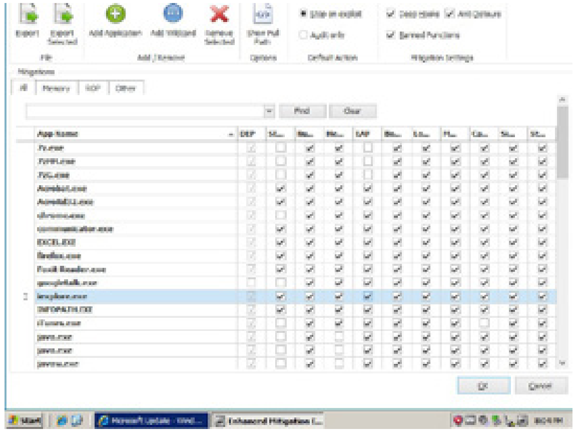


Figure 20: The Apps button opens the Configure Applications in EMET

[104] Microsoft. "Introducing Enhanced Mitigation Experience Toolkit (EMET) 4.1." Microsoft TechNet. https://blogs.technet.microsoft.com/srd/2013/11/12/introducing-enhanced-mitigation-experience-toolkit-emet-4-1/

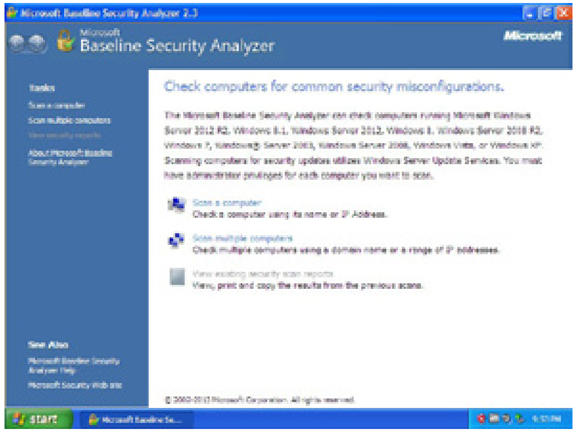
[105] Microsoft. "An update is available for the Enhanced Mitigation Experience Toolkit 4.1: April 2014." Microsoft Corp. https://support.microsoft.com/en-us/help/2964759/an-update-is-available-for-the-enhanced-mitigation-experience-toolkit-4.1-april-2014.

It is possible that one or more applications will be incompatible with mitigations provided by EMET. If this occurs, EMET will display a notification with the name of the program and the mitigation. To resolve this incompatibility close the application, open EMET, go to the ***Apps*** section by pressing `Ctrl+Shift+A`, and deselect (un-check) the mitigation for the application in question.

As with Data Execution Prevention, the Enhanced Mitigation Experience Toolkit is not a panacea nor a substitute for running a newer, more secure version of Windows. There have been several releases after EMET Version 4.1.0 update 1 that fix vulnerabilities and add new mitigations; these, however, are not available under Microsoft Windows XP. EMET cannot make your system invulnerable; what it can do is make it more secure.

Microsoft Baseline Security Analyzer

The Microsoft Baseline Security Analyzer (MBSA) is a tool developed by Microsoft to check for weak security settings as well as to identify any missing security-related updates for the operating system, as well as for Microsoft Office, and for Microsoft's IIS web server and SQL database software[106, 107, 108, 109]. The MBSA is available for desktop versions of Microsoft Windows from Windows 2000 to Windows 8.1 and their server version counterparts.



Check computers for common security misconfigurations.

The Microsoft Baseline Security Analyzer can check computers running Microsoft Windows Server 2012 R2, Windows 8.1, Windows Server 2012, Windows 8, Windows Server 2008 R2, Windows 7, Windows® Server 2003, Windows Server 2008, Windows Vista, or Windows XP. Scanning computers for security updates utilizes Windows Server Update Services. You must have administrator privileges for each computer you want to scan.

Scan a computer
Check a computer using its name or IP Address.

