070-270

TEST KING

LEADING THE WAY IN IT
TESTING AND CERTIFICATION TOOLS!

Study Guide

Installing, Configuring and Administering

Microsoft Windows XP Professional

Version 3.0

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ACRONYMS

ACL	Access Control List
ACPI	Advanced Configuration And Power Interface
AD	Active Directory
APM	Advanced Power Management
APIPA	Automatic Private Internet Protocol Addressing
CA	Certificate Authority
CAL	Client Access License
DHCP	Dynamic Host Control Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
EFS	Encrypting File System
FEK	File Encryption Key
GPO	Group Policy Object
GPT	Group Police Template
HCL	Hardware Compatibility List
IAS	Internet Authentication Services
ICF	Internet Connection Firewall
ICS	Internet Connection Sharing
IPSec	Internet Protocol Security
L2TP	Layer Two Tunnelling Protocol
LDAP	Lightweight Directory Access Protocol
LPD	Line Printer Daemon
MMC	Microsoft Management Console
NAT	Network Address Translation
NFS	Network File System
NTFS	NT File System
ODBC	Open Database Connectivity
OSI	Open Systems Interconnection (Model)
OU	Organizational Unit
PCMCIA	Personal Computer Memory Card Interface Adapter
PnP	Plug and Play
PPP	Point To Point Protocol

PPTP	Point To Point Tunnelling Protocol
PXE	Preboot Execution Environment
RAS	Remote Access Service
RIPrep	Remote Installation Preparation
RIS	Remote Installation Services
RRAS	Routing And Remote Access Service
SAM	Security Accounts Manager
SMP	Symmetric Multiprocessing
SMS	Systems Management Server
Sysprep	System Preparation
TFTP	Trivial File Transfer Protocol
UDF	Unique Database File
UNC	Universal Naming Convention
VPN	Virtual Private Network
WDM	Windows32 Driver Model

Installing, Configuring, and Administering Microsoft Windows XP Professional

Exam Code: 070-270

Certifications:

Microsoft Certified Professional (MCP)	
Microsoft Certified Systems Administrator (MCSA)	**Core**
Microsoft Certified Systems Engineer (MCSE)	**Core**
Microsoft Certified Systems Engineer 2003 (MCSE 2003)	**Core**

Prerequisites:
A+ certification or equivalent knowledge
Net+ certification or equivalent knowledge

About This Study Guide
This Study Guide provides all the information required to pass the Microsoft 70-270 exam – Installing, Configuring, and Administering Microsoft Windows XP Professional. It however, does not represent a complete reference work but is organized around the specific skills that are tested in the exam. Thus, the information contained Study Guide is specific to the 70-270 exam and not to Windows XP Professional. It includes the information required to answer questions related to Windows 2000 Professional, Windows 2000 Server, Windows NT 4.0, and UNIX that may be asked during the exam. Topics covered in this Study Guide includes installing Windows XP Professional; implementing and conducting administration of resources; implementing, managing, and troubleshooting hardware devices and drivers; monitoring and optimizing system performance and reliability; configuring and troubleshooting the desktop environment; implementing, managing, and troubleshooting network protocols and services; and implementing, monitoring, and troubleshooting security.

Intended Audience
This Study Guide is targeted specifically at people who wish to take the Microsoft MCSE exam 70-270, Installing, Configuring, and Administering Microsoft Windows XP Professional. This information in this Study Guide is specific to the exam and is not a complete reference work.

How To Use This Study Guide
To benefit from this Study Guide we recommend that you:

- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work

Note: Remember to pay special attention to these note boxes as they contain important additional information that is specific to the exam.

- Perform all labs that are included in this Study Guide to gain practical experience, referring back to the text so that you understand the information better. Remember, it is easier to understand how tasks are performed by practicing those tasks rather than trying to memorize each step.
- Be sure that you have studied and understand the entire Study Guide before you take the exam.

Good luck!

1. Installing and Deploying Windows XP Professional

You can install Windows XP Professional directly from the CD-Rom or from a network share. The Windows XP Professional installation process consists of four stages:

Stage 1: Hard Drive Preparation. In text mode Setup checks the hard drive for consistency and errors. It allows you to format and create the Windows XP Professional partition if you need to and copies setup files to the hard drive. Setup then reboots the computer.

Stage 2: Setup Wizard. The graphical user interface Setup Wizard gathers information from you; such as regional settings, your name and organization, the Windows XP Professional CD-key, and computer name. Creates the local Administrator user account and requests a password for it.

Stage 3: Installing Network Components. After the Setup Wizard has gathered the necessary information from you in Stage 2, it begins the network components installation. It detects your network adapter card; allows you to choose which network components, such as the network client, file and printer sharing and protocols, to install; allows you to join a workgroup or domain; and installs the components you have chosen.

Stage 4: Completing the installation. The Setup Wizard completes the installation by installing the start-menu items and applying and saving the configuration settings you chose in the previous stages. It then deletes the temporary setup files and reboots the computer.

Typical Network Settings

When you install Microsoft Windows XP Professional, you can either install the 'Typical Network Settings' or 'Customized Network Settings'. The Typical Network Settings installs:

- **Client for Microsoft Networks**
- **File and Printer Sharing**
- **TCP/IP**
- **DHCP**

1.1 System Requirements

Before installing Windows XP Professional, you must ensure that the computer meets the minimum system requirements as indicated in Table1.1.

TABLE 1.1: *Windows XP Professional System Requirements*

Hardware	Minimum Requirement
Processor	Intel Pentium 2 233 MHz (300 MHz recommended)
Memory	64 MB Ram (128 MB Ram recommended)
Hard disk space	2 GB with an additional 1.5 GB free space (2 GB free space recommended)
Networking	Network adapter card
Display	Video display adapter card and VGA monitor
I/O devices	Keyboard and mouse or other pointing device

Note: Windows XP Professional offers support for a maximum of 2 processors and a maximum of 4 GB Ram

1.2 Installing Windows XP Professional from the CD-Rom

When installing Windows XP Professional from the CD-Rom you can either boot directly from the CD-Rom or, if your computer system does not support booting from the CD-Rom, you can create boot disks.

