University of Texas at Arlington

Windows XP Operating System Security Guide

(Revision 3)

20081118

University of Texas at Arlington
Office of Information Technology
Information Security Office

Windows XP Operating System Security Guide

This guide is provided by the Office of Information Technology (OIT), Information Security Office as a basic and introductory guide for creating a more secure Operating System (OS) configuration than is traditionally gained with a normal Original Equipment Manufacturer (OEM) installation of Windows.

This guide is intended for use by UT Arlington Students, Staff, and Faculty for use with their **personally owned** computers.

This guide is intended for the Windows family of operating systems with an emphasis on Windows XP Professional, therefore some of the following items may or may not apply to your specific OS.

It is the responsibility of every user to ensure that their computer hardware, OS, and applications are kept up to date and configured in a secure manner so as to avoid system compromise, malware infection, and unauthorized use.

The following items are not all inclusive nor will they guarantee that your system will never be compromised.

It is the responsibility of the user to understand the consequence of making a configuration change and the associated benefits and negative impacts of applying any configuration change before that change is made.

OIT Information Security Office is not liable for nor does the OIT Information Security Office accept any responsibility for any damages to personal devices as a result of attempting these configuration changes.

All or some of the changes described below may require administrator level permissions.

Contents

1 - BASIC FEATURES

1.1 - Physical Security - basic

First and foremost physical security is critical to the overall security of your PC, especially mobile devices such as laptops. Knowing where your system is, who has physical access to the device, who has account access to the device (normally you should be the only one with an account on a personally owned device), are you currently logged on, logged off, is the screen locked, unlocked, etc.

- never leave your system unattended in a public area, internet café, classroom, airport, etc.
- always logoff or lock your screen if you are not at the keyboard.
- do not allow just any device or media to be plugged into your PC such as unknown CD / DVD's, random USB drives, a stranger's iPod, etc.
- transport your PC in a padded case inside a bag that does not look like a "laptop bag"
- consider how you are situated and can someone easily watch your monitor or shoulder surf.

In short a little paranoia goes a long way when it comes physical security.

Given physical access to a device it is simply a matter of time before that system is compromised. Depending on the attack vector and the desire and / or lack of desire to cause physical damage to the device an attacker who has physical access can compromise your device in seconds, minutes, or hours.

STOLEN DEVICES
All information available about your PC and / or portable devices should be recorded and kept in a safe place. In the event that your property is stolen you will then be able to provide that information to the police at the time of the report. If your device is stolen you cannot flip it over and look at the case for a serial number.

Information to record:
Manufacturer
Model Number
Serial Number
Service Tag Number
Windows Product Key (most pre-installed PCs have a Windows Authenticity Sticker on the case)
MAC Address (your device may have more than one.)
**NOTE - *The MAC Address is associated with a network interface card, some cards can be removed from the device and / or replaced with another card. Therefore this information is helpful but not a guarantee to verify ownership.*

In the event that a PC or portable device is stolen
Report theft of UT Arlington devices to the UT Arlington Helpdesk at ext. 2-2208 or 817-272-2208
Report theft of personally owned device that occurred on campus to the UT Arlington Police at ext. 2-3381 or 817-272-3381
Report theft of personally owned device that occurred off campus to the Arlington City Police at 817-459-5600.
**NOTE – *If you are traveling report the theft to the local authorities of the location the theft is believed to have occurred.*

1.2 - Use Strong Passwords (all accounts) - basic

Every account that is on the system should have a strong password. Passwords are required if the system is connected to any portion of the UTA campus network, UTA ResNet, UTA MavNet, or UTA Wireless Network.
**NOTE – *UT Arlington Information Security Office conducts periodic and reoccurring network scans, if a device is discovered with a blank password the network connection to that device may be disconnected prior to / or without user notification.*

Again, EVERY account on a system should have a strong password.

What is a strong password?
The commonly accepted definition of a strong password is a password that contains eight (8) or more alphanumeric characters with mixed case. At least one character is a capital, at least one character is a number, and at least one character is a special character (!@#$%^&*). Characters should not be sequential or repeating.

In general the more characters in the password the better.
The more characters that are not an alphabet character (abc….) the better.
The more random the characters the better.

The reason for a strong password is that the more complex and seemingly random the characters the longer it will take a program or person to guess and / or crack the password. As computers get bigger and faster a given password takes less time to crack.
A password of 8 characters that is only lower case alphabet characters can be cracked in about a half hour.
A password of 8 characters using both upper and lower case and numbers can be cracked in about a month.
A password of 8 characters of both, upper and lower case, numbers, and special characters can be cracked in about two years.

Due to the increasing speed of computers it is essential that the password chosen is strong and is changed frequently, every 3 to 6 months at a minimum.

Passwords should be long and complex however they also need to be easy to remember.
Never write down a password.

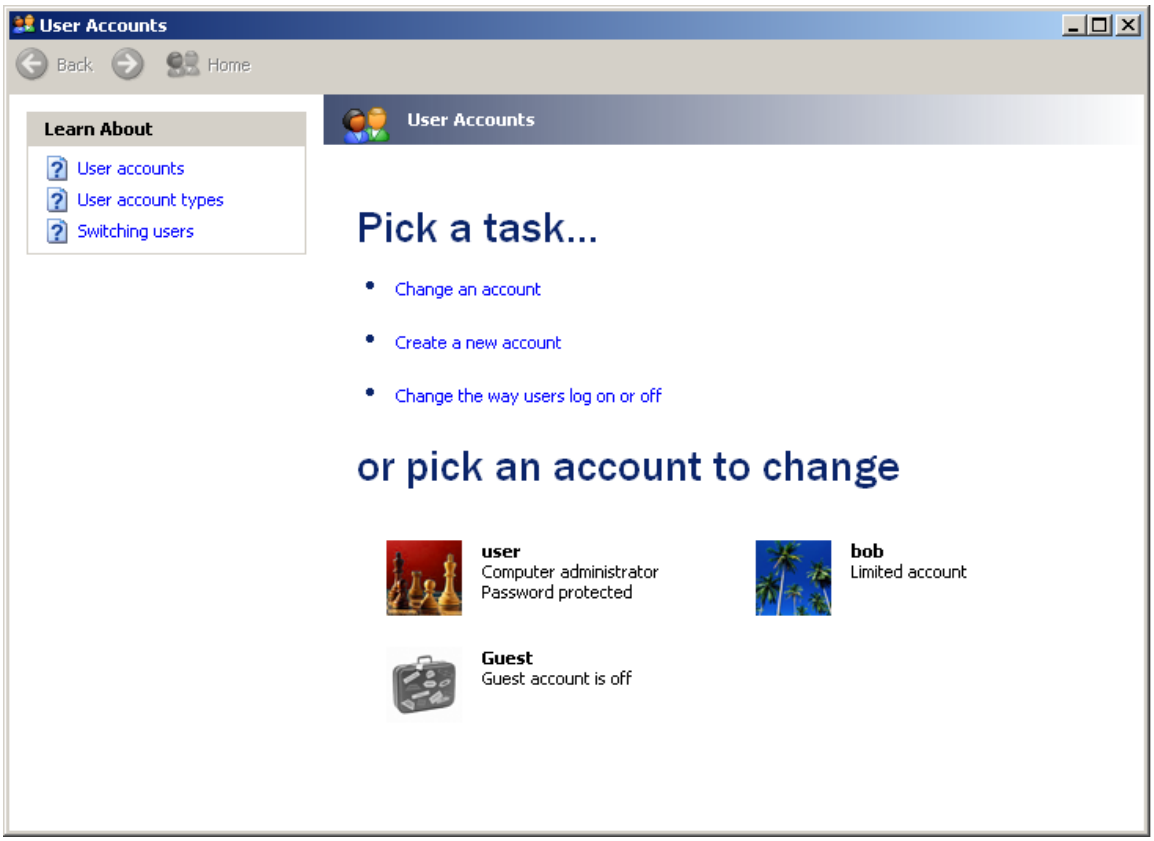
Example of a bad password
bob - Common word and too short
secretpassword - Longer but still common words and no non-alpha characters

Example of a better password
Mys3cr3tP@ssw0rd – longer good mix of characters. Uses letter substitution but still “spells” a common word so that it is easily remembered. This example however is still not preferred as letter substitution is a known strategy.

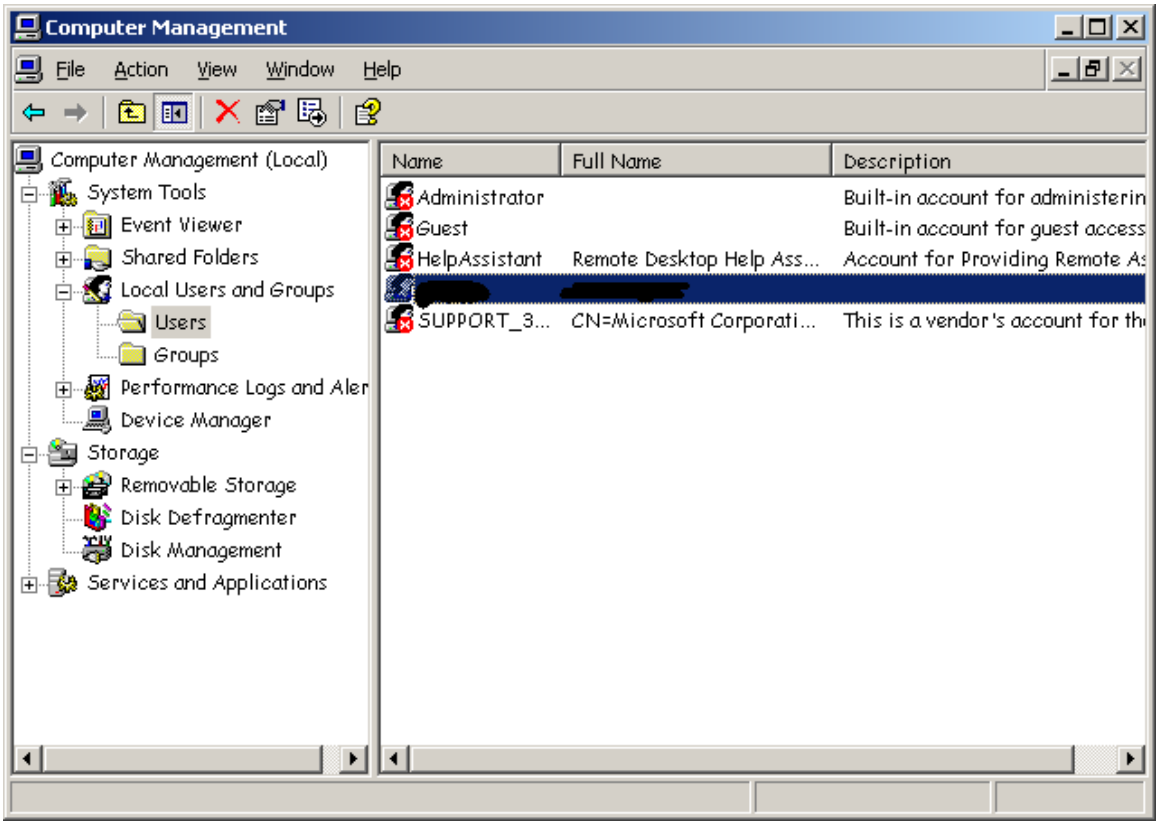
Example of a strong password
h5Qm!b7y* - Completely random but very hard to remember.
!Ht04nPeM – Strong password, good mix of characters, uses letter substitution, and appears random but uses mnemonics so that it is easily remembered. Each character is the first letter of a word in a sentence – I hate to order a new password each month.

There are many mnemonic systems that can be used to create a strong password; examples can be found with a simple internet search, such as ‘password mnemonics’.

To Change the password for a user account
In XP Home select Start → Settings → Control Panel → User Accounts
Select the user,
If the user previously did not have a password, select ‘Create a password’
If the user has a password, select ‘Change my password’



In XP Pro select Start → Settings → Control Panel → Administrative Tools → Computer Manager → Local Users and Groups → Users.
Select the user name
Right click and select the 'Set Password…'



More information on password security can be found at:
http://www.microsoft.com/athome/security/privacy/password.mspx

http://www.microsoft.com/athome/security/privacy/password_checker.mspx

---

1.3 - Limit the Number of Accounts - basic

Windows is shipped with several default accounts. These account names may vary based on the specific OS type and components installed. Your system may have default accounts such as:
Administrator
Guest
HelpAssistant
SUPPORT_xxx (where xxx is a number or code)
ASPNET
John (user account made at the time of OS installation)

It is recommended that any account that is not required for the system to function be disabled and / or deleted, with the exception of Administrator, Guest, and the user account made at the time of OS installation.
** NOTE - *Windows will not allow you to delete the Administrator and Guest accounts, nor would this be recommended.*

The more accounts on a system the more "doorways" there are to the system.