Scan multiple computers
Check multiple computers using a domain name or a range of IP addresses.

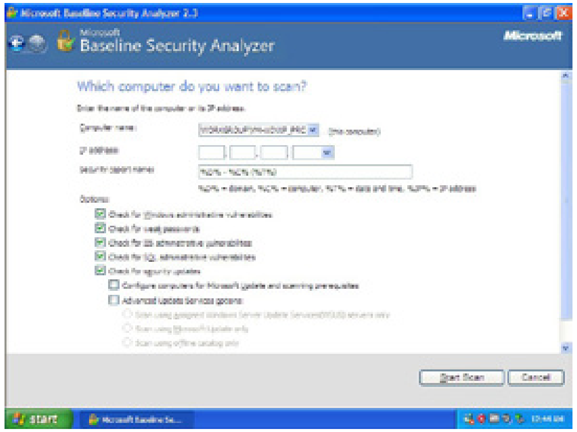
View existing security scan reports
View, print and copy the results from the previous scans.

© 2002-2013 Microsoft Corporation. All rights reserved.

Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
Tasks
Scan a computer
Scan multiple computers
View security reports
About Microsoft Baseline Security Analyzer
See Also
Microsoft Baseline Security Analyzer Help
Microsoft Security Web site
start
Microsoft Baseline Se...

Figure 21: Microsoft Security Baseline Analyzer Version 2.3 running on Windows XP

When *Scan a Computer* is selected, MBSA will ask which computer to scan for security issues, with the default option being the computer on which it is run.



Which computer do you want to scan?

Enter the name of the computer or its IP address.

Computer name: [illegible] (this computer)

IP address:

Security report name: %D% - %C% (%T%)

%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address

Options:

☑ Check for Windows administrative vulnerabilities
☑ Check for weak passwords
☑ Check for IIS administrative vulnerabilities
☑ Check for SQL administrative vulnerabilities
☑ Check for security updates
☐ Configure computers for Microsoft Update and scanning prerequisites
☐ Advanced Update Services options:
○ Scan using assigned Windows Server Update Services(WSUS) servers only
○ Scan using Microsoft Update only
○ Scan using offline catalog only

Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
Start Scan
Cancel
start
Microsoft Baseline Se...

Figure 22: Microsoft Baseline Security Analyzer asking which computer to scan

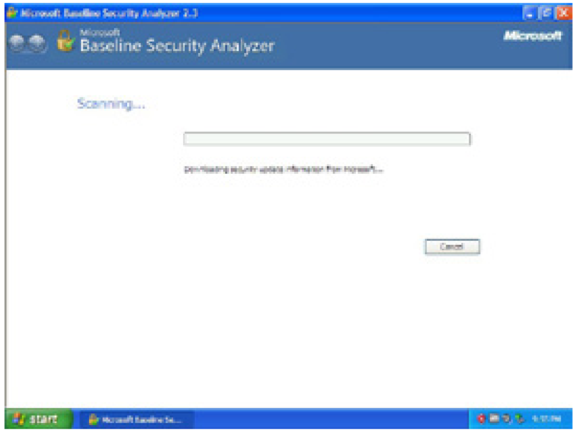
[106] Microsoft. "Microsoft Security Baseline Analyzer." Microsoft TechNet. https://technet.microsoft.com/en-us/security/cc184924.aspx.

[107] Microsoft. "Microsoft Security Baseline Analyzer 2.3 (for IT Professionals)." Microsoft Corp. https://www.microsoft.com/en-us/download/details.aspx?id=7558.

[108] Microsoft. " How To: Use the Microsoft Baseline Security Analyzer." Microsoft Developer Network. https://msdn.microsoft.com/en-us/library/ff647642.aspx.

[109] Wikipedia. "Microsoft Security Baseline Analyzer." Wikimedia Foundation. https://en.wikipedia.org/wiki/Microsoft_Baseline_Security_Analyzer.