1.2.1 Booting from the CD-Rom.

In your system BIOS set the CD-Rom drive as the ***First Bootable Device***. This is usually set in the ***BIOS Feature Setup***. While you are in the BIOS Setup you should also check that ***Boot Sector Virus Protection*** is disabled. The Boot Sector Virus protection prevents any attempt is made to write to the hard drive's boot sector or partition table. When BIOS detects an attempt to write to the boot sector it stops the computer and display an error message. The Windows XP Professional Setup program must write to the boot sector, therefore the ***Boot Sector Virus Protection*** must be disabled.

Once you have configured the BIOS, place the Windows XP Professional Installation disk in the CD-Rom drive and reboot the computer. During the boot process you will be prompted to ***press any key to boot from CD-Rom***. Once you have pressed a key the Installation of Windows XP Professional will begin.

1.2.2. Booting from boot disks.

If your computer system does not support booting from the CD-Rom, you will have to create boot disks on a computer that has an operating system installed on it already. Unlike the Windows 2000 Installation CD, the Windows XP Professional Installation CD does not contain a *makeboot.exe* utility. The Windows XP Professional *makeboot* utility must be downloaded from the Microsoft website at http://www.microsoft.com/downloads/release.asp?releaseid=33291. This file can be used to create the Windows XP Professional boot disks and requires 6 high density floppy disks. These disks can then be used to boot the computer and will load the necessary drivers required to access the CD-Rom drive.

> **Note:** Boot disks operate in a **16-bit DOS mode** environment. You therefore cannot use *winnt32.exe* to install Windows XP Professional as *winnt32.exe* is **32-bit** application. You must use *winnt.exe* which is the 16-bit equivalent of *winnt32.exe*, instead.

1.3 Installing Windows XP Professional over the network.

To install Windows XP Professional over the network you must copy the **i386** folder from the Windows XP Professional Installation CD to a shared folder on the network. You must prepare the client computer by creating a 1.5 GB FAT32 partition (2 GB recommended) that Windows XP Professional will copy the installation files to.

> **Note:** This partition must be formatted with the FAT32 file system and not the NTFS file system as network boot disks, which operate in a MS-DOS mode environment, cannot access a NTFS formatted partition.

You must also ensure that the computer has a can connect to the network share when it has booted. To be able to boot to the network share the computer must have a **PXE compliant** network adapter. If the computer cannot be booted over the network you will have to create a network boot disk for the computer. A boot disk can be created by using the *rbfg.exe* utility. If you must use a boot disk to boot the computer, you will have to run *winnt.exe* to install Windows XP Professional. Boot disks operate in a **16-bit DOS mode**

environment. You therefore cannot use *winnt32.exe* to install Windows XP Professional as *winnt32.exe* is **32-bit** application.

1.4 Performing an unattended installation.

Microsoft allows for the automated installation of Windows XP Professional through unattended installations. There are three mechanisms through which an unattended installation can be performed. These are through:

- unattended answer files;
- disk imaging using the System Preparation Tool; and
- remote Installation Services

1.4.1 Using an unattended answer file.

The first mechanism you can use to perform an unattended installation of Windows XP Professional is to use an **answer file** (*See Figure 1.1*). An answer file is an automated script that supply's the Windows XP Professional Setup program with all the information it would require during the installation.

You can use **Setup Manager** to create and modify an answer file. Setup Manager is located in the *deploy.cab* file in the *support/tools* folder on the Windows XP Professional Installation CD and can be extracted to your computer by double-clicking on the *deploy.cab* file. This will display the files contained in the *deploy.cab* file. Right-click on the files and select **Extract** on the menu that pops up.

You can use Setup Manager to create an answer file for an unattended installation, a sysprep install, and for a Remote Installation Services. You can also choose the level of automation. This can be:

Figure 1.1: *An Answer File*

- **Provide Defaults:** The answer file provides defaults that the user can see and allows the user to accept or change these settings during the installation.
- **Fully Automated:** No input is required from the user and the user cannot alter any of the settings.
- **Hide Pages:** All pages that the answer file provides answers for are hidden from the user.
- **Read Only:** The user can view any of the answers on the pages that are not hidden but cannot change them.
- **GUI Attended:** The first stage of the installation is automated but the user must supply the information required by the Setup Wizard during the graphical user interface stage (stages 2 and 3) of the installation.

Note: When creating a **Fully Automated** answer file, you must include all the information the Setup Wizard requires during the Installation this includes Product key, which must be specified in the **ProductID** variable in the **UserData** portion of the answer file. (*See Figure 1.1*) If the ProductID is missing the installation is stopped during the graphical user interface stage and the following error message is displayed:

```
Unattended Setup is unable to continue because a Setup parameter
specified by your system administrator or computer manufacturer
is missing or invalid.
```

The Answer File can be used in conjunction with a **Uniqueness Database File** (UDF). The latter provides multiple replacement settings for the settings configured in an **Answer File** and can be used to automate the installation of Windows XP Professional on **multiple client computers**.

The syntax for using the Answer file and the UDF file is:

- Answer File **winnt [/s:*sourcepath*] [/t:*drive*] [/u:*answer_file*]**
  winnt32 [s:/*sourcepath*] [/t:*drive*] [/u:*answer_file*]
- UDF File **winnt [/s:*sourcepath*] [/t:*drive*] [/u:*answer_file*] [/udf.id:[*UDF_file*]]**
  winnt32 [/s:*sourcepath*] [/t:*drive*] [/u:*answer_file*] [/udf.id:[*UDF_file*]]

For an explanation of these switches see Table 1.5 and Table 1.6.

1.4.2 Using the System Preparation tool (disk imaging).

With disk imaging it is possible to install and configure Windows XP Professional and all the applications and application update packs on a test computer and then create an exact image of the hard drive that can then be used to install Windows XP Professional and the applications on other client computers. These computers that will become recipients of the disk image installation are also referred to as target computers.

During an installation that uses disk imaging, the source files on Windows XP Professional Installation CD are not used, except for the initial installation on the test computer. In other words, you would not be using winnt.exe or winnt32.exe to install the disk image on the target computers and thus will not run the Windows XP Professional Setup program. Therefore, you will not be detecting the hardware devices and installing the appropriate drivers on the target computers. As a result, all the target computers must have the same hardware configuration as the test computer. You will also have to change the computer name of all the target computers as each computer on the network must have a unique name.

Microsoft has created a **System Preparation tool** (*Sysprep.exe*) which solves some of the problems associated with disk imaging. You would use the Sysprep, after installing and configuring Windows XP Professional, the applications and application update packages on a test computer, to prepare the computer of disk imaging. You would then run the disk imaging program after Sysprep has completed. Sysprep adds a mini-Setup Wizard to the disk image that will request the user-specific information such as productID, user name, network configuration, etc, on the first reboot of the target computer. This information can either be supplied by the user or by an answer file.