For the ultra cautious the Administrator account maybe renamed to prevent certain password guessing attempts. See Rename Administrator Account

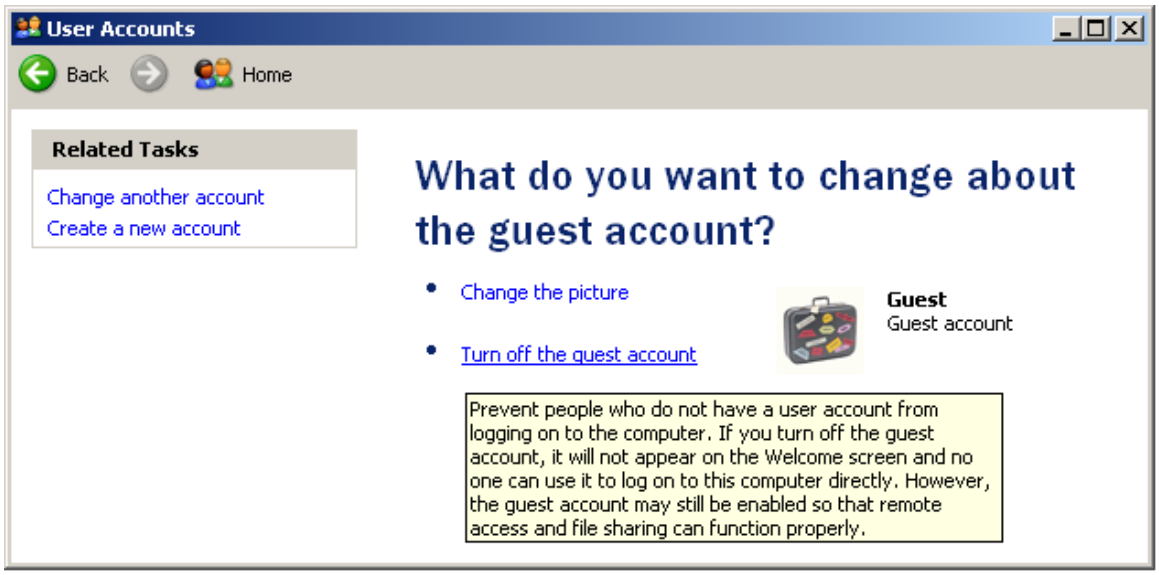
To delete a user account
In XP Home select Start → Settings → Control Panel → User Accounts
Select the user and select 'Delete the account'

In XP Pro select Start → Settings → Control Panel → Administrative Tools → Computer Manager → Local Users and Groups → Users.
Select the user name
Right click and select the 'Delete'.

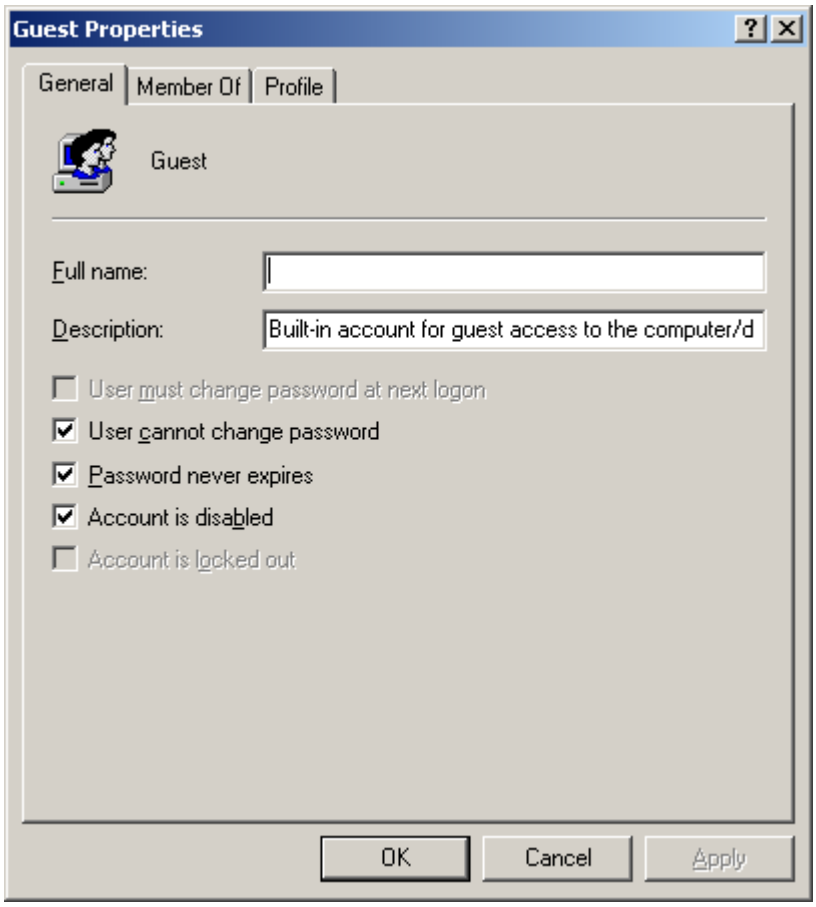
1.4 - Disable Guest Account - basic

Since the Guest account cannot be deleted it is recommended that this account be given a strong password and then disabled. A normal user will typically have no reason to use the Guest account.

To disable the Guest account (or any account)
In XP Home select Start → Settings → Control Panel → User Accounts → Guest → 'Turn off the Guest account'



In XP Pro select Start → Settings → Control Panel → Administrative Tools → Computer Manager → Local Users and Groups → Users
Select the user name
Right click and select the 'Properties'.
Select 'Account is disabled'

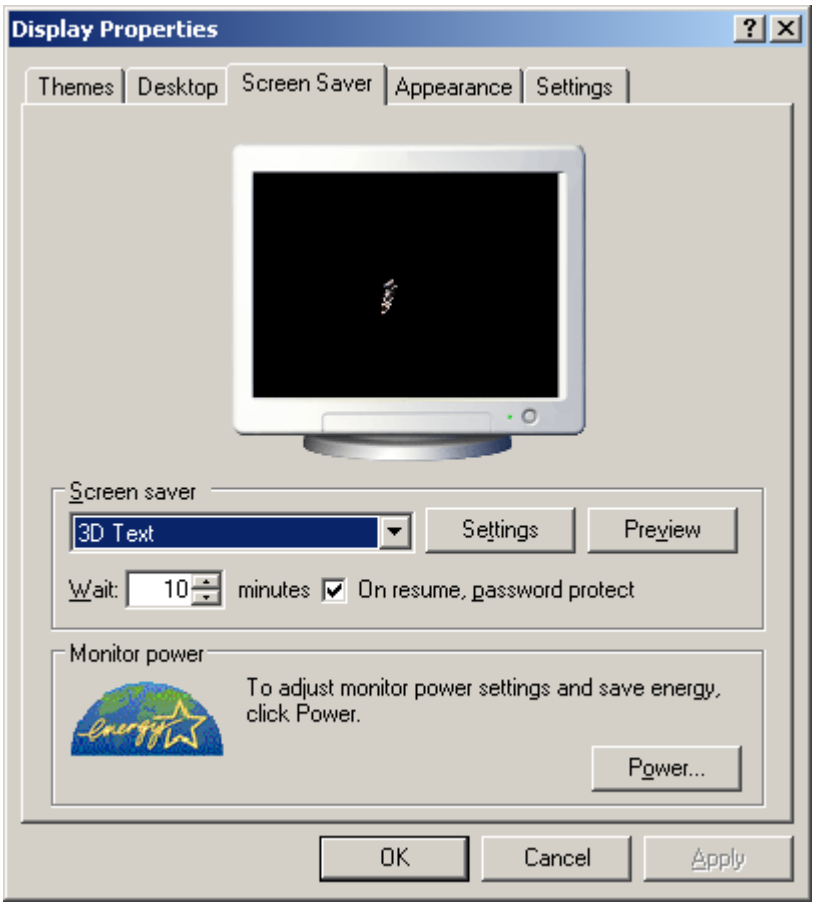


1.5 - Password Protected Screen Saver - basic

While we are recommending passwords for all accounts on the system let us not forget a very common mistake. Not using a screen saver, or using a screen saver with no password. It does no good to put looks on the door if you do not close the door behind you.

Always logoff of or lock your system when it is unattended, even if only for “a few minutes”.

To enable the system screen saver with password protection
Select Start → Settings → Control Panel → Display
Select the ‘Screen Saver’ tab
Select the screen saver of choice in the pull down menu
Set the desired time, 10 minutes is the default
Check the box for ‘On resume, password protect’



1.6 - Use Make Private Option - basic

In Windows XP Home there is an option in the User Accounts window that will allow you to limit the access to a user's files by other users. This option is labeled "Make my files private". This setting can only be selected once and it is highly recommended.

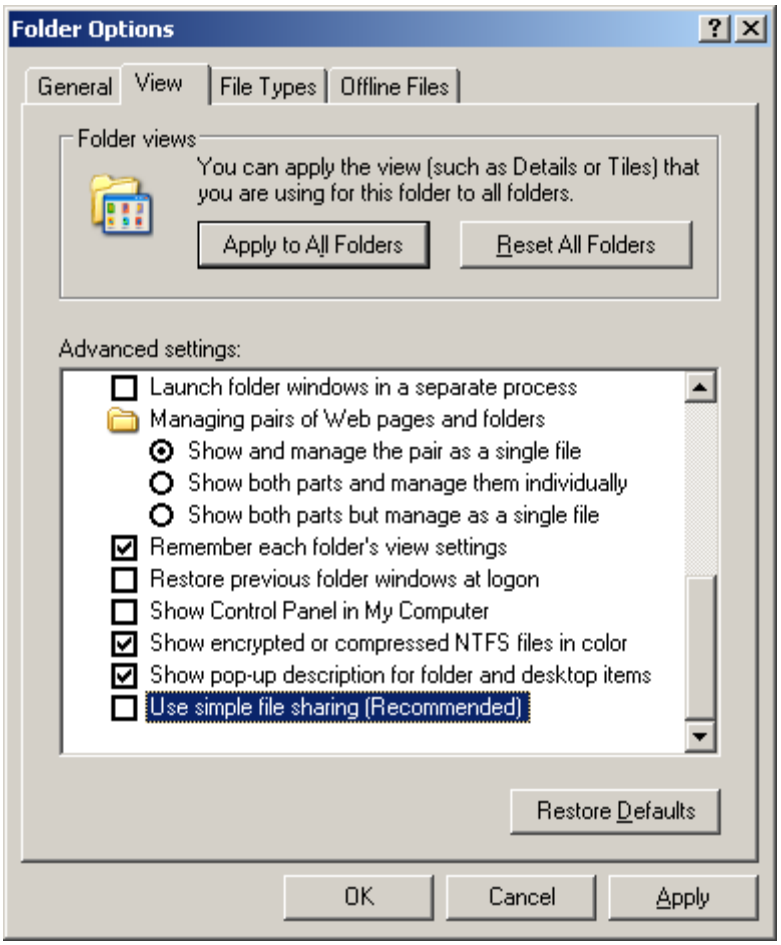
In XP Home select Start → Settings → Control Panel → User Accounts
Select the user and select 'Make my files private'

1.7 - Disable Simple File Sharing - basic

Windows XP home does not allow the user to disable Simple File Sharing. If you have Windows XP Home ensure that you have selected the 'Make Private' option.

Network shares can be powerful and helpful however Simple File Sharing does not allow the user to granularly specify who can access which share. If you must use shares these shares should be made very specific with permissions granted only to the user accounts that require access to that share. To provide proper shares 'Simple File Sharing' must be disabled and the share must be applied to the individual folders and / or files directly.

To disable Simple File Sharing
Open 'My Computer'
Select Tools → Folder Options
Select the 'View' tab
Within the 'Advanced Settings:' section uncheck 'Use simple file sharing (Recommended)



More information on Shares can be found at:
http://support.microsoft.com/default.aspx?scid=kb;EN-US;307874

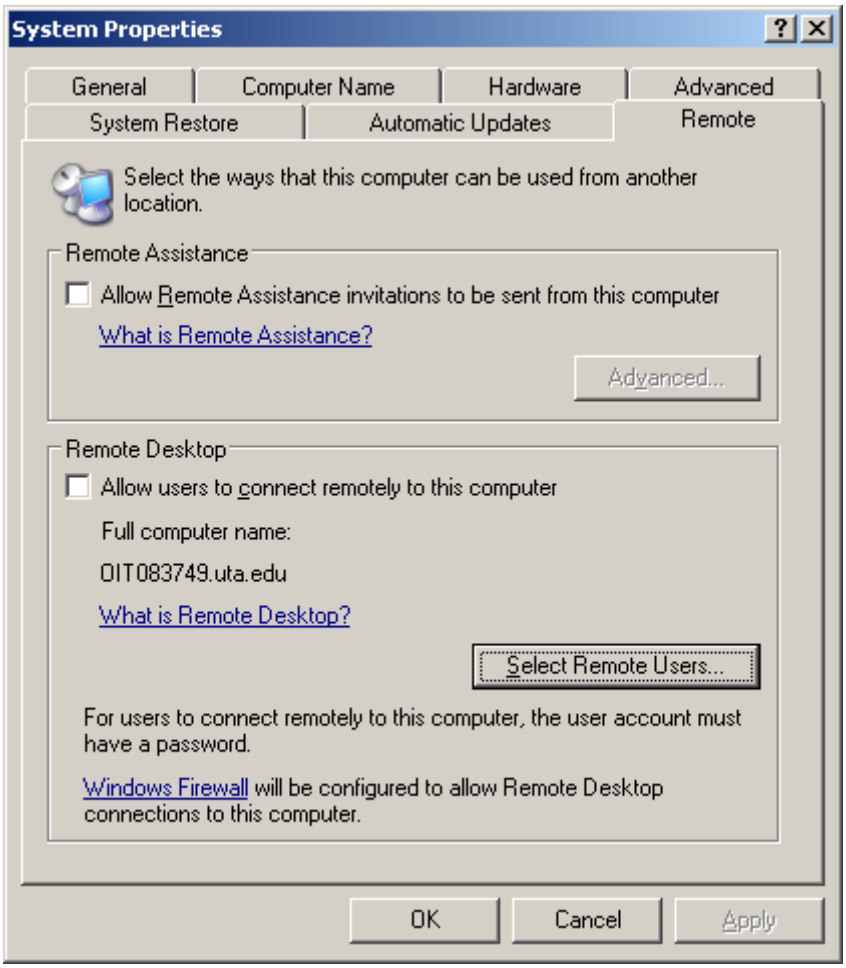
http://support.microsoft.com/?kbid=304040

1.8 - Disable Remote Assistance and Remote Desktop - basic

Remote Desktop although a very useful feature should only be enabled when it is needed and only for as long as needed. Most users will normally not require Remote Desktop features. There are also more secure alternatives available based on the actual requirements of the remote access.