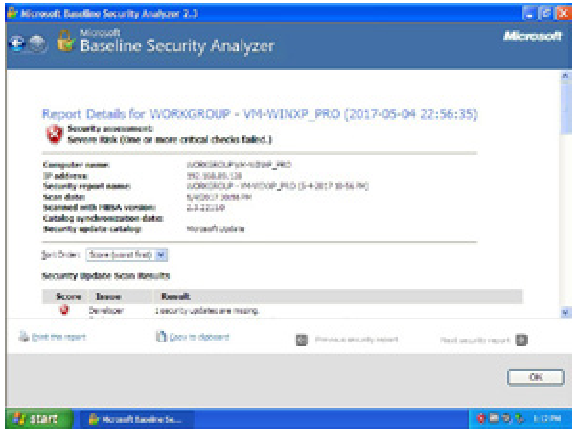
Selecting *Start Scan* will begin checking for missing security-related updates, a process that may take from several minutes to several hours, depending upon the age and speed of the computer and its network connection.



Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft
Scanning...
Downloading security update information from Microsoft...
Cancel
start
Microsoft Baseline Se...

Figure 23: Microsoft Security Baseline Analyzer contacts Microsoft for the latest information

After MSBA updates its security information, it will run and present the user with a report of its findings, which may comprise several screens of information.



Microsoft Baseline Security Analyzer 2.3
Microsoft
Baseline Security Analyzer
Microsoft

Report Details for WORKGROUP - VM-WINXP_PRO (2017-05-04 22:56:35)

Security assessment:
Severe Risk (One or more critical checks failed.)

Computer name:	WORKGROUP\VM-WINXP_PRO
IP address:	192.168.85.128
Security report name:	WORKGROUP - VM-WINXP_PRO (5-4-2017 10-56 PM)
Scan date:	5/4/2017 10:56 PM
Scanned with MBSA version:	2.3.2211.0
Catalog synchronization date:	
Security update catalog:	Microsoft Update

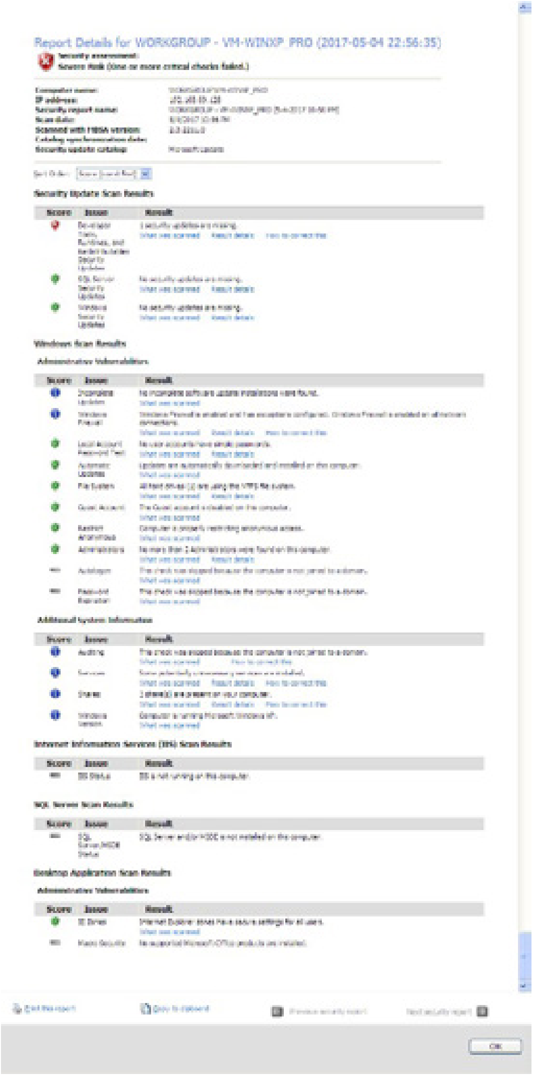
Sort Order: Score (worst first)

Security Update Scan Results

Score	Issue	Result
●	Developer	1 security updates are missing.