When using answer file with the sysprep tool, a Sysprep folder must be created on the *%systemdrive%* of the test computer or a ***Sysprep.inf*** file must be created and saved to a floppy disk that must be inserted at the beginning of the mini-Setup Wizard. The Sysprep folder that is created on the target computer when the disk image is copied is automatically deleted when the mini-Setup Wizard is completed.

Sysprep can also be used to force the target computer to perform Plug and Play detection and to install the correct device drivers on the first reboot of the target computer; however, the target computer and the test computer must have identical hard disk controllers and compatible **Hardware Abstraction Layers**. The –pnp switch is used to force the target computer to detect its hardware configuration on its first reboot. A full list of Sysprep switches are listed in Table 1.2.

TABLE 1.2: ***System Preparation Tool Switches***

Switch	Description
/reboot	Restarts the test computer rather than allowing it to shut down after sysprep.exe is completed.
/quiet	Mini-Setup runs without user input. Requires an answer file.
/pnp	Forces Plug and Play detection on the target computer.
/nosidgen	Does not regenerate the SIDs on the target computers.

1.4.3 Using Remote Installation Services (RIS)

Remote Installation is the process of connecting to **Remote Installation Services** (RIS) server from a target computer and then performing an automated installation of Windows XP Professional on the target computer. This is the most effective method of deploying Windows XP Professional. Remote Installation allows administrators to install Windows XP Professional on client (target) computers throughout a network from a central location. It however requires that your network has a Windows 2000 server infrastructure in place and that the client computers support remote booting. A list of network services that the RIS server requires is listed in Tabe1.3.

TABLE 1.3: ***Network Services Required by RIS***

Network Service	Reasons for RIS Requirement
DNS Service	Required for locating the Active Directory directory service and client computer accounts
DHCP Service	Required for supplying IP addresses to client computers
Active Directory	Required for locating existing client computers and the existing RIS servers

1.4.3.1 Setting up the RIS server

To set up a RIS server, you must install RIS on a NTFS version 5 partition that is at least 2GB size and that does not contain the operating system, i.e. the boot partition, and is not the system partition, i.e. the startup partition, by running the RIS Setup Wizard. And you must specify a Remote Installation Folder that cannot be on a Distributed File System (Dfs) shared folder or on an Encrypting File System (EFS) volume.

The RIS creates and uses CD-based images and disk images. The process of creating the disk image is similar to the process required when using the sysprep tool; first install and configure Windows XP Professional on a test computer, install and configure your applications, apply application update packs and then use the **Riprep utility** to create a **Riprep image**. Unlike the Sysprep tool, however, RIS creates its own disk images and does not require third party software. The Riprep utility automatically removes the test computer's SID from the image and creates an answer file based on the configuration of the operating system on the test computer.

1.4.3.2 Client requirements for Remote Installation

To deploy the image on the client computers, the client computers must be able to connect to the RIS server by booting from the network adapter card. To do this the client computer requires a **PXE-compliant network adapter**, which has a special chip that supports network booting. If the computer does not have a PXE-compliant network adapter card, you must use the *rbfg.exe* file to make network a boot disk for the computer. The network boot disk can then be used to simulate the PXE boot process.

In addition, the user account that will be used to perform the installation must be assigned the right to 'Logon as a batch job' and must be assigned permissions to create computer accounts in the domain that they will be joining.

1.4.4 Deploying Software applications

1.4.4.1 Overview

In Windows 2000 and Windows XP Professional you can use a **Group Policy Object** (GPO) in conjunction with **Windows Installer** to automate and manage software installations, updates and removal from a centralized location. Group Policy can be used to assign the software application to a group of users that are organized into a unit (an Organizational Unit) and allow you to manage the various phases of software deployment.

GROUP POLICY

Group Policy and Organizational Units are related to the Administration and management of a Windows 2000 network. They are covered in detail in the TestKing Study Guide 70-217: Implementing and Administering a Microsoft Windows 2000 Directory Services Infrastructure exam and in the TestKing Study Guide 70-218: Managing a Microsoft Windows 2000 Network Environment. For the 70-270 exam you are not required to understand the intricacies of these tools. Therefore it will not be discussed in detail here.

There are four phases of software deployment:

- **Preparation:** preparing the files that allows you to use Group Policy to deploy the application software. This involves copying the Windows Installer package files to a software distribution point. The Windows Installer application files can be obtained from the application's vendor or can be created through the use of third-party utilities.
- **Deployment:** the administrator creates a Group Policy Object (GPO) that installs the software on the target computers and links the GPO to the appropriate Organizational Unit. During this phase the software is installed.
- **Maintenance:** the software is upgraded with a new version or redeployed with a patch or a service pack.
- **Removal:** to remove software that is no longer required, you must remove the Windows installer package from the GPO that was used to deploy the software. The software is then automatically removed when a user log on or when the computer restarts.

1.4.4.2 Windows Installer

Windows Installer consists of Windows Installer **service**, which is a client-side service, and Windows Installer **package**. Windows Installer package uses the ***.msi*** file extension and contains all the information that Windows Installer services requires to install the software. The software developer provides the Windows Installer package with the application. If a Windows Installer package does not come with an application, you can create a Windows Installer package or repackage the application, using a third-party utility. Alternatively you could create an application file (.zap) that uses the application's existing setup program. A .zap file is not a native Windows Installer package.

Advantages of using Native Windows Installer packages:

- **Automatic File Repair** when a critical application file becomes corrupt. The application automatically returns to the installation source to retrieve a new copy of the file.
- **Clean Removal** without leaving orphaned files and without deleting shared files used by another application.
- **Transformable.** You can customize a Windows Installer package to meet the requirements set by your company by using authoring and repackaging tools. Transformed Windows Installer packages are identified by the *.mst* file extension.
- **Patches.** Patches and upgrades can be applied to the installed applications. These patches use the *.msp* file extension.

> **Note:** A *.zap* file is not a native Windows Installer package and does not offer the same benefits as Windows Installer packages. It therefore does not support **automatic repairing** and cannot be transformed.