To disable Remote Desktop
Right click “My Computer”
Select “Properties”
Select the “Remote” tab
Within “Remote Assistance” section uncheck “Allow Remote Assistance invitation to be sent from this computer”
Within the “Remote Desktop” section uncheck “Allow users to connect remotely to this computer”

If Remote Desktop must be used you should limit the access to specific users via the “Select Remote Users…” settings.



1.9 - Enable Auditing - basic

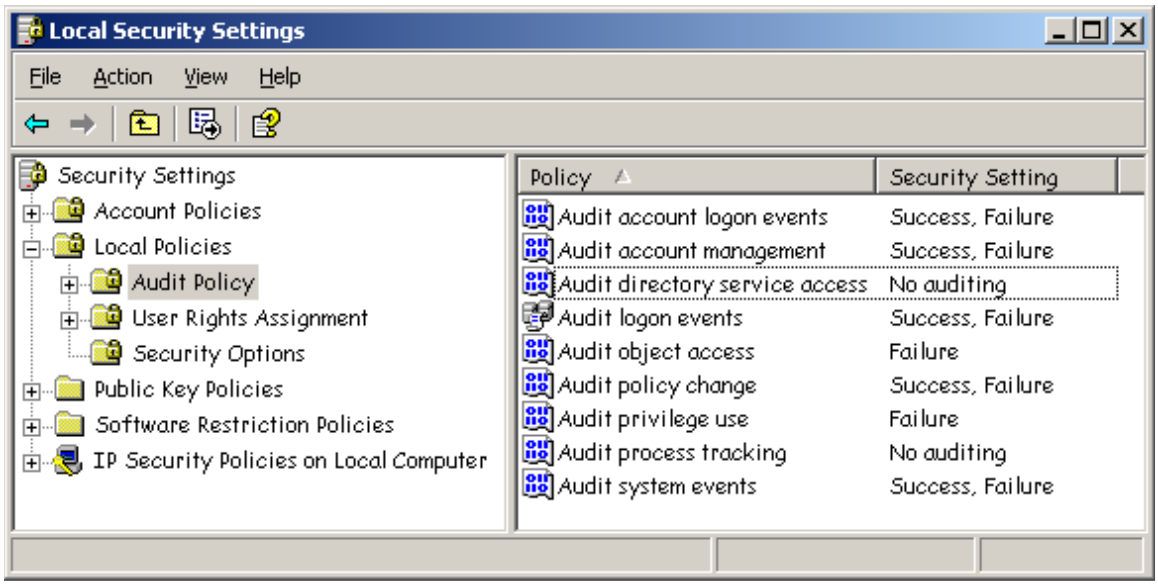
In the event that your PC should become compromised an audit trail may give the user (you) information as to how the system was compromised, the user account that performed the compromise, and what should be changed to prevent further compromise.

By default Windows is configured with little to no logging enabled. Windows Audit Logging is not available for Windows Home.

The following settings will provide a good starting point for audit logging.
To enable logging
Select Start → Settings → Control Panel → Administrative Tools → Local Security Policy
Select “Audit Policy” in the left pane
Double click each entry in the right pane and check the appropriate settings.

Account logon events	-	Success, Failure
Account management	-	Success, Failure

Directory Service Access	-	no auditing
Logon events	-	Success, Failure
Object access	-	Failure
Policy change	-	Success, Failure
Privilege use	-	Failure
Process Tracking	-	no auditing
System events	-	Success, Failure



More information on Auditing can be found at:
http://support.microsoft.com/?kbid=310399

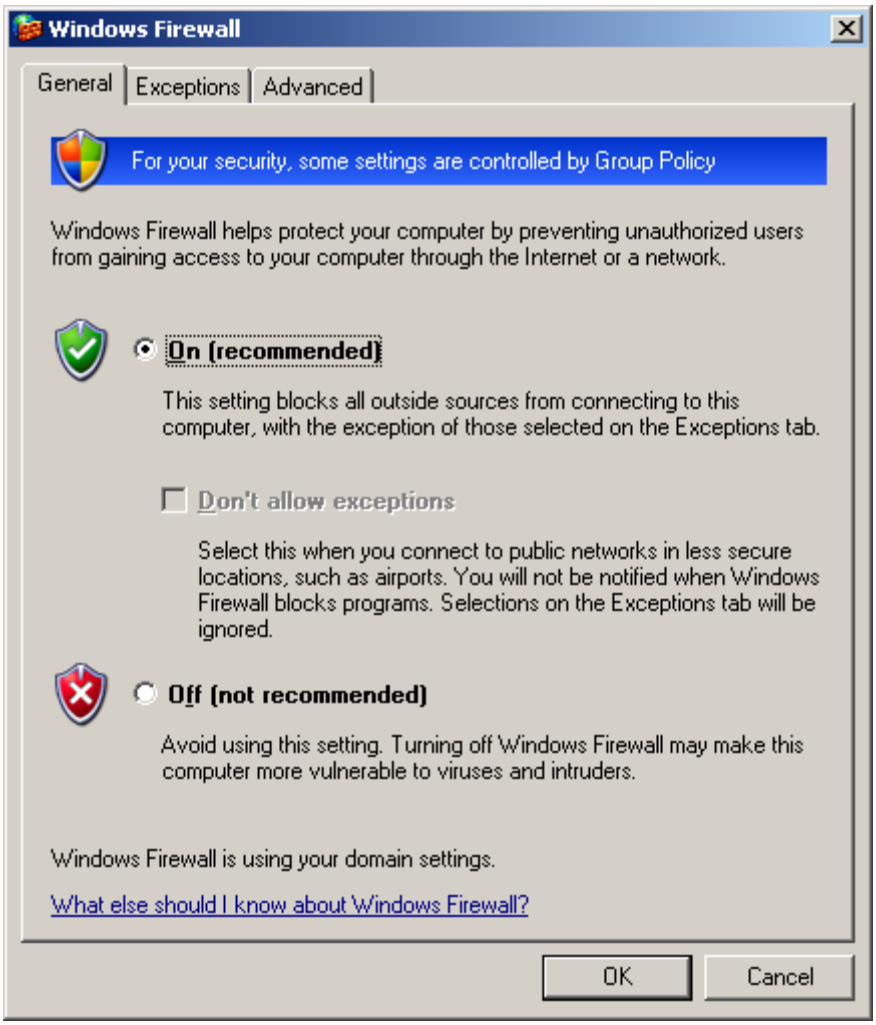
1.10 - Enable Windows Firewall - basic

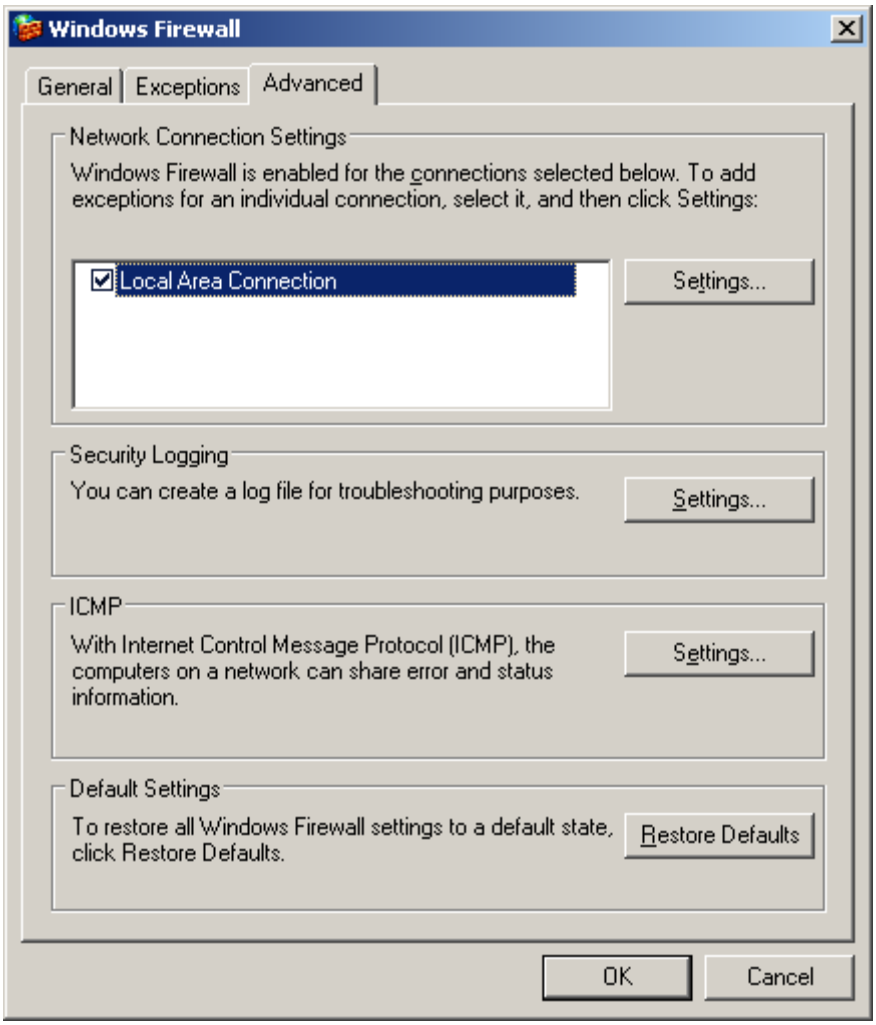
Windows XP Service Pack 2 comes with a firewall built into the Windows OS. This native firewall is free and a good start for host based firewall protection. However the native Windows firewall is limited in its configuration options.

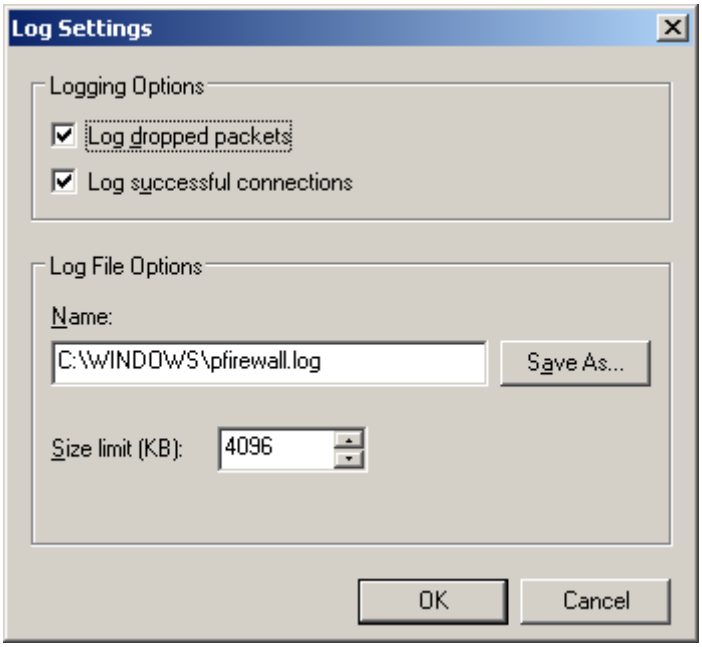
Ideally a purpose built firewall application should be used for any serious and / or complex firewall needs. There are many commercial products available on the market along with a few open source products. See Install Third Party Firewall.