Figure 24: The beginning of a completed Microsoft Baseline Security Analyzer report

Depending upon the length, it may be easier to print the report, or copy it and paste it into another application, such as a word processor, for further review.



Report Details for WORKGROUP - VM-WINXP_PRO (2017-05-04 22:56:35)

Security assessment:
Severe Risk (One or more critical checks failed.)

Security Update Scan Results

Windows Scan Results

Administrative Vulnerabilities

Additional System Information

Internet Information Services (IIS) Scan Results

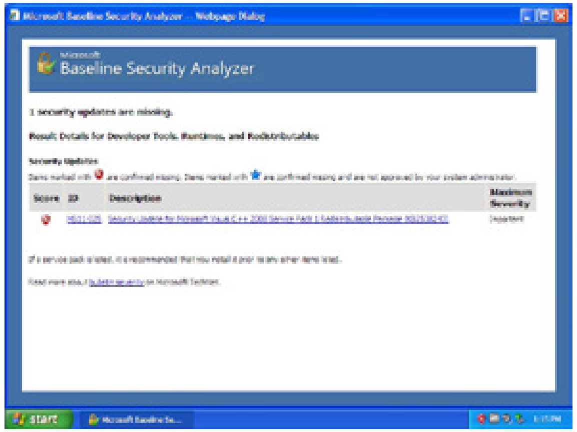
SQL Server Scan Results

Desktop Application Scan Results

Administrative Vulnerabilities

Figure 25: A report from Microsoft Baseline Security Analyzer's may be long.

Clicking on *Result Details* for any entry in the report gives more information about the nature of the issue that was found, such as a missing security update, along with links to security bulletins and download links, as applicable.



Microsoft Baseline Security Analyzer -- Webpage Dialog

Microsoft Baseline Security Analyzer

1 security updates are missing.

Result Details for Developer Tools, Runtimes, and Redistributables

Security Updates

Score	ID	Description	Maximum Severity
	MS11-025	Security Update for Microsoft Visual C++ 2008 Service Pack 1 Redistributable Package (KB2538242)	Important

If a service pack is listed, it is recommended that you install it prior to any other items listed.

Read more about bulletin security on Microsoft TechNet.

Figure 26: Microsoft Baseline Security Analyzer has identified a missing security update

We recommend addressing any security issues found by the Microsoft Baseline Security Analyzer. However, it is also a good idea to make a backup of the system in case one of the updates is incompatible with your computer's hardware or software. More information about backups can be found in the **Backing Up Your Software** section, above.

Microsoft Security Essentials

Microsoft Security Essentials was Microsoft's free anti-malware program that was released in September, 2009 for Windows XP, Windows Vista and Windows 7[110, 111]. Microsoft ceased providing Microsoft Security Essentials for download in April, 2014, but continued to provide updates for already installed copies until July, 2015[112, 113, 114].

Because of the speed at which new threats appear, using an anti-malware program that is several years out of date offers effectively no protection. If the computer running Windows XP has Microsoft Security Essentials installed on it, it should be removed and replaced with reputable anti-malware software that supports Microsoft Windows XP from an established security company.

Tools from Third-Parties for Securing Windows XP

In addition to programs such as Microsoft's own Enhanced Mitigation Experience Toolkit (EMET) and Microsoft Baseline Security Analyzer (MBSA) tools, there are similar tools available from third parties that can help make Windows XP more secure. Belarc and Flexera (formerly Secunia) are among several companies that offer tools that not only check for missing Windows updates, but also for programs such as Adobe Flash and Oracle Java, which are the frequent target of attacks. They may even find updates for Microsoft's own software that the Microsoft Security Baseline Analyzer missed.

Belarc Advisor

Belarc, Inc. is a company that makes system management software for businesses[115]. It also offers a free program for consumers called Belarc Advisor, which inventories the software and hardware, identifies missing Microsoft updates, and provides a security assessment of the computer on which it is run[116]. This is displayed in the form of a report shown in the web browser.