1.5 Upgrading to Windows XP Professional

You can upgrade Windows 98, Windows Millennium Edition, Windows NT Workstation 4.0 **Service Pack 6**, and Windows 2000 Professional directly to Windows XP Professional. However, Windows 3.1 and Windows 95 must first be upgraded to at least Windows 98 and can then be upgraded to Windows XP Professional. Windows for Workgroups 3.1, Windows NT Workstation 3.5, Windows NT Workstation 3.5.1 and Windows NT Workstation 4.0 must first be upgrade to at least Windows NT Workstation 4.0 Service Pack 6 and can then be upgraded to Windows XP Professional. Windows NT Server 4.0 and the various versions of Windows 2000 Server cannot be upgraded to Windows XP Professional. Windows NT Server 4.0 and the various versions of Windows 2000 Server are **server-based** Operating Systems while Windows XP Professional is a client-based Operating System.

> **Upgrading to Windows 2000 Professional and then to Windows XP Professional**
>
> **Windows for Workgroups 3.1 and Windows NT Workstation 3.5 cannot be upgraded directly to Windows 2000 Professional either. Windows for Workgroups 3.1 and Windows NT Workstation 3.5 must first be upgraded to Windows NT Workstation 3.5.1 or Windows NT Workstation 4.0 and can then be upgraded to Windows 2000 Professional before being upgraded to Windows XP Professional.**

TABLE 1.4: *Windows XP Professional Upgrade Paths*

Operating System	Upgrade Path
Windows 3.1	First upgrade to Windows 98 and then to Windows XP Professional

Windows for Workgroups 3.1	First upgrade to Windows NT Workstation 4.0 SP6 and then to Windows XP Professional
Windows 95	First upgrade to Windows 98 and then to Windows XP Professional
Windows 98	Upgrade directly to Windows XP Professional
Windows NT Workstation 3.5	First upgrade to Windows NT Workstation 4.0 SP6 and then to Windows XP Professional
Windows NT Workstation 3.5.1	First upgrade to Windows NT Workstation 4.0 SP6 and then to Windows XP Professional
Windows NT Workstation 4.0	First apply Service Pack 6 and then upgrade to Windows XP Professional
Windows 2000 Professional	Upgrade directly to Windows XP Professional

You can use Windows XP Professional to generate an **upgrade compatibility report** that can be used to check whether the devices and drivers on the existing operating system are compatible with Windows XP. You can generate this compatibility report by running the ***winnt32 /checkupgradeonly*** command or the ***Chkupgrd.*****exe** utility, which runs the Windows XP Readiness Analyzer but must be downloaded from Microsoft website. The */checkupgradeonly* switch of the *winnt32* command runs the first part of the Windows XP Professional Setup program and checks only for compatible hardware and software. For a full list of *winnt32* see Table 1.5 and for a full list of *winnt* switches see Table 1.6.

TABLE 1.5: ***WINNT32 switches***

Switch	Description
/checkupgradeonly	Checks the computer for upgrade compatibility with Windows XP
/copydir:*folder_name*	Creates a folder in the *systemroot* folder (which contains the Windows XP Professional system files).
/copysource:*folder_name*	Creates a folder in the *systemroot* folder. Files created with /copysource are automatically deleted after the installation is completed.
/cmd: *command_line*	Specifies a command to be run before the final phase of Setup.
/cmdcons	Adds a Recovery Console option to the operating system selection screen.
/debug[*level*] [:*file_name*]	Creates a debug log at the specified level.
/m:*folder_name*	Specifies that Setup must copy replacement files from another location and to look for files in that location first.
/makelocalsource	Specifies that Setup must copy all installation files to the hard drive.
/noreboot	Prevents Setup from rebooting the computer following the file copy phase. This enables a command to be entered by the user

	prior to completing setup.
/s:*source_path*	Specifies the source location of Windows XP Professional installation files.
/syspart:*drive_letter*	Copies Setup startup files to a hard disk and marks the drive as active. You can then install the drive on another computer. When you start that computer, Setup starts at the next phase. This requires use of the /tempdrive switch.
/tempdrive:*drive_letter*	Specifies a drive to contain temporary setup files and installs Windows XP Professional on that drive.
/unattend [number][:*answer_file*]	Performs an unattended installation using an answer file that provides your custom specifications to the Setup program.
/udf:id[,*udf_file*]	Indicates an identifier (ID) that Setup uses to specify how a Uniqueness Database File (UDF) modifies an answer file

Note: *winnt32.exe* is **32-bit** application. It cannot be used in a MS-DOS-based environment such as MS-DOS mode. Boot disks operate in a **16-bit MS-DOS mode** environment. You therefore cannot use *winnt32.exe* to install Windows XP Professional from a boot disk. You must use *winnt.exe*, which is the 16-bit equivalent of *winnt32.exe*, instead.

TABLE 1.6: *WINNT Switches*

Switch	Description
/a	Enables accessibility options
/e[:*command*]	Specifies a command to be executed at the end of Setup's GUI mode.
/r[:*folder*]	Specifies an optional folder to be installed on the hade drive that is retained after Setup is completed.
/rx[:*folder*]	Specifies an optional folder to be installed on the hade drive. Setup deletes the folder after installation
/s[:*sourcepath*]	Specifies the source location of Windows XP Professional files.
/t[:*tempdrive*]	Specifies a drive to contain temporary setup files.
/u[:*answer file*	Performs an unattended installation using an answer file that provides your custom specifications to the Setup program. This requires the /s switch.
/udf:*id*[,*UDF_file*]	Indicates an identifier (ID) that Setup uses to specify how a Uniqueness Database File (UDF) modifies an answer file

1.6 Deploying Service Packs

Windows XP Professional supports the integration of service-packs called **slipstreaming**, so service packs can be integrated with the Windows XP Professional installation files. This allows you to keep an image of the operating system. When Windows XP Professional is installed from this image, the appropriate files

from the service pack are also installed. To apply a new service pack, run the *update.exe* file from the service pack with the */slip* switch. This will replace the existing Windows XP Professional files with the appropriate files from the service pack.

You can also apply a service pack to computers that are already running Windows XP Professional by running the *update.exe* file. This replaces the existing Windows XP Professional files with the appropriate files from the service pack.

1.7 Installing Windows XP Professional on a dual boot configuration

A dual boot configuration allows you to install two or more operating systems on your computer and to choose between them each time you start your computer. This allows you to run applications that are not compliant with Windows XP Professional on an existing operating system, while using Windows XP Professional for all other applications.