** NOTE - *All firewalls are susceptible to being circumvented, some more easily than others.*

To enable the native Windows firewall
Select Start → Settings → Control Panel → Windows Firewall
On the “General” tab, select “On (recommended)”
Select the “Advanced” tab
Within the “Security Logging” section select “Settings…”
Within the “Logging Options” section
Check the box for “Log dropped packets”
Check the box for “Log successful connections”


Windows Firewall
General
Exceptions
Advanced
For your security, some settings are controlled by Group Policy
Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.
On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.
Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.
Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.
Windows Firewall is using your domain settings.
What else should I know about Windows Firewall?
OK
Cancel


Windows Firewall
General
Exceptions
Advanced
Network Connection Settings
Windows Firewall is enabled for the connections selected below. To add exceptions for an individual connection, select it, and then click Settings:
Local Area Connection
Settings...
Security Logging
You can create a log file for troubleshooting purposes.
Settings...
ICMP
With Internet Control Message Protocol (ICMP), the computers on a network can share error and status information.
Settings...
Default Settings
To restore all Windows Firewall settings to a default state, click Restore Defaults.
Restore Defaults
OK
Cancel


Log Settings
Logging Options
Log dropped packets
Log successful connections
Log File Options
Name:
C:\WINDOWS\pfirewall.log
Save As...
Size limit (KB):
4096
OK
Cancel

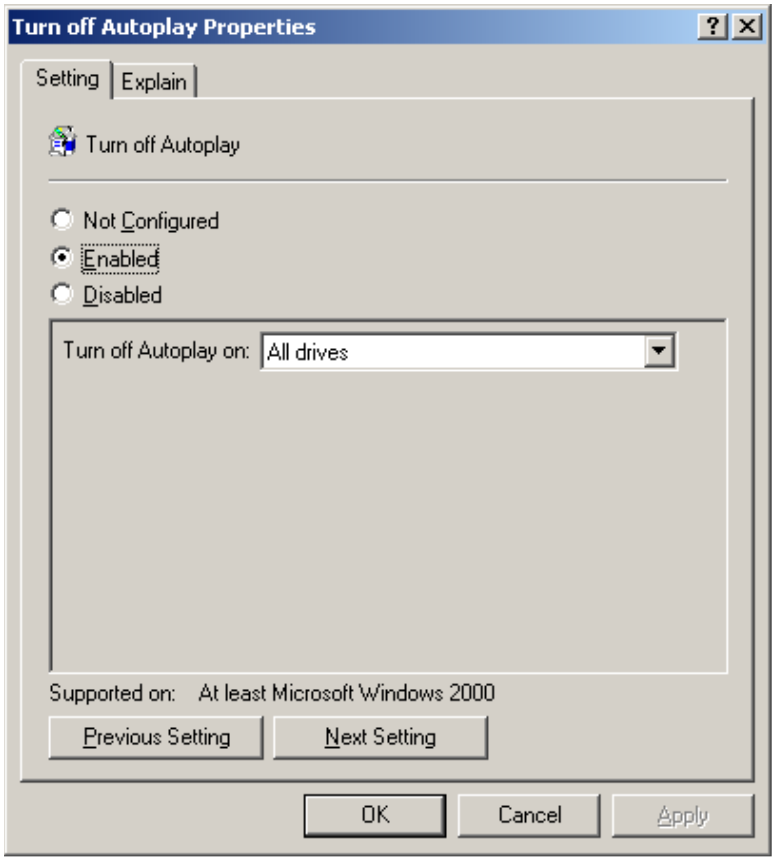
1.11 - Disable AutoRun - basic

AutoRun is another feature that can be handy or annoying based on user preference. However AutoRun also opens the door to malicious code to install itself in a stealthily manner. The infamous Sony rootkit was installed via the AutoRun feature. Many viruses, malware, and otherwise unwanted software can be installed without the user's consent on a machine that has AutoRun enabled.

AutoRun is enabled by default on all Windows systems.

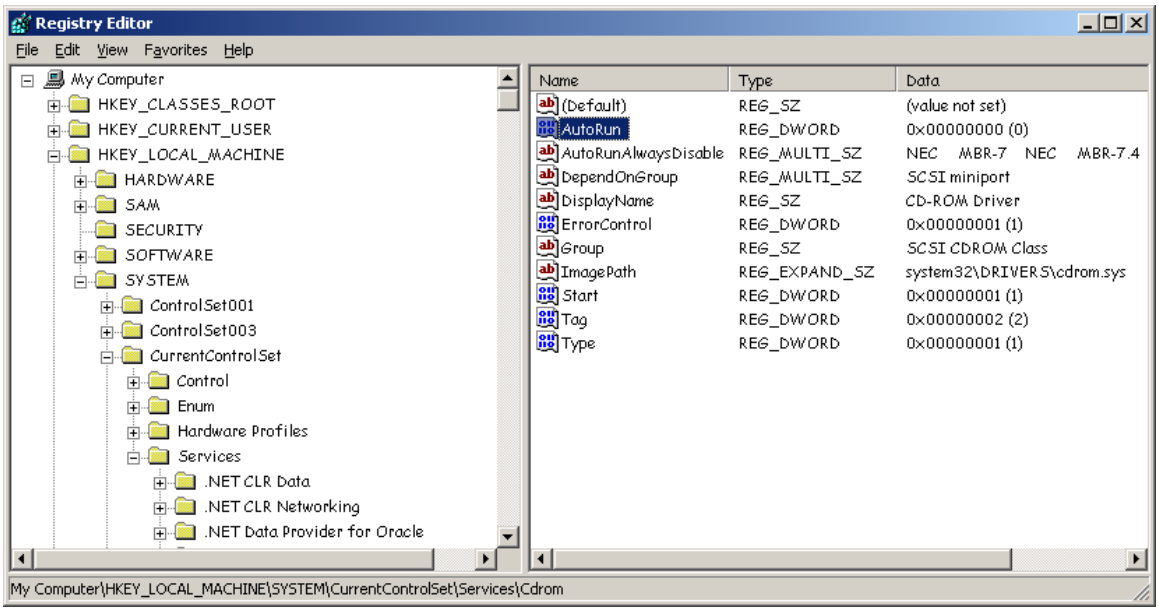
To disable AutoRun
First ensure that you have the patch MS08-038, KB950582, installed on your PC.

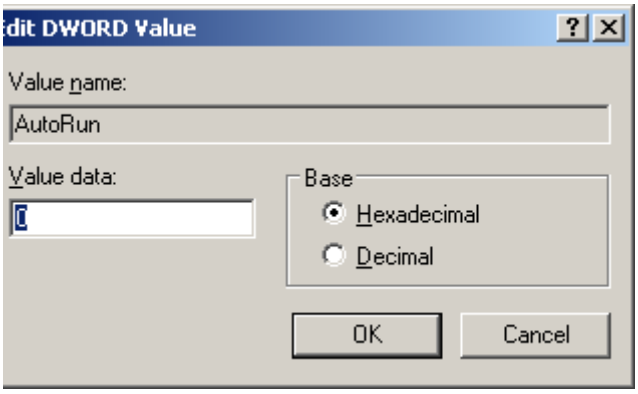
Then Select Start → Run…
Enter the command "gpedit.msc" (without quotes)
When the policy editor window pops up
Select → Computer Configuration → Administrative Templates → System
Double click on Turn of Autoplay
Select Enabled
Select All Drives
Select Apply
Select OK



Alternate method superseded by the method above
** NOTE - T*his change is a registry edit. Before making changes to the registry the user should back up the registry.*

Select Start → Run…
Enter the command “regedit.exe” (without quotes)
When the registry windows pops up
Double click (expand) HKEY_LOCAL_MACHINE
Double click (expand) SYSTEM
Double click (expand) CurrentControlSet
Double click (expand) Services
Select Cdrom
In the right pane select and double click the value AutoRun
Set the “Value data” to a zero 0
Reboot the PC.





Under Windows Vista this process is simplyifed and there is GUI based menu under 'Control Panel' to enable and disable AutoRun for each type of device.

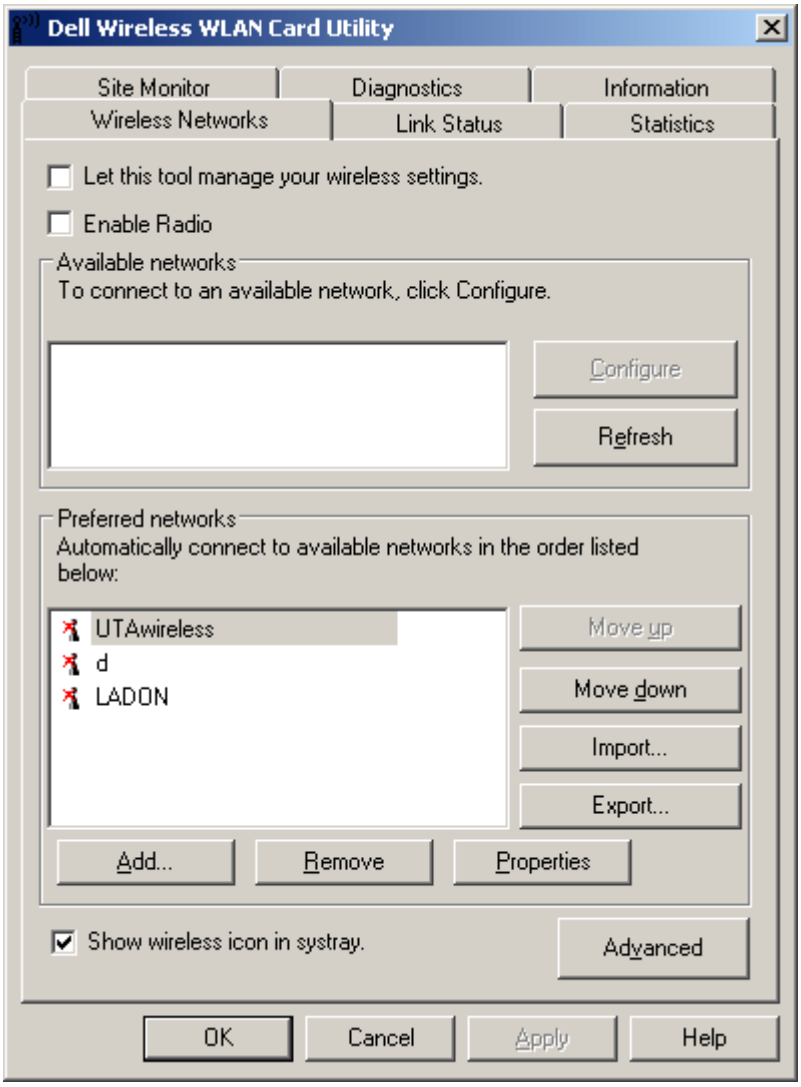
1.12 - Disable Wireless Interface - basic

Wireless networks allow a great range of mobility and flexibility, especially for laptop users. However by default windows enables the wireless interface each and every time the machine is booted up. Although convenient this opens a large security hole in any device that has a wireless interface.

The wireless interface of any PC should only be enabled when the user is actively using a wireless connection and should only be enabled for as long as necessary.

It is recommended that the manufacturer software be used for controlling the settings of your wireless network interface card. This recommendation is made as the manufacturer's software typically allows for more control and advanced settings of the wireless card than the basic Windows wireless wizard.
Each Wireless network interface card should come with software to control the wireless settings and each manufacturer's software varies in look and feel. Below is an example of a Dell Wireless GUI.

To open the Dell Wireless GUI
Select Start → Programs → Dell Wireless → Dell Wireless WLAN Card Utility
To enable the wireless card check the box next to "Enable Radio"
Likewise to disable the card uncheck the same box.



1.13 - Operating System Updates and Patches - basic

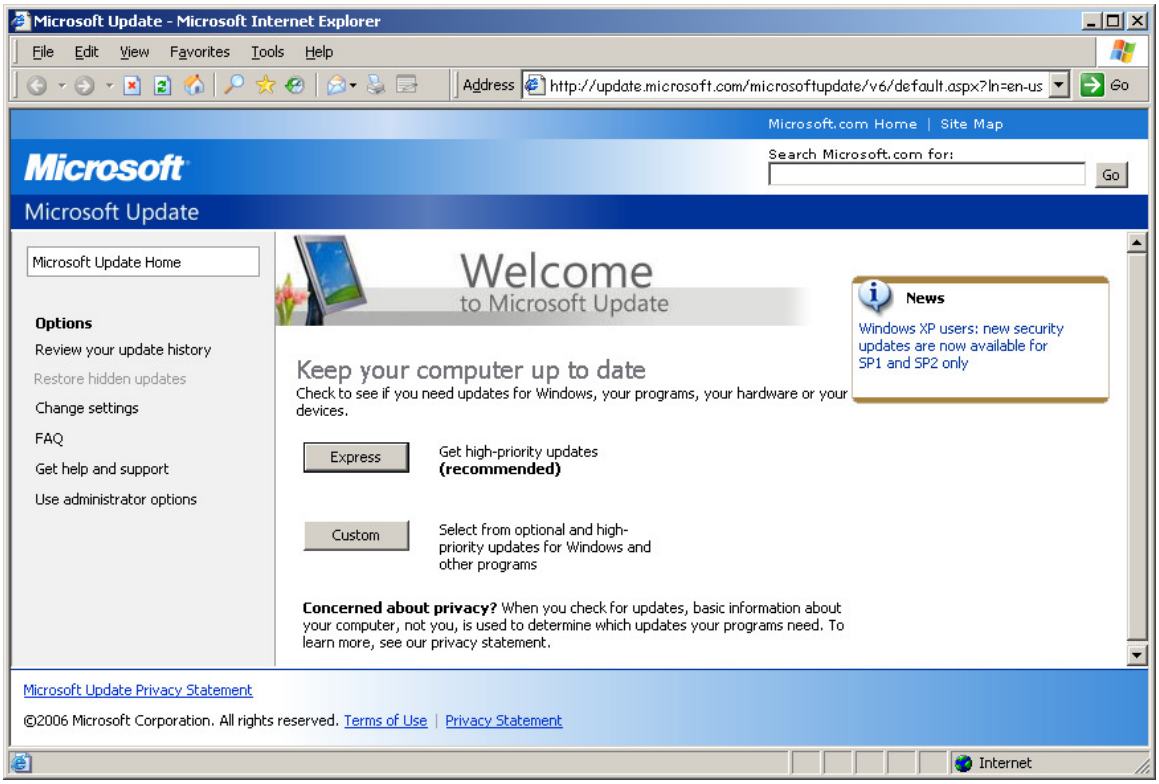
One of the most simple steps to ensuring system security is to check for and install Operating System (OS) updates and patches regularly.
Microsoft delivers regular patch releases on a monthly basis with the release being made on the second Tuesday of each month. This has become know as Microsoft Super Tuesday.
In the event that a patch is of extreme importance Microsoft will make an “out of cycle” release dependent on the patch availability.