[110] Microsoft. "Get free virus protection with Microsoft Security Essentials." Microsoft Corp. *https://www.microsoft.com/en-us/safety/pc-security/microsoft-security-essentials.aspx*.

[111] Mediati, Nick. "Microsoft Security Essentials Launches Tuesday." PCWorld. *https://www.pcworld.com/article/172762/microsoft_security_essentials_launches_tuesday.html*.

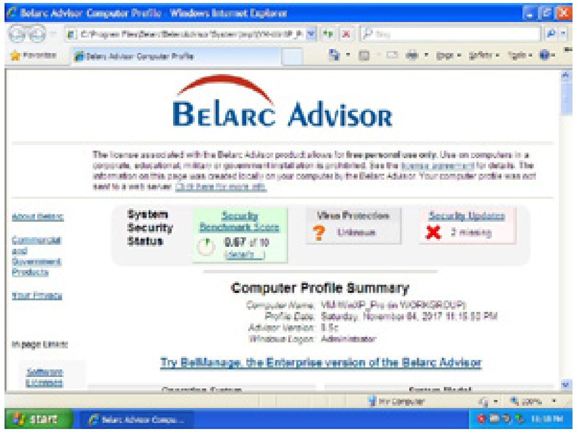
[112] Microsoft. "Microsoft antimalware support for Windows XP." Microsoft Windows Security blog. *https://blogs.technet.microsoft.com/mmpc/2014/01/13/microsoft-antimalware-support-for-windows-xp/*.

[113] Seltzer, Larry. "Microsoft to extend Windows XP anti-malware updates one year." ZDNet. *http://www.zdnet.com/article/microsoft-to-extend-windows-xp-anti-malware-updates-one-year/*

[114] Ringer, Brian H. "End of Updates for (MSE) Microsoft Security Essentials and MSRT (Malicious Software Removal Tool) for Windows XP-July 14, 2015." Microsoft Answers. *https://answers.microsoft.com/en-us/protect/forum/all/end-of-updates-for-mse-microsoft-security/91800f6f-262e-48d0-8be7-7a8f9d768cbf?auth=1*.

[115] Belarc. "About Belarc." Belarc, Inc. *http://www.belarc.com/en/about_us*.

[116] Belarc. "Belarc Advisor." Belarc, Inc. *http://www.belarc.com/en/products_belarc_advisor*.



Belarc Advisor Computer Profile - Windows Internet Explorer

Belarc Advisor

The license associated with the Belarc Advisor product allows for free personal use only. Use on computers in a corporate, educational, military or government installation is prohibited. See the license agreement for details. The information on this page was created locally on your computer by the Belarc Advisor. Your computer profile was not sent to a web server. Click here for more info.

System Security Status — Security Benchmark Score: 0.67 of 10 (details...) — Virus Protection: ? Unknown — Security Updates: ✗ 2 missing

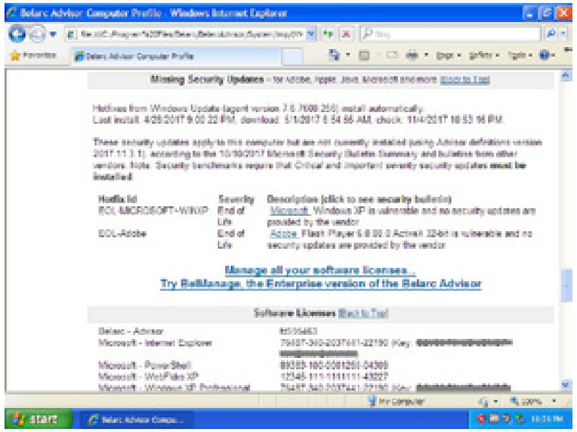
Computer Profile Summary

Computer Name: VM-WinXP_Pro (in WORKGROUP)
Profile Date: Saturday, November 04, 2017 11:15:53 PM
Advisor Version: 8.5c
Windows Logon: Administrator

Try BelManage, the Enterprise version of the Belarc Advisor

Figure 27: log file from Belarc Advisor

The screen shot above shows Belarc Advisor after running it on a computer that previously had been checked and updated using Microsoft Security Baseline Analyzer (MSBA).