Some operating systems, such as MS-DOS, cannot access partitions that are formatted with the FAT32 or NTFS file systems. However, the active partition is the partition from which the computer starts, and must be formatted with a file system that is accessible by both operating systems.

It is recommended that you install the other operating system and then Windows XP Professional as pre-Windows NT operating systems must be located on the active partition. Windows XP Professional can however be installed on the active partition or on another primary or extended partition. When you install Windows XP Professional on a partition other than the active partition, Windows XP Professional will copy the necessary files to start the boot process to the active partition, which is referred to as the Windows XP Professional system partition. This enables Windows XP Professional to begin the boot process. The remainder of the operating system files will be copied to the non-active partition, which is referred to as the Windows XP Professional boot partition. During the boot process the Windows XP Professional operating system will be located through the **ARC path** in the *boot.ini* file.

1.8 Activating Windows XP Professional

After completing an installation of Windows XP Professional, you must activate the Operating System. The first time that a user logs on to a computer running Windows XP Professional, the **Activate Windows** dialog box appears, and the user is prompted to activate the installed copy of Windows XP Professional. A user can choose not to activate the software, in which case reminders to activate will periodically appear until the user activates the software.

To activate the Operating System:

- Select the **Yes, let's activate Windows over the Internet now** option, and then click **Next**; or
- If the computer is not connected to the Internet, the user can click the **Telephone** button, and then follow the directions for activating Windows XP Professional over the telephone.

Users in large organizations can use a Volume License Product Key that will eliminate the need to individually activate each installation of Windows XP Professional. Additionally, users can automatically activate Windows XP Professional as part of an automated installation.

Note: Users must activate Windows XP Professional within seven days of

installation. If not activated within seven days, users are prevented from gaining access to Windows XP Professional until activation occurs.

1.9 The Windows XP Professional Boot Process

1.9.1 Files Used in the Boot Process

A Windows XP Professional Intel-based boot sequence requires a number of files. A list of these files, their appropriate locations and the stages of the boot process associated with each file are listed in Table 1.7

Note: ***Systemroot*** represents the path to your Windows XP Professional installation folder, which by default is ***C:\Winnt***

TABLE 1.7 *Files Used in the Windows XP Professional Boot Process*

File	Location	Boot stage
Ntldr	System partition root (C:\ )	Preboot and boot
Boot.ini	System partition root	Boot
Bootsect.dos	System partition root	Boot (optional)
Ntdetect.com	System partition root	Boot
Ntbootdd.sys	System partition root	Boot (optional
Ntoskrnl.exe	*systemroot*\System32	Kernel load
Hal.dll	*systemroot*\System32	Kernel load
System	*systemroot*\System32\Config	Kernel initialization
Device drivers	*systemroot*\System32\Drivers	Kernel initialization

Note: The string ***systemroot*** (typed as *%*systemroot*%*) represents the folder in the boot partition that contains the **Windows XP Professional system files**.

1.9.1.1 Preboot Sequence

During startup, a Windows XP Professional-based computer initializes the boot portion of the hard disk and the preboot sequence begins. This sequence consists of four steps:

- The computer runs power-on self test (POST) process to determine the amount of physical memory; and
- The hardware components are present.
- If the computer has a Plug and Play (BIOS), enumeration and configuration of hardware devices occurs.
- The computer BIOS locates the boot device and loads and runs the master boot record (MBR).

Note: Windows XP Professional modifies the boot sector during installation so that Ntldr loads during system startup. Therefore you should disable the ***Boot Sector Virus Protection*** in your BIOS Setup.

1.9.1.2 Boot Sequence

After the computer loads **Ntldr** into memory, the boot sequence gathers information about hardware and drivers in preparation for the Windows XP Professional load phases. The boot sequence uses the following files: **Ntldr**, *Boot.ini*, *Bootsect.dos* (optional), *Ntdetect.com*, and *Ntoskrnl.exe*.

The boot sequence also has five phases:

- **Initial Boot Loader Phase:** During the initial boot loader phase, **Ntldr** switches the microprocessor from real mode to 32-bit flat memory mode, which **Ntldr** requires. Then, **Ntldr** starts the appropriate the minifile system drivers. The minifile system drivers are built into **Ntldr** so that **Ntldr** can find and load Windows XP Professional from partitions formatted with either the FAT or NTFS file system.
- **Operating System Selection Phase:** During the boot sequence, **Ntldr** reads the *Boot.ini* file. If multiple operating systems are supported on the computer in the *Boot.ini* file, then the **Please Select The Operating System To Start** screen, which you can use to select the operating system that should be loaded within a specified time before the default operating system. If no *Boot.ini* file is present, **Ntldr** attempts to load Windows XP Professional from the *Winnt* folder on the first partition of the first disk, typically *C:\Winnt*.
- **Hardware Detection Phase:** On Intel-based computers, *Ntdetect.com* and *Ntoskrnl.exe* perform hardware detection. *Ntdetect.com* executes if Windows XP Professional should be loads. *Ntdetect.com* collects a list of installed hardware components and returns this list to **Ntldr** for later inclusion in the registry under the HKEY_LOCAL_MACHINE\HARDWARE key.
- **Configuration Selection Phase:** After **Ntldr** starts loading Windows XP Professional and collects hardware information, the operating system loader process displays the **Hardware Profile/Configuration Recovery Menu** screen, which contains a list of the hardware profiles that have been created on the computer, if more that one hard profile exists on the computer. The first hardware profile is highlighted. You can press the Down arrow key to select another profile. You can also press L to invoke the **Last Known Good Configuration** option.
- **Windows XP Professional Logon Phase:** The Windows XP Professional boot sequence is complete once the user has successfully logged on at the computer.

1.9.1.3 Kernel Load

After the configuration selection, ***Ntoskrnl.exe***, the Windows XP kernel loads and initializes. *Ntoskrnl.exe* also loads and initializes device drivers and loads services. If you press Enter when the **Hardware Profile/Configuration Recovery Menu** screen displays, or if **Ntldr** makes the selection automatically, the computer enters the kernel load phase. The screen clears and a series of white rectangles appears across the bottom of the screen. During the kernel load phase, **Ntldr**:

- Loads Ntoskrnl.exe but does not initialize it.
- Loads the hardware abstraction layer file (*Hal.dll*).
- Loads the HKEY_LOCAL_MACHINE\SYSTEM registry key.
- Selects the control set required to initialize the computer.
- Loads device drivers with a value of 0x0 for the Start entry. These are typically low-level hardware device drivers, such as those for a hard disk.

