



Power Checklist:  
**Securing Windows XP**



# Securing Windows XP


If you have just finished installing Windows XP and you think the work is done, you are wrong. Some of the most important steps to getting Windows XP up and running come after the installation of the operating system. At this point, you need to make specific configuration changes and install additional software to ensure that your computer is secure.

With its default configurations, Windows XP is not very secure. However, by making the recommended changes in the checklist below, you can secure your system and data from attackers and viruses.

Note: Windows XP Professional edition is inherently more secure than Windows XP Home edition. Since Windows XP Home does not contain as many security features, it is strongly recommended that you upgrade to Windows XP Professional.

## File System

Windows XP supports both FAT32 and NTFS. NTFS supports additional features that can be used to secure your system. For example, NTFS allows you to set permissions at the file level, not just at the folder level. If you formatted any partitions with FAT32, there is a one time conversion from FAT32 to NTFS without any data loss.

-  **Convert Partitions to NTFS.** It is recommended that you convert all partitions and volumes to NTFS to take advantage of advanced security features that are not included with FAT32.

One way of converting to NTFS is to use the convert command from the command prompt. The syntax for the command is as follows:

```
Convert x: /fs:ntfs
```

Where *x* is the letter assigned to the partition or volume you want to convert.

After you press Enter, you'll be asked to confirm your actions by pressing Y and the conversion is done. You can now set security at the file level. If the partition or volume is currently in use, prime example is if you are trying to convert your system volume, you can opt to have the conversion take place the next time the computer is restarted.

A word of caution though as this is a one time conversion which means there isn't any going back from NTFS to FAT32 unless you format the volume or find a third party utility that can perform this task.

- ◆ **Choosing between NTFS, FAT, and FAT32.**  
([http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/choosing\\_between\\_ntfs\\_fat\\_and\\_fat32.mspx?mfr=true](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/choosing_between_ntfs_fat_and_fat32.mspx?mfr=true))  
Learn about the differences between Windows XP's file systems
- ◆ **How to Convert FAT Disks to NTFS.**  
(<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/convertfat.mspx>)  
This TechNet article describes the exact process for converting a disk to NTFS.

## Automatic Updates

Keeping your system up-to-date is crucial to maintaining security. Microsoft releases security updates and makes them available for download on the Windows Update web site. Using Automatic Updates, Windows XP can be configured to download and install updates for you automatically.

- Use Automatic Updates.** Ensure your computer has the latest software updates by configuring Windows XP to automatically download and install updates for you at a certain schedule.

You can configure a schedule to instruct Windows XP when to install new updates on your computer. A handy feature for those of you who do not want updates installed when you are busy using your computer for other tasks. You can configure a schedule so the updates are installed when your computer is not being used for anything too important.

The process of configuring a schedule is very straight forward. In Windows XP, you can use the following steps to enable this feature:

1. Right click My Computer and select Properties.
2. Click the Automatic Updates tab from the System Properties dialog box.
3. Select the option to Automatically download the updates, and install them on the schedule that I specify as shown in the following figure.
4. Select the day and the time when you want the updates installed.
5. Click Ok.

- ◆ **How to configure and use Automatic Updates in Windows XP.**

(<http://support.microsoft.com/kb/306525/>)

Learn more about how to configure the Automatic Updates feature in Windows XP.

## Windows Firewall

Windows XP includes the ICF (Internet Connection Firewall) service. As you will see in Windows XP Service Pack 2, ICF is renamed to Windows Firewall and it is enabled by default. It is designed to protect your computer from external intrusion while it is connected to the Internet.

- Enable Windows Firewall.** Verify that the Windows Firewall is enabled on your Internet connection.

Note: if you are setting up a home network, do not enable ICF on your LAN (local-area network) connection. Only enable it on the Internet connection. If you enable ICF on your LAN connection, it will block File and Printer Sharing.

- ◆ **Understanding Windows Firewall.**

([http://www.microsoft.com/windowsxp/using/security/internet/sp2\\_wfintro.msp](http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.msp))

Read more about how the Windows Firewall protects your computer against attackers.

- ◆ **Configure the Windows Firewall after Service Pack 2.**

([http://techrepublic.com.com/5100-1035\\_11-5305934.html?tag=search](http://techrepublic.com.com/5100-1035_11-5305934.html?tag=search))

Mark Kaelin walks you through the process of configuring the Windows Firewall in Windows XP.

## User and Group Permissions

Simple file sharing is enabled when Windows XP is installed. This allows you to share folders with everyone in your workgroup. However it does not allow you to limit which specific users and groups can access your folders.

- Disable Simple File Sharing.** With Simple File Sharing disabled, you can assign permissions to specific users and groups. This provides you with a finer granularity of control over controlling access to resources.

Simple File Sharing can be disabled by opening the Folder Options applet in the Control Panel. Click the View tab and remove the check beside the Use simple file sharing (recommended) option.