Belarc Advisor Computer Profile - Windows Internet Explorer

Missing Security Updates - for Adobe, Apple, Java, Microsoft and more (Back to Top)

Hotfixes from Windows Update (agent version 7.6.7600.256) install automatically.
Last install: 4/25/2017 9:00:22 PM, download: 5/1/2017 6:54:56 AM, check: 11/4/2017 10:53:16 PM

These security updates apply to this computer but are not currently installed (using Advisor definitions version 2017.11.3.1), according to the 10/10/2017 Microsoft Security Bulletin Summary and bulletins from other vendors. Note: Security benchmarks require that Critical and Important severity security updates must be installed.

Hotfix Id	Severity	Description (click to see security bulletin)
EOL-MICROSOFT-WINXP	End of Life	Microsoft Windows XP is vulnerable and no security updates are provided by the vendor
EOL-Adobe	End of Life	Adobe Flash Player [illegible] ActiveX 32-bit is vulnerable and no security updates are provided by the vendor

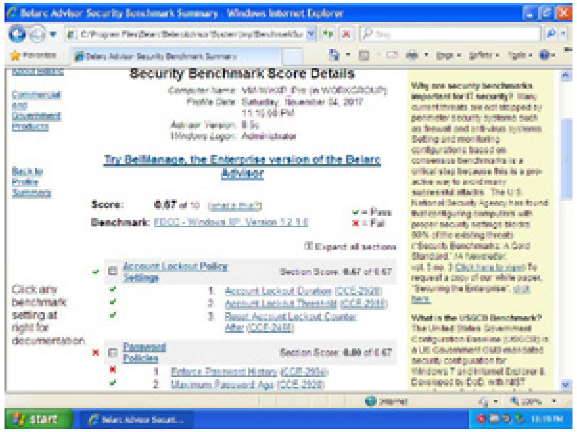
Manage all your software licenses...
Try BelManage, the Enterprise version of the Belarc Advisor

Software Licenses (Back to Top)

Belarc - Advisor	[illegible]
Microsoft - Internet Explorer	76487-360-2037461-22190 (Key: [redacted]
Microsoft - PowerShell	89383-100-0001260-04309
Microsoft - WebFldrs XP	12345-111-1111111-43227
Microsoft - Windows XP Professional	76487-360-2037461-22190 (Key: [redacted]

Figure 28: Belarc Advisor identifying Windows XP and Adobe Flash as end of life software.

Here, Belarc Advisor identified two missing security updates for Microsoft Windows XP on this computer, and assessed the computer's security level at 0.67 on a scale of 0 to 10.



Belarc Advisor Security Benchmark Summary - Windows Internet Explorer

Security Benchmark Score Details

Computer Name: VM-WinXP_Pro (in WORKGROUP)
Profile Date: Saturday, November 04, 2017 11:15:08 PM
Advisor Version: 8.5c
Windows Logon: Administrator

Try BelManage, the Enterprise version of the Belarc Advisor

Score: 0.67 of 10 (what's this?)
Benchmark: FDCC - Windows XP, Version 1.2.1.0

✓ = Pass
✗ = Fail

⊞ Expand all sections

✓ ⊟ Account Lockout Policy Settings — Section Score: 0.67 of 0.67
✓ 1. Account Lockout Duration (CCE-2928)
✓ 2. Account Lockout Threshold (CCE-2986)
✓ 3. Reset Account Lockout Counter After (CCE-2466)

✗ ⊟ Password Policies — Section Score: 0.00 of 0.67
✗ 1. Enforce Password History (CCE-2994)
✓ 2. Maximum Password Age (CCE-2920)

Click any benchmark setting at right for documentation.