1.9.1.4 Kernel Initialization

When the kernel load phase is complete, the kernel initializes and takes control from **Ntldr**. The system displays a graphical screen with a status bar that indicates load status. During the kernel initialization stage four tasks are performed:

- The Hardware key is created.
- The Clone control set is created.
- Device drivers are loaded and initialized.
- Services are started.

1.9.1.5 Logon

The logon process begins at the end of the kernel initialization phase, when the Win32 subsystem automatically starts *Winlogon.exe*, which starts Local Security Authority (*Lsass.exe*) and displays the Logon dialog box. This allows you to log on while Windows XP initializes the network device drivers.

> **Note:** Windows XP startup is not considered **successful** until a user logs on at the computer. After a **logon**, the system automatically copies the Clone control set to the LastKnownGood control set making the current control set the ***Last Known Good Configuration***

1.10 The Registry

Microsoft Windows XP Professional stores hardware and software settings in the registry. The registry controls the Windows XP Professional operating system by providing the appropriate initialization information to boot Windows XP Professional, to start applications, and to load components, such as device drivers and network protocols.

Management of the registry is an important part of the administrator's job and includes viewing, editing, backing up, and restoring the registry. You use Registry Editor to view and change the registry configuration.

1.10.1 The Hierarchical Structure of the Registry

The registry is organized in a hierarchical structure that is displayed by the Registry Editor. This hierarchy is made up of:

- **Subtree** To make the information in the registry easier to find and view, there are five predefined subtrees that can be seen in the editor. These subtrees are listed in Table 1.8
- **Keys** correspond to hardware or software objects and groups of objects. Subkeys are keys within higher level keys
- **Entries** Keys contain one or more entries. An entry has three parts: name, data type, and value (data or configuration parameter)
- **Hive** A hive is a discrete body of keys, subkeys, and entries that has a corresponding registry file and .log file located in %systemroot%\ System32\Config. Windows XP Professional uses the .log file to record changes and ensure the integrity of the registry
- **Data types** Each entry's value is expressed as one of these data types:

- **REG_SZ (String value)**. Which is one value that Windows XP Professional interprets it as a string to store.
- **REG_BINARY (Binary value)**. Which is one value that must be a string of hexadecimal digits.
- **REG_DWORD (DWORD value)**. Which is one value that must be a string of 1-8 hexadecimal digits.
- **REG_MULTI_SZ (Multistring value)**. Can be multiple values that Windows XP Professional interprets each string as a component of multi_sz separate entries.
- **REG_EXPAND_SZ (Expandable string value)**. Similar to REG_SZ, except the text can contain a replaceable variable.
- **REG_FULL_RESOURCE_DESCRIPTOR**. Stores a resource list for hardware components or drivers. You cannot add or modify an entry with this data type.

TABLE 1.8: *The Registry Subtrees*

Subtree	Description
HKEYLOCAL_MACHINE	Contains all configuration data for the local computer, including hardware and operating system data such as bus type, system memory, device drivers, and startup control data. Applications, device drivers, and the operating system use this data to set the computer configuration. The data in this subtree remains constant regardless of the user.
HKEYUSERS	Contains two subkeys: DEFAULT, which contains the system default settings (system default profile) used to display the Ctrl+Alt+Delete logon screen, and the security identifier (SID) of the current user; and HKEYCURRENT_USER, which is a child of HKEY_USERS.
HKEY_CURRENT_USER	Contains data about the current user. Retrieves a copy of each user account used to log on to the computer from the NTUSER.DAT file and stores it in the %systemroot%\Profiles\username key. This subtree takes precedence over HKEY_LOCAL_MACHINE for duplicated values.
HKEY_CLASSES_ROOT	Contains software configuration data: object linking and embedding (OLE) and file-class association data. This subtree points to the Classes subkey under HKEY_LOCAL_MACHINE\SOFTWARE
HKEY_CURRENT_CONFIG	Contains data on the active hardware profile extracted from the SOFTWARE and SYSTEM hives. This information is used to configure settings such as the device drivers to load and the display resolution to use

1.10.2 The HKEY_LOCAL_MACHINE Subtree

The HKEY_LOCAL_MACHINE root key has five subkeys. These are listed in Table 1.9.

TABLE 1.9: ***HKEY_LOCAL_MACHINE Subkeys***

Subkey	Description
HARDWARE	Contains information on the type and state of physical devices attached to the computer. Windows XP Professional builds this subkey from information gathered during startup and therefore it is not mapped to a file on the disk. Applications query this subkey to determine the type and state of physical devices attached to the computer.
SAM	Contains information on the directory database for the computer and is mapped to the SAM and SAM.LOG files in the %systemroot% \System32\Config directory. Applications that query SAM must use the appropriate application programming interfaces (APIs).
SECURITY	Contains the security information for the local computer and is mapped to the Security and SECURITY.LOG files in the %systemroot%\System32\Config directory. Applications cannot modify the keys contained in the SECURITY subkey. Instead, applications must query security information by using the security APIs.
SOFTWARE	Contains information about the local computer software that is independent of user configuration information and is mapped to the Software and SOFTWARE.LOG files in the %systemroot%\System32\Config directory.
SYSTEM	Contains information about system devices and services. When you install or configure device drivers or services, they add or modify information under this hive. The SYSTEM hive is mapped to the System and SYSTEM.LOG files in the %systemroot% \System32\Config directory. The registry keeps a backup of the data in the SYSTEM hive in the SYSTEM.ALT file.

1.11 The Boot.ini File

The *Boot.ini* file is a hidden file that the Windows XP Professional Setup program saves in the active partition when you install Windows XP Professional. **Ntldr** uses information in the *Boot.ini* file to display the **Please Select The Operating System To Start** menu, from which you select the operating system that should be loaded.

1.11.1 Components of the Boot.ini File

The *Boot.ini* file includes two sections, **[Boot Loader]** and [Operating Systems] (*See Figure 1.2*) The [Boot Loader] section of a *Boot.ini* file contains the specified time that the **Please Select The Operating System To Start** menu is displayed and the default operating system that should be loaded if no selection is made within the specified time. The **[Operating Systems]** section of the *Boot.ini* file contains a list of all the operating systems that are installed on the computer.