- ◆ **10 things you should know about working with NTFS permissions.**  
([http://techrepublic.com.com/5100-1035\\_11-6059618.html?tag=search](http://techrepublic.com.com/5100-1035_11-6059618.html?tag=search))  
Rick Vanover provides with a top 10 list of best practices when using NTFS permissions.
- ◆ **Create and control shared folders in Windows XP.**  
([http://techrepublic.com.com/5100-1035\\_11-1054837.html?tag=search](http://techrepublic.com.com/5100-1035_11-1054837.html?tag=search))  
Dr. Thomas Shinder walks you through the process of configuring share permissions in Windows XP.

## User Accounts

Windows XP includes various built-in user accounts. There are certain steps that you should take after installing Windows XP to ensure they are not compromised.

- Disable the Guest Account.** Verify that the Guest account is disabled. The guest account has always been a huge hacker hole and should remain disabled if it is not required.
- Require passwords for all user accounts.** Both Windows XP Professional and Windows XP Home Edition allow user accounts to utilize blank passwords to log into their local workstations, although in Windows XP Professional, accounts with blank passwords can no longer be used to log on to the computer remotely over the network.

Obviously, blank passwords are a bad idea if you care about security. Make sure you assign passwords to all accounts, especially the Administrator account and any accounts with Administrator privileges. The local password policy should be configured to require all passwords to be a minimum of eight characters in length.

Keep in mind that in the Windows XP Home Edition all user accounts have administrative privileges and no password by default. Make sure you close this hole as soon as possible.

- Rename the Administrator account.** By renaming the administrator account hackers not only have to guess the password but also the name assigned to the account.

Many hackers will argue that this won't stop them, because they will use the SID to find the name of the account and hack that. Our view is, why make it easy for them. Renaming the Administrator account will stop some amateur hackers cold, and will annoy the more determined ones. Remember that hackers won't know what the inherit or group permissions are for an account, so they'll try to hack any local account they find and then try to hack other accounts as they go to improve their access. If you rename the account, try not to use the word Admin in its name. Pick something that won't sound like it has rights to anything.

Another strategy is to create a local account named Administrator, then give that account no privileges and 10+ digit complex password. This should keep the script kiddies busy for a while. If you create a dummy Administrative account, enabled auditing so you'll know when it is being tampered with. You should be able to catch the culprits in the act before they are able to gain access to your systems.

◆ **Description of the Guest account in Windows XP.**

(<http://support.microsoft.com/?kbid=300489>)

Find out more about the Guest account in Windows XP Home and Windows XP Professional.

◆ **Password Policy.**

(<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/pptopnode.mspx?mfr=true>)

Get a complete description of all the settings available in Windows XP's password policy.

## Remote Desktop

Windows XP Professional's Remote Desktop allows users to connect remotely to your computer. Although it can be useful for obtaining remote assist with troubleshooting, it is also an open door for attackers

**Disable Remote Desktop.** Remote Desktop should be disabled and only enabled on an as need basis.

Remote Desktop is disabled using the Remote tab from the System Properties dialog box. Under the Remote Desktop heading, remove the check beside the All users to connect remotely to this computer option.

◆ **How to Disable Remote Desktop by using Group Policy.**

(<http://support.microsoft.com/kb/306300>)

This article describes how you can disable Remote Desktop through a computer's local group policy.

## Anti-virus Software

Anti-virus software is a program designed specifically to detect and remove viruses, making it an essential application to install. Once you install anti-virus software, it will scan your computer and clean any viruses it finds.

**Install anti-virus software.** Anti-virus should be installed as soon as possible to protect your computer from viruses.


Some of the more popular antivirus software programs are listed below.

1. Trend Micro
2. McAfee
3. F-secure
4. Symantec
5. Computer Associates
6. Panda Software

Most anti-virus software must be purchased or it may be included with the purchase of a new computer. Some vendors also offer specials or free trial periods. In any case, if you have just performed a clean installation of Windows there will be no anti-virus software on your computer. The installation process will vary from vendor to vendor

## Screensavers

You are sitting at your desk, your computer is idle, and suddenly, a cool image appears on your desktop that completely mesmerizes you. That would be your screensaver. Screensavers can serve a much more important purpose other than providing us with a few minutes of visual pleasure. Believe it or not, enabling a screensaver can actually increase the security on your computer.

-  **Use a password protected screensaver.** Enable a password protected screensaver so other users can not access your computer.

You can configure a screensaver to start when your computer has been idle for a specific amount of time (for example, after 5 minutes). By password protecting the screensaver, the computer will be locked when the screensaver starts. This is a great idea for those of us who forget to lock our workstations when we leave. In order to return to the desktop and resume working, you will need to supply the correct password. So once a password protected screensaver has been enabled, you can walk away from your computer knowing that your folders and files are secured. In Windows XP, you can use the steps outlined below to enable a password protected screensaver.

1. Right click your desktop and click Properties.
2. From the Display Properties dialog box, select the Screensaver tab.
3. Use the drop down arrow to select your screensaver of choice.
4. Change the Wait value to specify how long the computer can remain idle before the screensaver is started.
5. Select the On resume, password protect option. If you do not select this option any activity will cause the desktop to appear.