** NOTE - *Microsoft Update does not guarantee all patches for every program used on your system. Microsoft Update will check for OS updates and patches. If you have Microsoft Office installed Microsoft Update will also check for Office updates and patches. If you are using specialized software such as Microsoft SQL Server, Microsoft Project, etc. Microsoft Update will not recognize these programs and will not alert you to new updates. These Specialized programs must be checked manually by the user on the appropriate software website.*

The Microsoft Update feature can and should be used to check for new updates and patches. Microsoft update is available at:
http://www.update.microsoft.com/

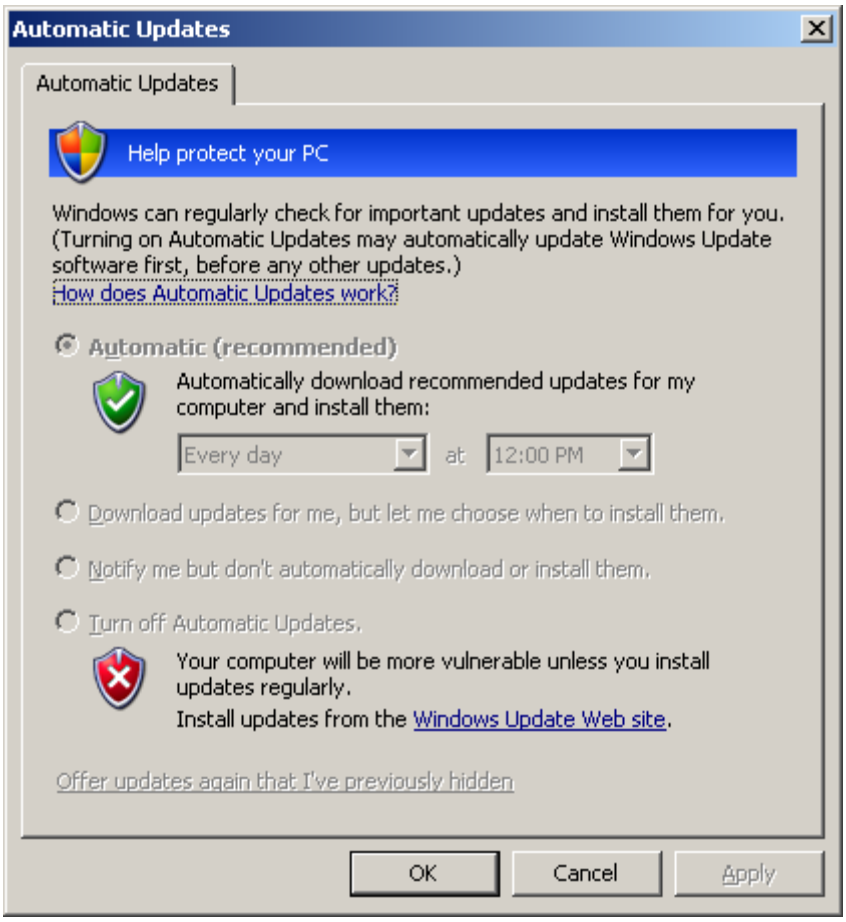
OR
Select Start → Microsoft Update (it may also be labeled as Windows Update)

OR
Open an Internet Explorer (IE) browser window and select Tools → Windows Update



Microsoft Also has a feature for the system to conduct automatic updates. Once "Automatic Updates" is enabled the system will check with Microsoft.com as scheduled and will prompt the user for installation.

To enable automatic updates select Start → Settings →Control Panel → Automatic Updates.



More information on Windows updates and security can be found at:
http://www.microsoft.com/athome/security/update/bulletins/default.mspx

http://www.microsoft.com/downloads/Browse.aspx?displaylang=en&categoryid=7

http://blogs.technet.com/msrc/

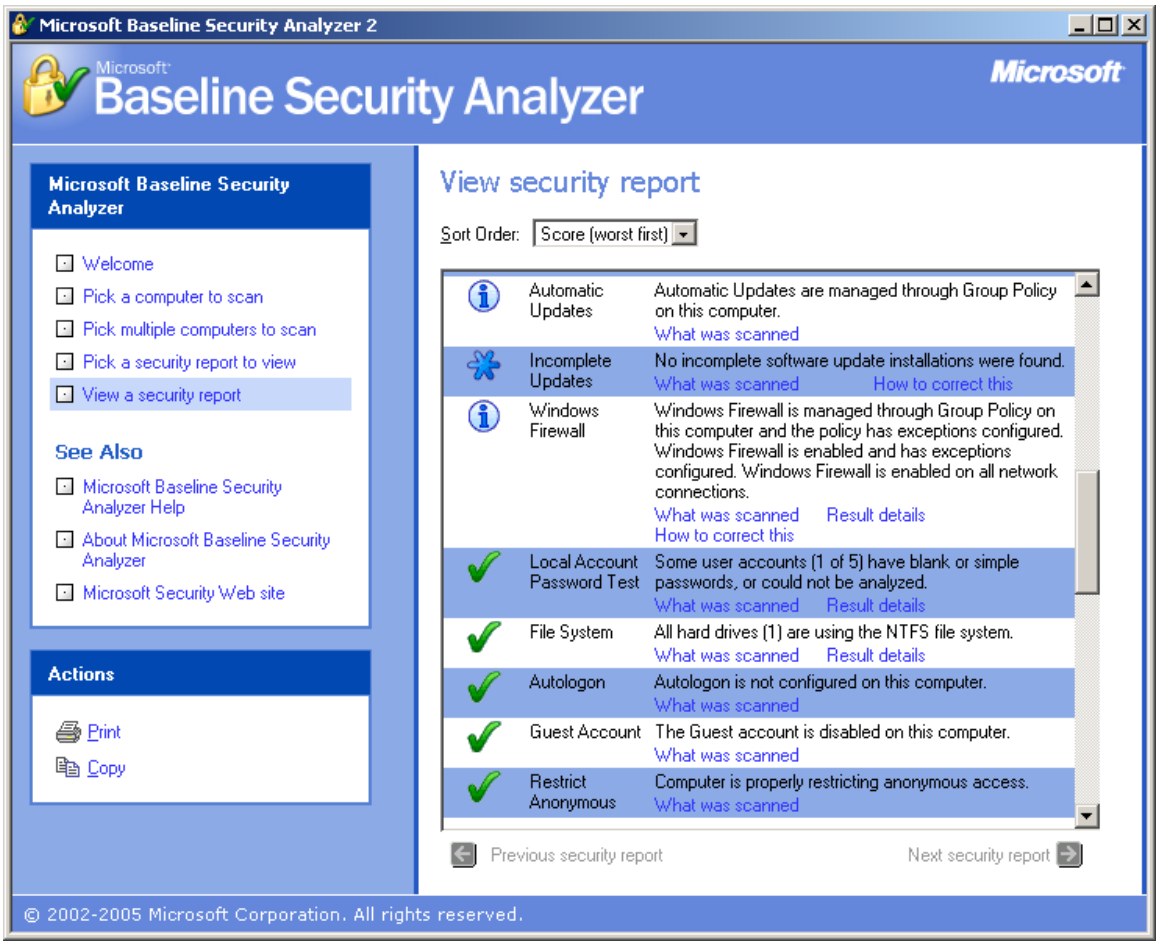
http://blogs.technet.com/swi/

1.14 - Use Microsoft Baseline Security Analyzer (MBSA) - basic

Microsoft provides a user friendly tool to check your system's patch level and security settings called Microsoft Baseline Security Analyzer (MBSA).
The MBSA is available at
http://www.microsoft.com/technet/security/tools/mbsahome.mspx

An example of the MBSA interface after it is installed.

An example of a system after being scanned with MBSA



1.15 - Install Anti-Virus Software - basic

Anti-Virus Software used to be an optional item, however in today's world of Hi-Speed, Wireless, Always-On internet connections, and the general pervasiveness of computer devices, along with the ever increasing number of malware programs Anti-Virus software is a must have. Without it your PC's days are truly numbered.

There are a number of commercially available products along with a few open source and / or free products. It is recommended to stick with well known vendors with a solid reputation.
** NOTE - *Be wary of any product that advertises via pop-up ads and otherwise unsolicited messages. Many nefarious companies have actually spread malware under the guise of being an Anti-Virus / security product.*

UT Arlington provides a copy of Symantec Endpoint Protection free of cost to all active and current UT Arlington Students, Faculty, and Staff. This software can be acquired on-line or at the Computer Store in Ransom Hall.
**NOTE - *The Computer Store has CD's of the program for five dollars ($5 USD). This cost is for the physical media and packaging overhead, not the software itself.*

The UT Arlington Anti-Virus website is
http://www.uta.edu/antivirus

Microsoft also offers a free Malicious Software Removal Tool
http://www.microsoft.com/security/malwareremove/default.mspx

1.16 - Use of Anti-Spyware Software - basic

Anti-Spyware is the "new Anti-Virus". As with Anti-Virus software Anti-Spyware software is a must have. Spyware can be more pervasive, annoying, and detrimental to the performance of your machine than a large percentage of the known viruses. Often times it is also more difficult to completely remove Spyware. Spyware can bring a system to a crawl, inundate the user with pop-ups, steal passwords and credentials, display pornography which can be deemed offensive (esp. during a presentation), to name a few things.

There are a number of commercially available products along with many open source and freeware products. It is recommended to stick with well known vendors with a solid reputation.
** NOTE - *Be wary of any product that advertises via pop-up ads and otherwise unsolicited messages. Many nefarious companies have actually spread Spyware under the guise of being an Anti-Spyware product.*

Many times various Anti-Spyware products will detect different threats. It is a commonly accepted practice to use multiple products.

Symantec Endpoint Protection has built in Anti-Spyware capabilities. Check your settings to ensure that these capabilities are enabled.

Three free and well trusted products are:
Microsoft Windows Defender
http://www.microsoft.com/windows/products/winfamily/defender/default.mspx

Spybot Search and Destroy
http://www.safer-networking.org/en/

Lavasoft Ad-aware
http://www.lavasoft.com/software/adaware/

1.17 - Application Updates and Patches - basic

In section 1.13 we discussed the importance of keeping up to date with OS patches. Equally important is the need to ensure that the applications that you install and use on your system are also kept up to date.

Application patches have a few unique
- What applications are on your system? Many commercial over the counter (COTS) PCs and Laptops come pre-installed with a multitude of applications. Many of which are never used by the consumer.
- Where and how do the application vendors announce updates and make patches available? More companies are starting to use auto-update features however this is not a universal concept, these features can also be deactivated. Other companies only post patches to their respective websites, while some companies just don't bother.

- How can the user check the application version? For those applications that have update features built in, find and run that update feature regularly. For the applications that do not have built-in update features look at the application 'About' or 'Help' information. Make not of the version number and manually check by visiting their website.

There are a few products that will automate some of this for you, most however will cost money.

If the application vendor does not readily post security information for their products there are numerous security websites that report advisories and vulnerabilities. One of the better sites is Secunia, www.secunia.com. Secunia also provides a free tool Personal Software Inspector (PSI) that will scan your machine, report out of date applications and will usually provide a link to the current update. ** NOTE – *PSI is for use on personally owned machines only.*

---

2 - INTERMEDIATE FEATURES

2.1 - Remove Welcome Screen - intermediate

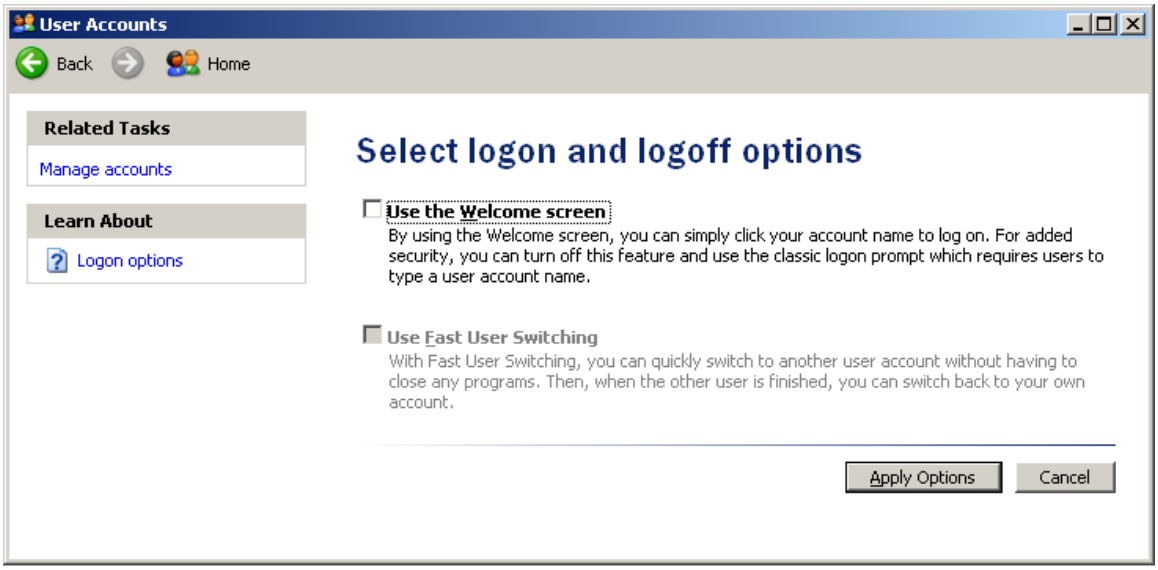
Many preinstalled PCs with Windows XP will boot up and start windows under the assumption that your user id is the primary id and will automatically login, or they are configured to present a user list with a picture for each user.

Although this configuration may feel more personal or friendly it carries with it several vulnerabilities.

Automatic login, very bad, not good, DO NOT do it.