Why are security benchmarks important for IT security? Many current threats are not stopped by perimeter security systems such as firewall and anti-virus systems. Setting and monitoring configurations based on consensus benchmarks is a critical step because this is a pro-active way to avoid many successful attacks. The U.S. National Security Agency has found that configuring computers with proper security settings blocks 90% of the existing threats ("Security Benchmarks: A Gold Standard," IA Newsletter, vol. 5 no. 3 Click here to view). To request a copy of our white paper, "Securing the Enterprise", click here.

What is the USGCB Benchmark? The United States Government Configuration Baseline (USGCB) is a US Government OMB mandated security configuration for Windows 7 and Internet Explorer 8. Developed by DoD, with NIST

Figure 29: Belarc Advisor identifying weaknesses in password handling

While such scoring may be partially due to the fact that the operating system has reached end of life status and no longer receives security updates, it does indicate there are additional steps that must be taken to better secure Windows XP.

Secunia PSA

Secunia was a company that made vulnerability checking software. In 2015, Secunia was acquired by Flexera, a company with complementary offerings[117, 118]. Flexera continues to distribute Secunia PSI (Personal Software Inspector), a free program for consumers that checks for missing security updates for Microsoft Windows XP and other software packages[119].

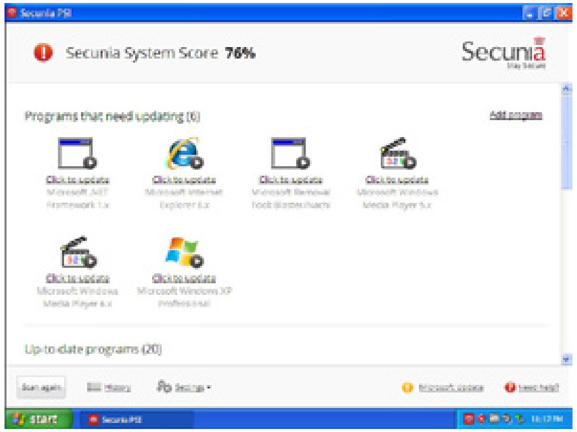


Figure 30: Secunia PSI identifying missing updates

When run on a particular computer that previously had been checked and updated using Microsoft Security Baseline Analyzer (MSBA), Secunia PSI identified six programs that required updating, and assessed the computer as being "76% secure."

Third-Party Security Software

As previously ***noted***, Microsoft no longer provides anti-malware software for Microsoft Windows XP. This means that it is important to use reputable software from an established security company that protects Microsoft Windows XP from malware. There are numerous companies that do continue to provide security software for Windows XP, including ESET.

Some companies offer a free version (with limited features, support, and reminders to upgrade) while others offer paid versions. Regardless of how a company markets its anti-malware software, if it is reputable it will offer a trial version capable of detecting, removing, and preventing malware--and possibly other threats--from your computer. You should be cautious of any company offering security software that claims to find threats but will not remove them unless purchased. A reputable company will allow you to evaluate its software's ability to detect **and** remove threats to your system.

Find out how long the company will continue to provide support for Windows XP. For example, if you expect to use Windows XP for three more years, it would not be beneficial to use security software from a company that that was discontinuing support for Windows XP before then.

While evaluating security software, you should contact the company's technical support department for assistance with installation and configuration. Even--especially--if you know the answer, this will allow you to determine how quickly and thoroughly they respond to support requests. You should also read independent, unbiased tests to determine how capable a particular security software package is of protecting the computer.

Reputable security software companies and testers adhere to the standards and guidelines set up by the Anti-Malware Testing Standards Organization (AMTSO), a not-for-profit organization that serves as a

[117] Flexera. "Software Buyers Optimize and Secure Your Business." Flexera Software. *https://www.flexera.com/enterprise/*.