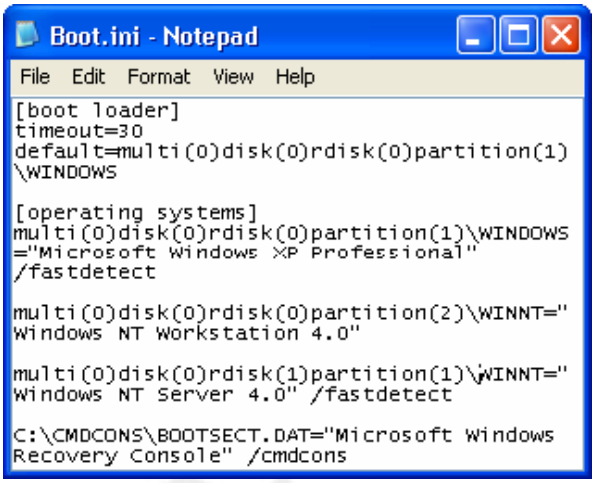


Figure 1.2: *A Boot.ini File.* (NOTE the *ARC path*)

1.11.2 ARC Paths

During installation, Windows XP Professional generates the *Boot.ini* file, which contains **Advanced RISC Computing** (ARC) paths pointing to the computer's boot partition.

TABLE 1.10: *ARC Path Naming Conventions*

Convention	Description
multi(*x*) | scsi(*x*)	The hardware **adapter or disk controller**. Use **scsi** only to indicate a SCSI controller on which SCSI BIOS is not enabled. All other hardware adapter or disk controllers use **multi**. **(x)** represents a number that indicates the load order of the hardware adapter. The hardware adapter first to load and initialize receives number 0.
Disk(*y*)	The **SCSI ID**. For multi, this value **(y)** is always (0)
Rdisk(*z*)	A number **(*z*)** that identifies the disk and starts with (0).
Partition(*a*)	A number **(*a*)** that identifies the partition. Partition numbers start with (1)

Note: The lowest possible ARC path, i.e. the ARC path that points to your primary boot partition an your primary master drive (**C:**) is **multi(0)disk(0)rdisk(0)partition(1)**

1.11.3 Boot.ini Switches

You can add a variety of switches to the entries in the [Operating Systems] section of the *Boot.ini* file to provide additional functionality. Table 1.11 lists some of these switches.

TABLE 1.11: *Boot.ini Switches*

Switch	Description
/basevideo	Boots the computer using the standard VGA video driver.
/bootlog	Enables boot logging to Ntbtlog.txt in the systemroot folder.

/debug	Loads the Windows kernel debugger.
/fastdetect=[com*x* | com*x,y,z.*]	Disables serial mouse detection. Without a port specification, this switch disables peripheral detection on all COM ports. By default, this switch is included in every entry in the Boot.ini file.
/maxmem:*n*	Specifies the amount of RAM that the operating system should use.
/noguiboot	Boots the computer without displaying the graphical boot status screen.
/safeboot	Forces the computer to start in safe mode. You can specify safeboot parameters when using this switch.
/sos	Displays the device driver names as they are loading.

1.12 Advanced Boot Options

The Windows XP Professional advanced boot options include Safe Mode, Enable Boot Logging, Enable VGA Mode, Last Known Good Configuration and Automated System Recovery.

- **Safe Mode** can be used if your computer does not start properly. Pressing **F8** during the operating system selection phase displays a screen with advanced options for booting Windows XP Professional. If you select Safe Mode, Windows XP Professional loads only basic files and drivers that are required to support the operating system. If your computer does not start using safe mode, you can try Windows XP Professional **Automated System Recovery (ASR)**. You can also choose **Safe Mode With Networking**, which is the same as Safe Mode except that it adds the drivers and services required to enable network access, and **Safe Mode With Command Prompt**, which is the same as Safe Mode except when the computer restarts, it displays a command prompt.
- **Enable Boot Logging** logs the loading and initialization of drivers and services in the ***ntbtlog.txt*** file, which is located in the *windir* folder and can be used for troubleshooting boot problems.
- **Enable VGA Mode** option starts Windows XP Professional with a basic VGA driver.
- **Last Known Good Configuration** starts Windows XP Professional using the registry information that Windows XP Professional saved after the last successful startup of Windows XP Professional. Windows XP Professional startup is not considered **successful** until a user logs on at the computer. After a **logon**, the system automatically copies the Clone control set to the LastKnownGood control set making the current control set the ***Last Known Good Configuration***

> **Note: Last Known Good Configuration** cannot be used to recover from a start up failure that caused by a **hardware failure,** or a **missing** or **corrupt file** as these are not loaded from the **registry** when you boot Windows XP Professional.

1.12.1 The Recovery Console

The Recovery Console is a **command-line** interface that can be used to perform a variety of troubleshooting and recovery tasks, including

- Starting and stopping services;

- Reading and writing data on a local drive; and
- Formatting hard disks.

1.12.1.1 Installing and Starting the Recovery Console

You can install the Recovery Console from the Windows XP Professional Installation CD by running the winnt32 command with the /cmdcons switch from the command prompt. After Recovery Console is installed, you can access it from the **Please Select Operating System To Start** menu. You can also use the Windows XP Professional Installation CD to start your computer and then select the Recovery Console option when you are prompted to choose repair options.

> **Note:** On a **64-bit**, Intel Pentium 4 computer you can use **\ia64\winnt32.exe /cmdcoms** to install the Recovery Console

1.12.1.2 Using the Recovery Console

The Recovery Console provides you with a limited set of DOS-based administrative commands that you can use to repair your Windows XP Professional installation. A list of the Recovery Console commands is shown in Table 1.12.

TABLE 1.12: *Some Recovery Console commands*

Command	Description
Chdir (cd)	Displays the name of the current folder or changes the current folder
Chkdsk	Checks a hard drive and displays a status report
Copy	Copies a single file from a stiffy drive or CD-Rom drive to the hard drive
Delete (del)	Deletes one or more files
Dir	Displays a list of files and subfolders in a folder
Disable	Disables a system service or a device driver
Enable	Starts or enables a system service or a device driver
Exit	Exits the Recovery Console and restarts your computer
Fdisk	Manages partitions on your hard disks
Fixboot	Writes a new partition boot sector onto the system partition
Fixmbr	Repairs the master boot record of the partition boot sector
Format	Formats a disk
Help	Lists all of the Recovery Console commands
Listsvc	Lists the device drivers and services that are currently installed on the computer
Mkdir (md)	Creates a folder
Rmdir (rd)	Deletes a folder

Rename (ren)	Renames a single file
Systemroot	Sets the current folder to the systemroot folder of the system that you are currently logged on to
Type	Displays a text file

1.12.2 Automated System Recovery (ASR)

You can also user the Automated System Recovery (ASR) to recover from boot problems. The ASR process allows you to recover a system that is unable to start because of a hardware malfunction, the loss of a storage device, or another system disaster. After installing Windows XP Professional you can prepare the ASR process by running the Automated System Recovery Preparation Wizard and creating an ASR Disk. You can use the Automated System Recovery Preparation Wizard to back up an entire partition. The ASR disk enables you to gain access to that backed up data. The data can be backed up to a tape drive or writable CD-ROM, or backed up to a file and then burned to a CD or tape. The floppy disk created at the end of the backup process contains the ASR state file, named Asr.sif, and other files needed to restore the system to its original state.