Presentation of user list. There are two pieces of information that generally allow someone to use a PC. User ID and User Password. By displaying a list of users on the login screen you have just given away half of that information.

To disable the Welcome Screen
Select Start → Settings → Control Panel → User Accounts
Select "Change the way users log on or off"
Uncheck the box for "Use the Welcome screen"



OR
You can modify the Windows Registry
** NOTE - *This change is a registry edit. Before making changes to the registry the user should back up the registry.*

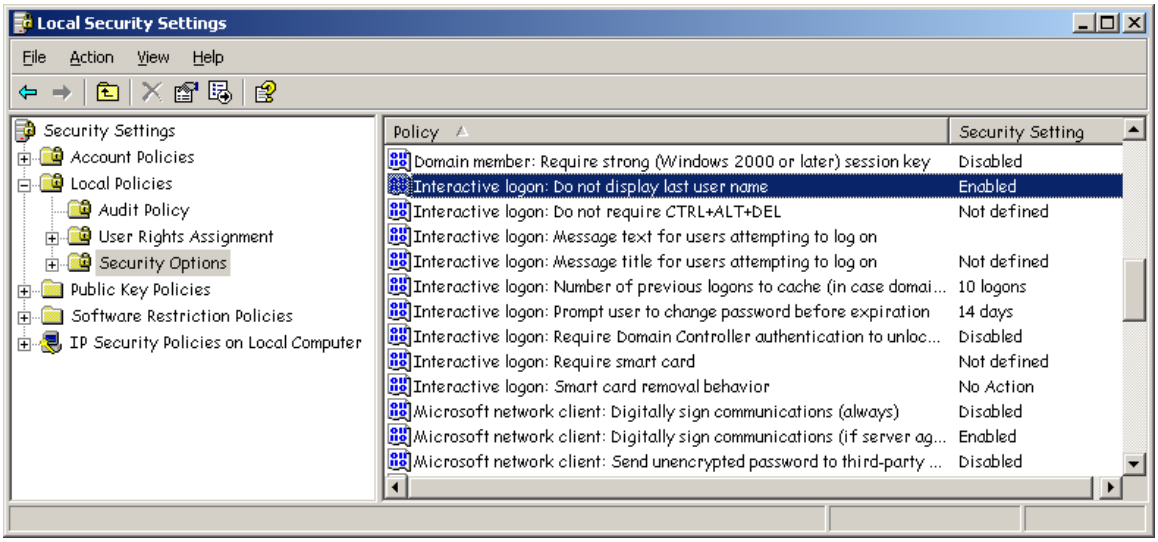
Select Start → Run…
Enter the command “regedit.exe” (without quotes)
When the registry windows pops up
Double click (expand) HKEY_LOCAL_MACHINE
Double click (expand) SOFTWARE
Double click (expand) Microsoft
Double click (expand) Windows NT
Double click (expand) CurrentVersion
Select Winlogon
In the right pane select and double click the value “Userinit”
Set the “Value data” to a zero ‘C:\Windows\System32\Userinit.exe,’ (without quotes)
Reboot the PC.

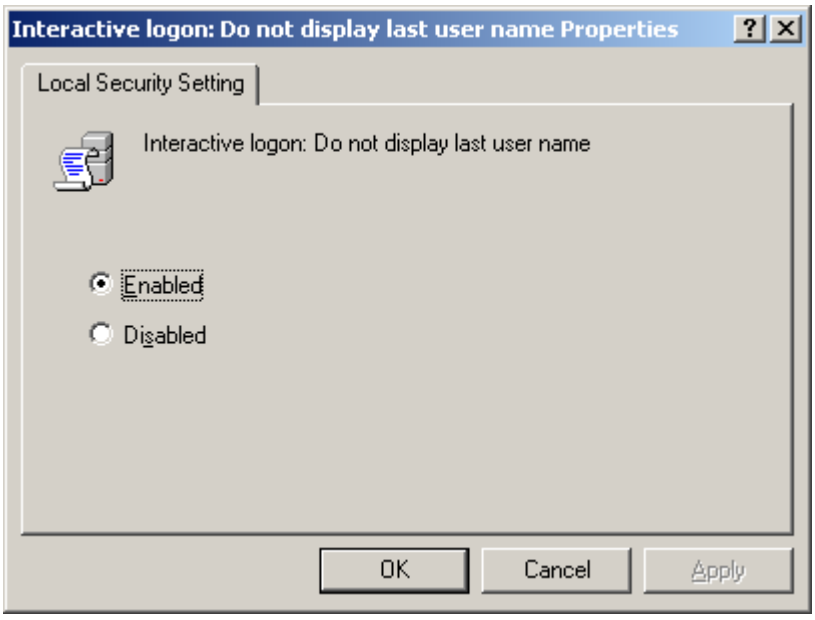
2.2 - Disable Display of Last User - intermediate

Windows XP Pro (feature not available in XP Home)

Presentation of user list. There are two pieces of information that generally allow someone to use a PC. User ID and User Password. By displaying a list of users on the login screen you have just given away half of that information.

To disable the display of the last user on the logon screen
Select Start → Settings → Control Panel → Administrative Tools → Local Security Policy
Select and double click "Interactive logon: Do not display last user name"
Select “Enabled”





2.3 - Use of NTFS File System - intermediate

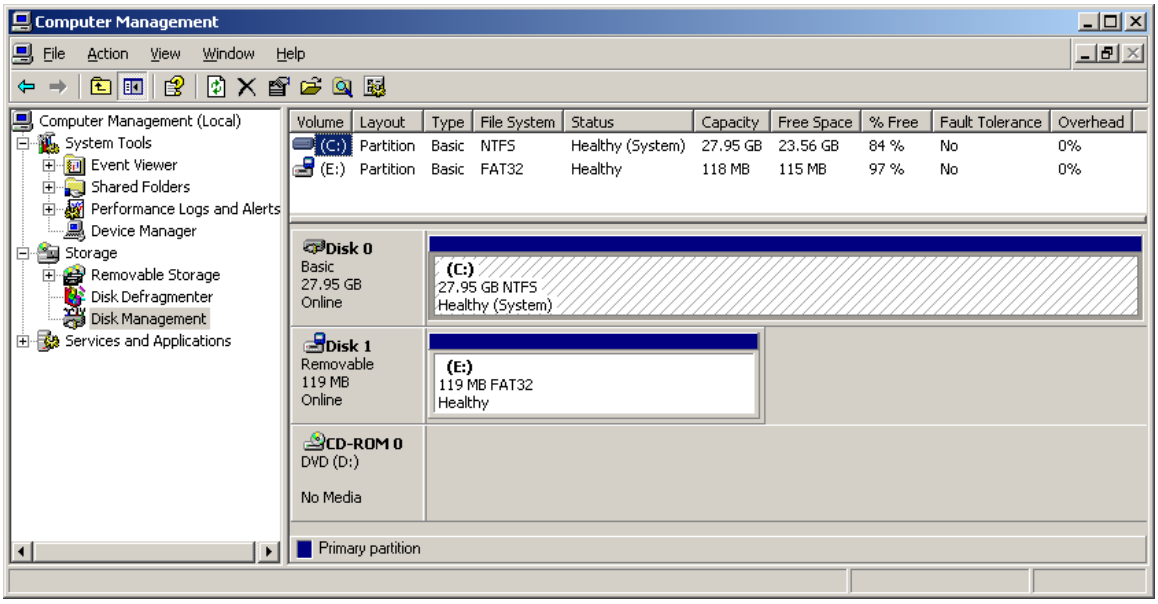
Microsoft typically provides two types of file systems for use with the Windows OS, FAT32 and NTFS.

FAT32 is an older and more basic file system that dates back to Windows 95 and Windows 98. FAT32 has little to no security measures built in and all users can see all the files on the system.

NTFS is a newer file system that was introduced in Windows NT and continued in Windows 2000 and Windows XP. By default most pre-built systems purchased from a store or manufacturer will normally have NTFS pre-installed. NTFS allows for the segmentation and separation of files. User A cannot see User B's files unless User B explicitly shares those files. Also included are many other security features.

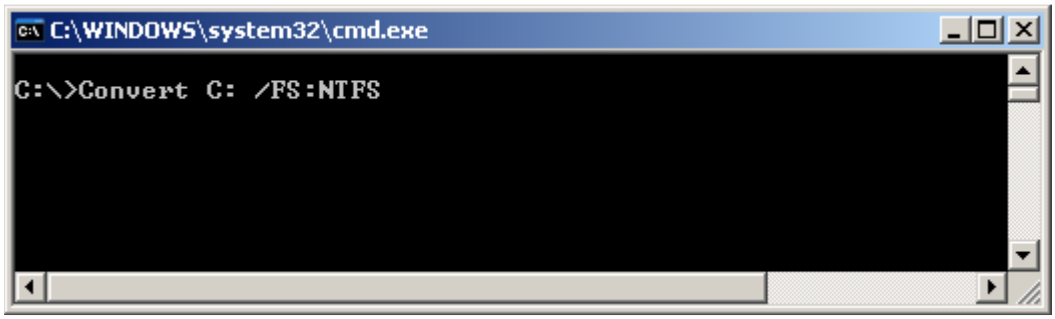
**NOTE – *A user with administrator permissions can see and view the files owned by other users, regardless of share permissions.*

To check which file system is in use on your system
Select Start → Settings → Control Panel → Administrative Tools → Computer Management → Disk Management
This will display all the drives in your system and their current settings. You should see something like (C:) 80 GB NTFS



IF your system is currently using FAT32 and FAT32 is not absolutely required it is recommended that your convert the system to NTFS.
** **CAUTION** - *This is a one way process and once the system is set to NTFS it cannot be returned to FAT32. In order to reinstate the FAT32 file system the hard drive must be wiped and reformatted.*

To convert the file system
Open a Command Prompt window
Select Start → Run, and enter 'cmd.exe' (without the quotes)
Select 'OK'
At the command prompt enter the following command (without the quotes)
'CONVERT C: /FS:NTFS' and hit enter.

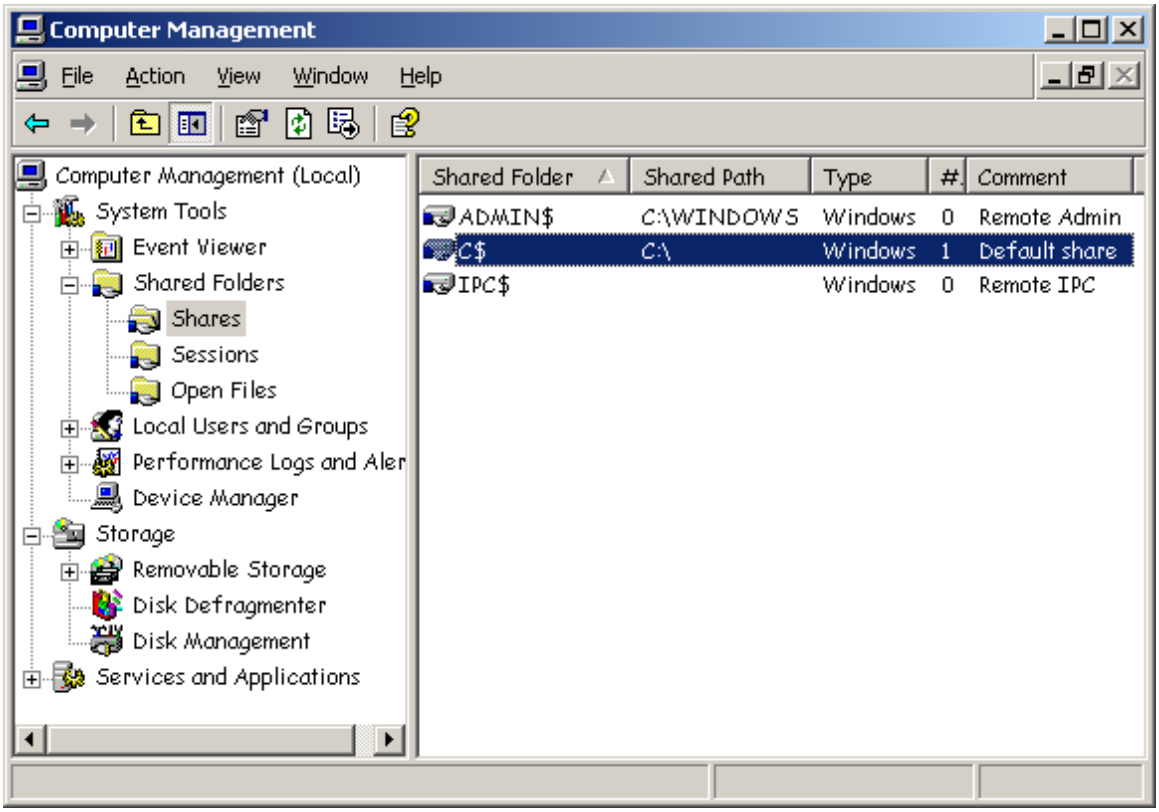


2.4 - Disable File Shares - intermediate

Shares are powerful, useful, and can be potentially dangerous.

It is recommended that shares that are not absolutely required be disabled. If a share is required ensure that the share is limited in scope to specific users, folders, and files.