[118] Flexera. "Flexera Software Acquires Secunia, Adding Software Vulnerability Management Solutions That Reduce Cybersecurity Risks." Flexera Software. *https://www.flexera.com/producer/company/news-center/press-releases/Flexera-Software-Acquires-Secunia-Software-Vulnerability-Management.html*.

[119] Flexera. "Free Instant Download: Personal Software Inspector." Flexera Software. *http://learn.flexerasoftware.com/SVM-EVAL-Personal-Software-Inspector*.

clearinghouse. For more information, visit AMTSO's web site at **https://www.amtso.org/**.

For the up-to-date information about ESET's support for Windows XP, see ESET Knowledgebase Article #3505, ***Microsoft Windows XP end of support and ESET products***.

THE FUTURE

At some point, the time will come to decommission the remaining computer(s) running Microsoft Windows XP in your environment. While it is possible that they might be replaced with a computer running Windows Vista, Windows 7, Windows 8.1 or perhaps even macOS or Linux, it is more likely it will be replaced with a computer running Windows 10, the latest, and perhaps last, desktop version of Microsoft Windows for the foreseeable future.

While Microsoft Windows 10 looks and behaves differently than Windows XP; some of the biggest changes to it are in terms of security. ESET has conducted in-depth research into Windows 10's security, and here are some resources to help you bridge the gap of a decade-and-a-half's worth of changes to Windows:

- *It's time to finally say goodbye to Windows XP. And Vista. Again.* (2017-04-07)
- *Windows 10 Anniversary Update: Security and privacy, hope and change?* (2017-01-12)
- *Windows Exploitation in 2016* (2017-01-05)
- *ESET Trends 2017 – Security Held Ransom* [PDF] (2016-12)
- *Windows 10 security and privacy: An in-depth review and analysis* (2016-06-15)
- *ESET Trends 2016 – (In)security Everywhere* [PDF] (2016-02)
- *Windows Exploitation in 2015* (2016-01-26)
- *ESET Trends for 2016: Threats keep evolving as security becomes part of our lives* (2016-01-20)
- *Microsoft ends support for old Internet Explorer versions* (2016-01-12)
- *Should I stay or should I go … to Windows 10?* (2016-01-07)
- *ESET predictions and trends for cybercrime in 2016* (2015-12-23)
- *Ambiguous new Windows 10 update 'improves functionality'* (2015-08-21)
- *20,000 NHS Wales PCs still running Windows XP from beyond the grave* (2015-08-07)
- *Windows 10, Privacy 0? ESET deep drives into the privacy of Microsoft's new OS* (2015-08-06)
- *Aryeh Goretsky talks "very promising" Windows 10 security* (2015-05-19)
- *Will Windows 10 leave enterprises vulnerable to zero-days?* (2015-03-13)
- *The end of mainstream support for Windows 7. Learn from past mistakes* (2015-01-14)
- *Windows Exploitation in 2014* (2015-01-08)
- *Windows 10 to tighten security with prominent 2FA* (2014-10-23)
- *Windows 8.1 – security improvements* (2013-11-17)
- *Six months with Windows 8 (white paper)* (2013-06-06)
- *Windows Exploitation in 2013* (2013-02-11)
- *A white paper: Windows 8's Security Features* (2012-10-09)

Acknowledgements:

The author would like to thank his colleagues Artem Baranov, Jean-Ian Boutin, Bruce P. Burrell, Graham Cluley, Stephen Cobb, Gerald Ellison, Nick FitzGerald, Greg Gallagher, Ondrej Kubovič, Andrew Lee, Fer O'Neil, Sabrina Pagnotta, Emilio Plumey, Ben Reed, Javier Segura and Darren Stordahl, as well as Roger Fraumann from the Securing our eCity Foundation, for their assistance in writing this white paper. Thanks also to VMware for the virtualization technology used during the writing of this paper.

March 2018

ENJOY SAFER TECHNOLOGY™

ESET, spol. s r.o.
Aupark Tower, 16th Floor
Einsteinova 24, 851 01 Bratislava
Slovak Republic