To Disable a Share
Select Start → Settings → Control Panel → Administrative Tools → Computer Management
In the right pane Select Shares
In the left pane right click on the desired share and select “Stop Sharing”



More information on Shares can be found at:
http://support.microsoft.com/?kbid=304040

http://support.microsoft.com/default.aspx?scid=kb;EN-US;307874

http://www.microsoft.com/windowsxp/using/security/learnmore/sp2firewall.mspx

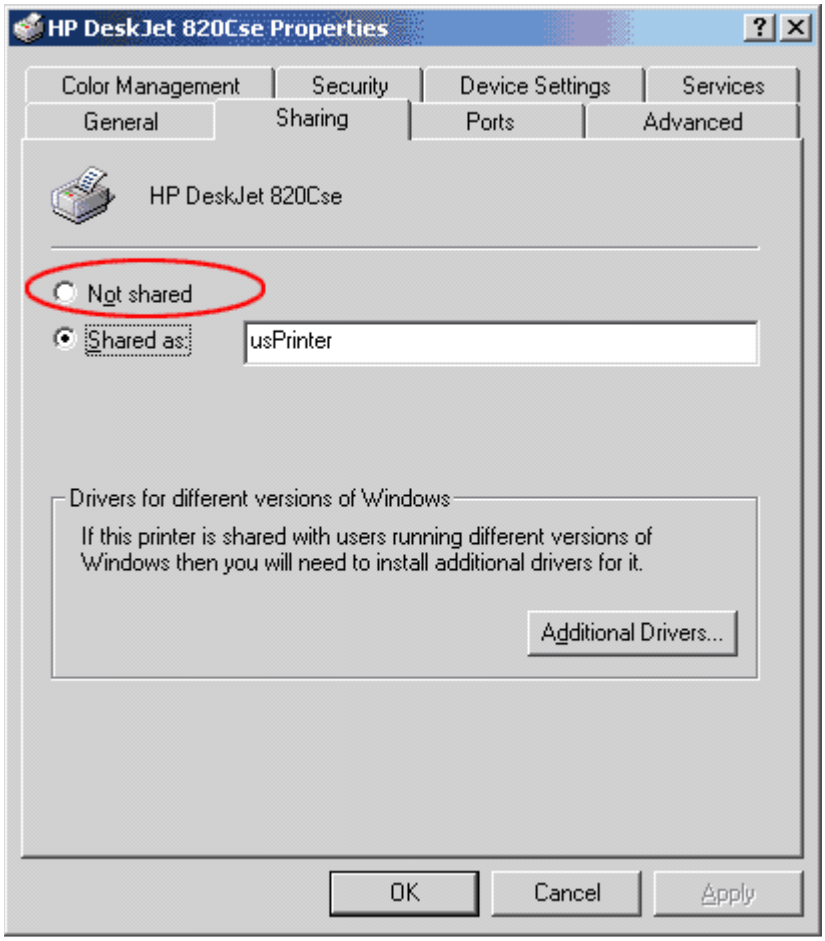
---

2.5 - Disable Print Shares - intermediate

Most users will have no reason to share a local printer.
Print shares should only be used when absolutely necessary.

To disable a Print Share
Select Start → Settings → Printers and Faxes
If you have any Print Shares the icon will be of a printer with a hand under it

Right click the printer you wish to disable sharing for
Select "Sharing…"
Select "Not Shared"



More information on Printer Shares can be found at:
http://www.microsoft.com/windowsxp/using/security/learnmore/sp2firewall.mspx

---

2.6 - Restrict Anonymous - intermediate

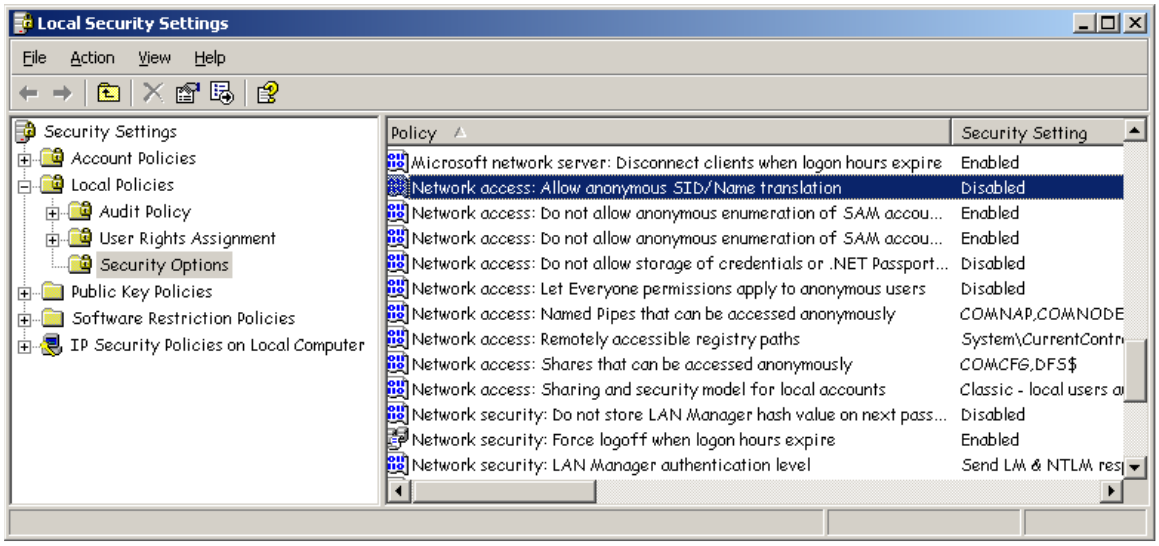
Windows systems are intended for ease of use and the ability to quickly establish communications with other systems. This is good for the usability of the system by new and novice users however this imposes several security risks. By default Windows 2000 and Windows XP (prior to Service Pack 2) allow for anyone to view key information about your system that is best kept private. This information in the hands of a less than nice person can give them a

head start to compromising your system. With the release of Windows XP Service Pack 2 Microsoft started to close some of these settings however they should be verified by the user.

The following Settings will affect the ability for any remote system to connect to your system and gain information such as a list of known users, known shares, if a user has a password or has a blank password, etc.

Restrict Anonymous via the Local Security Policy. (Windows XP Pro only)
** NOTE – *Windows Home does not have the Local Security Policy GUI and changes are made directly to the registry, see below.*

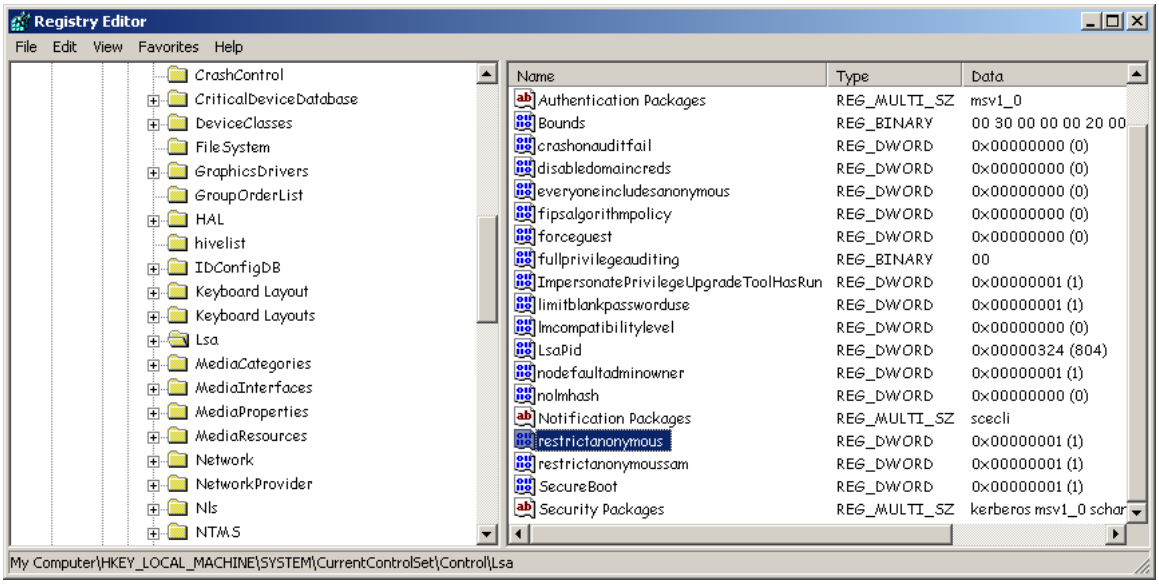
To access the Local Security Policy
Select Start → Settings → Control Panel → Administrative Tools → Local Security Policy
In the right pane select "Security Options"
In the left pane
Double Click "Network access: Allow anonymous SID/Name translation"
Select "Disabled"
Double Click "Network access: Do not allow anonymous enumeration of SAM accounts"
Select "Enabled"
Double Click "Network access: Do not allow anonymous enumeration of SAM accounts and shares"
Select "Enabled"
Double Click "Network access: Let Everyone permissions apply to anonymous users"
Select "Disabled"

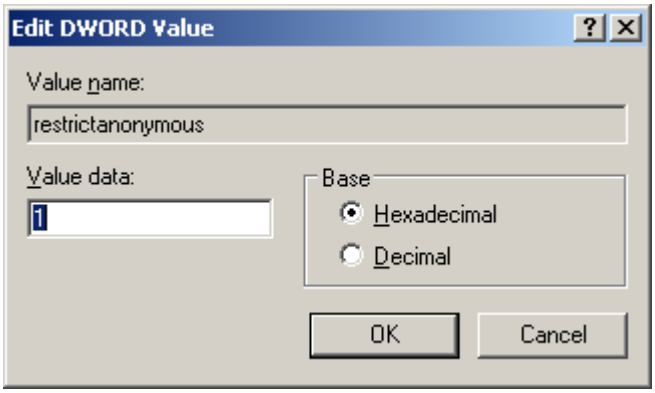


Alternately you can modify the registry (Windows XP Pro and Windows Home)
** NOTE - *This change is a registry edit. Before making changes to the registry the user should back up the registry.*

Select Start → Run…
Enter the command "regedit.exe" (without quotes)
When the registry windows pops up
Double click (expand) HKEY_LOCAL_MACHINE
Double click (expand) SYSTEM
Double click (expand) CurrentControlSet

Double click (expand) Control
Select LSA
In the right pane select and double click the value “restrictanonymous”
Set the “Value data” to a one 1





Repeat this for the following values.
In the right pane select and double click the value “restrictanonymoussam”
Set the “Value data” to a one 1
In the right pane select and double click the value “everyoneincludesanonymous”
Set the “Value data” to a zero 0
Reboot the PC.

More information on the Restrict Anonymous can be found at:
http://support.microsoft.com/kb/143474/

2.7 - Rename Administrator Account – Intermediate

It is not necessary however it is fairly common practice to rename the Administrator Account. ** ** NOTE - *In some operating systems older than Windows XP such as Windows 2000 this can actually cause problems with the system.*

Every Windows system has an Administrator account and as such this account is commonly targeted by crackers and malware. If you desire that extra edge in "hiding" your user accounts you can rename the Administrator account.

To Rename Administrator (Windows XP Home)
Select Start → Settings → Control Panel → User Accounts
Select and double click the account you wish to rename
Select "Change My Name"
Enter a new name

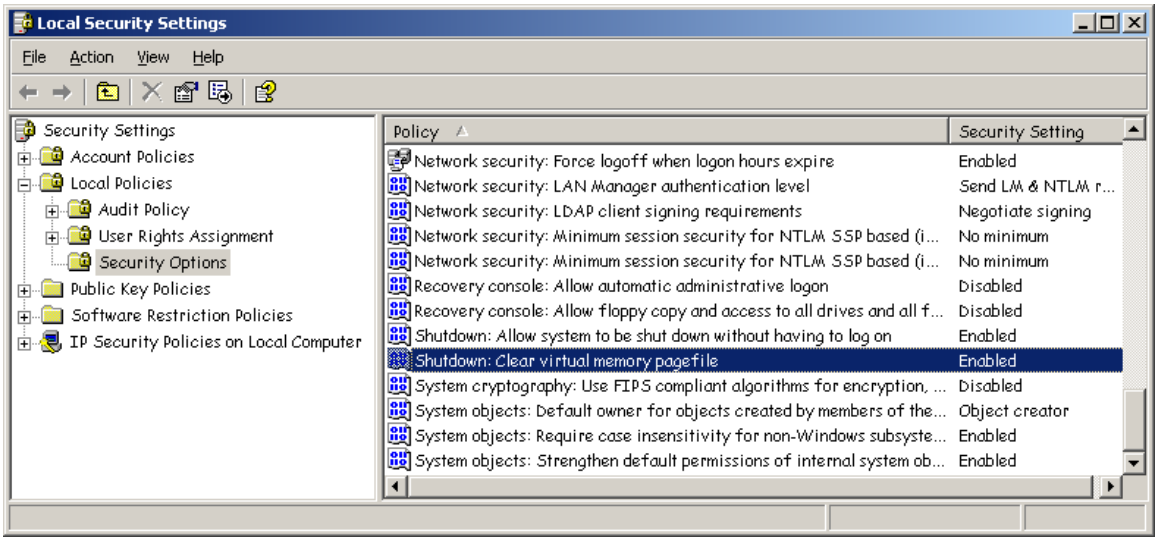
To Rename Administrator (Windows XP Pro)
Select Start → Settings → Control Panel → User Accounts
Select the account you which to rename
Select "Properties"
Enter a new name

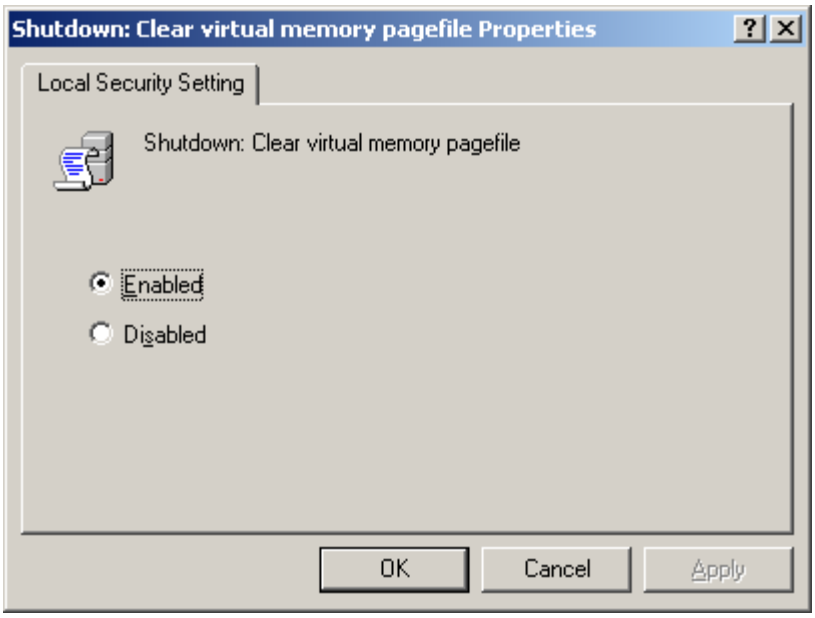
2.8 - Clear Page File on Shutdown - intermediate

Windows XP Pro (feature not available in XP Home)

As the Dump File can contain sensitive information so can the Page File. It is recommended these files be cleared upon shutdown.

To clear Page Files on Shutdown
Select Start → Settings → Control Panel → Administrative Tools → Local Security Policy
Select and double click "Shutdown: Clear virtual memory pagefile"
Select "Enabled"

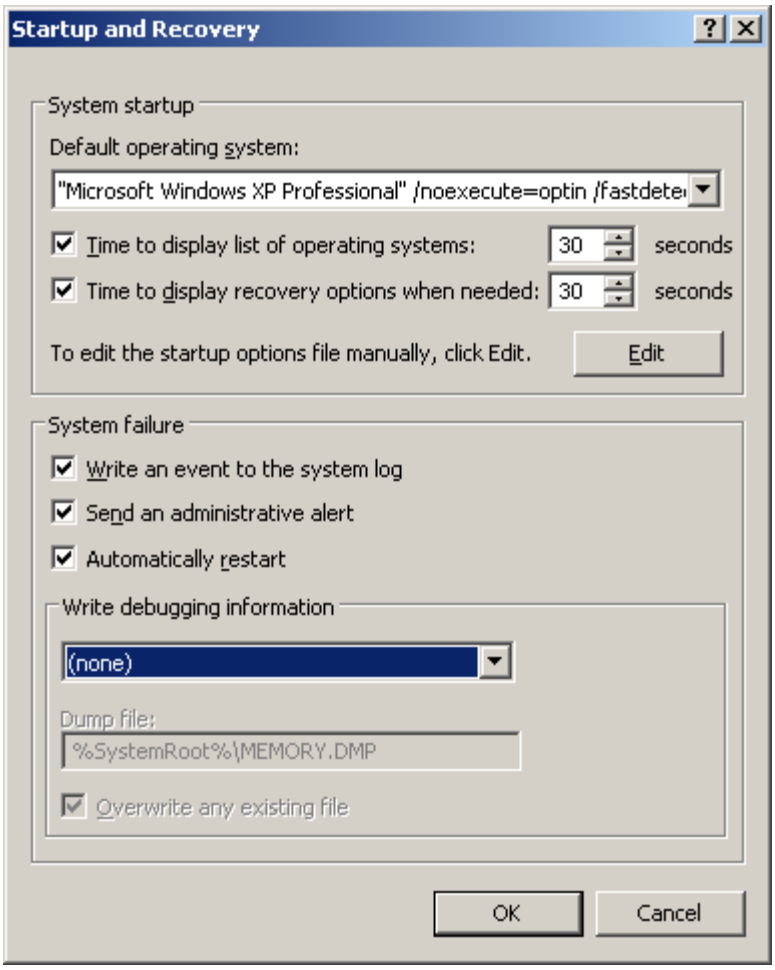




2.9 - Disable Dump Files Creation - intermediate

Dump files can be useful when troubleshooting the system or when debugging system development. Most users however will not look at a dump file during the course of their system usage. Dump files can contain sensitive information such as user names and passwords.

To Disable Dump File Creation
Select Start → Settings → Control Panel → System
Select the “Advanced” tab
In the “Startup and Recovery” section select “Settings”
Change the value for “Write debugging information” to ‘none’



2.10 - Install Third Party Firewall - intermediate

Windows XP Service Pack 2 comes with a firewall built into the Windows OS. This native firewall is free and a good start for host based firewall protection. However the native Windows firewall is limited in its configuration options. The Windows XP Firewall only blocks inbound network traffic, that is network communications originating from a remote system on the internet attempting to talk to or enter your PC. All outbound traffic is automatically passed by the Windows XP firewall without inspection. This is important to note because if you machine gets compromised, let's say with a spam bot that performs mass email distribution, the Windows XP firewall will do nothing to stop the 80,000 email messaged coming out of your PC.

If you install and use a commercial or open-source firewall that inspects both inbound and outbound traffic you can more tightly control not only who is able to talk to your PC, but with whom your PC is able to talk. Keep in mind that most firewalls will have few rules by default and you must ensure that they are configured properly based on your typical network functions. You may have to read more about TCP/IP to get the most out of your firewall.

Symantec Endpoint Protection has a built in firewall. Check your settings to ensure that these capabilities are enabled.

**NOTE – *If you choose to use a third party firewall instead of the Windows XP firewall it is recommended that you disable the Windows XP firewall.*

UT Arlington provides a copy of Symantec Endpoint Protection free of cost to all active and current UT Arlington Students, Faculty, and Staff. This software can be acquired on-line or at the Computer Store in Ransom Hall.
**NOTE - *The Computer Store has CD's of the program for five dollars ($5 USD). This cost is for the physical media and packaging overhead, not the software itself.*

The UT Arlington Anti-Virus website is
http://www.uta.edu/antivirus

---

3 - ADVANCED FEATURES

3.1 - Disable Unnecessary Services - advanced

If you are NOT running a Server version of Windows (Windows 2000 Server, Windows Server 2003, etc.) the default services should be fine and should not require modification.

If you are running a Server version or really need that extra fine tuning modify your services at your own risk. Details about the various services available on a Windows system is outside the scope of this check list and should be researched thoroughly by a user before attempting any changes to service settings.

3.2 - Use of Windows Security Policies - advanced

** This feature is not available on Windows XP Home

Windows has various templates available for use ranging from very open (insecure) to very closed (secure). Some of the more secure templates may "break" an application or a communications channel on which you rely. These templates are meant as starting points and can be customized to fit your needs. There are also third party templates that can be downloaded such as the NSA security template. However use of third party templates requires great caution and the source of the template should be verified before it is used.

More information on Security Policy Templates can be found at:
http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/xpsgch04.mspx

---

3.3 - Disable Boot From Removable Media – advanced

Many systems will check for the existence of a floppy disk, bootable CD-Rom, or bootable DVD during start up. This practice can allow foreign media to be inserted into the PC and allow for malicious code to be executed.

To prevent such activity it is a common practice to configure a PC to boot directly from the internal hard drive as its default setting.
**NOTE - *This counter measure is more for the assurance against very blatant mistakes. If you need to boot from a CD-Rom of other removable media this setting will have to be modified each time you wish to do so. An attacker with physical access can easily change this setting if the BIOS setup is not password protected.*

To disable booting from removable media
Enter your systems BIOS setup (performed at initial power up)
Each system varies in how the BIOS is called (F2, alt+del, shift+del, etc)
Within the menu structure there should be an entry for “Boot Order” or “Power Up Options”.
Ensure that the internal hard drive is the primary boot device.
Save and Exit
Reboot system

3.4 - Password Protect System BIOS - advanced

As stated above if the BIOS is not password protected anyone with physical access to your PC can change various configuration settings.

To password protect the system BIOS
Enter your systems BIOS setup (performed at initial power up)
Each system varies in how the BIOS is called (F2, alt+del, shift+del, etc)
Within the menu structure there should be an entry for “Security” or “Password Protection”.
Enter a password where appropriate
Save and Exit
Reboot system

3.5 - Enable EFS - advanced

Windows XP Pro (feature not available in XP Home)

EFS (Encrypting File System) is the native Windows encryption for the system hard drive. This encryption when applied to the hard drive, folders, or files will prevent someone from reading the data on the hard drive if the hard drive is removed from your PC and connected to another PC or device as a slave.

**NOTE enabling encryption can have negative consequences. Before enabling encryption be sure to understand the Pros and Cons of encryption and measure its benefit to you and your system. In the event you forget your password your data will remain encrypted and unreadable without the use of specialized software.

Encryption is becoming more common and is especially gaining industry recognition and often mandated via corporate policy for mobile devices (laptops, PDA’s, “smart” cell phones, etc.). Encryption concepts are beyond the scope of this checklist however many resources can be found with a simple search engine query.

To learn more about Microsoft EFS
http://www.microsoft.com/technet/security/guidance/cryptographyetc/efs.mspx

There are also other encryption products for use such as PGP and the open source GPG.
See Install Third Party Encryption Software.

3.6 - Encrypt Offline Cache - advanced

If encryption is used you should also encrypt the locations that Microsoft uses for files that are actively being used and / or modified. Windows stores copies of files but does not always clean up those copies.

3.7 - Encrypt Temp - advanced

If encryption is used you should also encrypt the locations that Microsoft uses for files that are actively being used and / or modified. Windows stores copies of files but does not always clean up those copies.

3.8 - Install Third Party Encryption Software - advanced

Encryption is becoming more common and is gaining industry recognition and often mandated via corporate policy especially for mobile devices (laptops, PDA's, "smart" cell phones, etc.).

If you choose to operate your PC with encryption keep in mind that there are typically two models of encryption that can be implemented typically in one of two ways.
Symmetric Key Encryption – commonly referred to as shared key. This encryption model uses a single key or password to perform both the encryption and decryption and must be shared with each person that will access the data. Because the key must be shared it is typically considered less secure.
Asymmetric Key Encryption – commonly referred to a Public Key Infrastructure. This encryption model uses two keys a Public Key used to encrypt the data and a Private key used to decrypt the data.
Whole Disk Encryption – can be implemented to encrypt the entire hard drive of a system and takes effect at the BIOS or boot level of the system. If you forget your password your PC is effectively reduced to a paper weight. Be extremely careful when implementing whole disk encryption.
File System Encryption – is implemented by encrypting a portion of the hard drive, called a partition. This means of encryption is independent of the system BIOS and boot operations, as such it is typically the preferred method of encryption for USB drives.

Before you perform any encryption operations it is extremely important that you understand the software of choice and preferably have thoroughly tested it on a "spare" PC or hard drive. Also ensure that ALL your data is backed up before using any encryption software.

Some encryption vendors include
PGP - http://www.pgp.com/
TrueCrypt - http://www.truecrypt.org/

---

4 - LINKS AND REFERENCES

Links:
UT Arlington Antivirus (Symantec)
- http://www.uta.edu/antivirus

Microsoft Update
- http://www.update.microsoft.com/

Microsoft MBSA
- http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Microsoft Malicious Software Removal Tool
- http://www.microsoft.com/security/malwareremove/default.mspx

Microsoft Windows Defender
- http://www.microsoft.com/windows/products/winfamily/defender/default.mspx

Spybot Search and Destroy
- http://www.safer-networking.org/en/

Lavasoft Ad-aware
- http://www.lavasoft.com/software/adaware/

Secunia PSI
- http://www.secunia.com
- https://psi.secunia.com/

Technical References:
Passwords
- http://www.microsoft.com/athome/security/privacy/password.mspx
- http://www.microsoft.com/athome/security/privacy/password_checker.mspx
- http://www.lockdown.co.uk/?pg=combi&s=articles
- http://www.google.com/search?hl=en&q=password+mnemonics&btnG=Google+Search

File Shares
- http://support.microsoft.com/default.aspx?scid=kb;EN-US;307874
- http://support.microsoft.com/?kbid=304040

AutoPlay
- http://support.microsoft.com/default.aspx?scid=KB;EN-US;953252

Audit Logs
- http://support.microsoft.com/?kbid=310399

Microsoft Patches
- http://www.microsoft.com/technet/security/bulletin/advance.mspx
- http://www.microsoft.com/athome/security/update/bulletins/default.mspx
- http://www.microsoft.com/downloads/Browse.aspx?displaylang=en&categoryid=7
- http://blogs.technet.com/msrc/
- http://blogs.technet.com/swi/

Microsoft Shares
- http://support.microsoft.com/?kbid=304040
- http://support.microsoft.com/default.aspx?scid=kb;EN-US;307874
- http://www.microsoft.com/windowsxp/using/security/learnmore/sp2firewall.mspx

Microsoft Anonymous Enumeration
- http://support.microsoft.com/kb/143474/

Microsoft Security Policy Templates
- http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/xpsgch04.mspx

Microsoft EFS
- http://www.microsoft.com/technet/security/guidance/cryptographyetc/efs.mspx

Source References:
http://labmice.techtarget.com/articles/winxpsecuritychecklist.htm

http://labmice.techtarget.com/articles/securingwin2000.htm

http://www.securityfocus.com/columnists/220