2. Configuring Windows XP Professional

Control Panel in Windows XP Professional can be used to configure hardware settings, manage user-specific settings, and manage computer-specific settings.

2.1 Configuring Hardware Profiles

A hardware profile is used to store the configuration settings for a set of devices and services on a computer. In Windows XP Professional you can create different hardware profiles for each user who uses a particular computer, or to meet a user's needs in different situations. The user can then choose the appropriate profile the Windows XP Professional should load when starting the computer.

A default hardware profile is created during the installation process of Windows XP Professional. This profile is listed as Profile 1 (Current) in the Hardware tab in the System Properties dialog box. To create a new profile:

- Click on the **START** button
- Point to **SETTINGS**
- Open **CONTROL PANEL**
- Open **SYSTEM**
- Click on the **HARDWARE** tab
- Click on **HARDWARE PROFILES**
- Select the **Profile** that you want to copy
- Click **COPY**
- Click **PROPERTIES**
- Select **ALWAYS INCLUDE THIS PROFILE AS AN OPTION WHEN WINDOWS STARTS** check box
- Reboot the computer and select the new profile when Windows XP Professional boots.

The new profile will then be loaded when the boot sequence is complete and you can then set which devices must be disabled for the new profile. You can make the new profile the default profile on the **HARDWARE PROFILES** list by using the arrow buttons to the right of the list box to move the new profile to the top of the list.

HOT DOCKING

Portable computers that are Plug and Play compliant automatically create separate hardware profiles for when the computer is docked and when it is undocked. These are called the *Docked Profile* and *Undocked Profile* and are automatically selected when the computer is docked or undocked. If the computer is not fully Plug and Play compliant, you might have to create these profiles and select the appropriate one when booting the computer.

2.2 Installing New Hardware

Installing a new device to a Windows XP Professional computer typically involves physically connecting the device to the computer; loading the appropriate device drivers; and configuring the device properties and settings if required.

Note: To be able to install a device you must be logged on as an **administrator** or as a member of the **Administrators group**.

When you install a Plug and Play device, Windows XP Professional automatically configures the device so that it works properly with the other devices that are already installed on the computer. This includes

assigning the appropriate system resources, such as Interrupt Request (IRQ) line number, Direct Memory Access (DMA) channels, Input/Output (I/O) port addresses and Memory Address ranges, to the device. Each device must be assigned a unique system resource or the device will not function properly. When you install a non-Plug and Play, or a legacy device, you must use the Add/Remove Hardware Wizard. If Windows XP Professional does not detect the device you must configure the system resources for the device manually. You can assign system resources to the device in Device Manager.

Note: Some old **legacy ISA** devices require the use of a specific IRQ number that Windows XP Professional may have assigned to a Plug and Play device. In this event you should **reserve** the IRQ that is required by the device in your **system BIOS**. Windows XP Professional then will assign another IRQ to the Plug and Play device that was using the IRQ that you have reserved.

2.2.1 Installing Additional Processors

By adding processors to your computer you can improve performance. This is called **scaling**. When you install an additional processor, you must update the Hardware Abstraction Layer (HAL) on your computer. The HAL functions in a similar way to an application programming interface (API) and is used by programmers to write device-independent applications. This HAL must be updated so that the applications can be supported on both processors. You can use Device Manager to upgrade the HAL.

- Click on the **START** button
- Point to **SETTINGS**
- Open the **CONTROL PANEL**
- Open **SYSTEM**
- Click on the **HARDWARE** tab
- Click on **DEVICE MANAGER**
- Expand **COMPUTER**
- Right-click **ADVANCED CONFIGURATION AND POWER INTERFACE (ACPI) PC** or similar model
- Click **PROPERTIES**
- Click on the **DRIVER** tab
- Click **UPDATE DRIVER**
- Click **NEXT** on **THE WELCOME TO THE UPGRADE DEVICE DRIVER WIZARD** page
- Click **DISPLAY A LIST OF THE KNOWN DRIVERS FOR THIS DEVICE SO THAT I CAN CHOOSE A SPECIFIC DRIVER** on the **INSTALL HARDWARE DEVICE DRIVERS** page
- Click **NEXT**
- Click **SHOW ALL HARDWARE OF THIS DEVICE CLASS** on the **SELECT A DEVICE DRIVER** page
- Click the appropriate **MANUFACTURER**
- Click the appropriate **COMPUTER MODEL**
- Click **NEXT**
- Click **NEXT**
- Click **FINISH**

2.2.2 Installing and Configuring Fax Devices

If you have installed a fax modem, a fax icon will be displayed in the Control Panel. This icon can be used to add, monitor, and troubleshoot fax devices.

> **Note:** By default, the fax modem is configured send faxes, but is not configured to receive faxes. You can use the Fax Service Management console to receive faxes. You can also use the Fax Service Management console to change security permissions for users, to configure the number of rings before a fax device answers a fax receive, to configure the number of retries before a fax terminates a fax send, and to Configure where to store sent and received faxes.

2.3 Using Driver Signing

Some device drivers and some applications overwrite existing operating files as part of their installation process. These files can cause system errors that are difficult to troubleshoot. Microsoft has greatly simplified the tracking and troubleshooting of altered files by digitally signing the original operating system files and allowing you to verify these signatures.

2.3.1 Configuring Driver Signing

You can configure how the computer responds to unsigned files on **HARDWARE** tab of **SYSTEM**. Here you can configure one of three responses:

- **Ignore** allows any files to be installed regardless of whether they are digital signature or not.
- **Warn** displays a warning message before allowing the installation of an unsigned file. This is the default option.
- **Block** prevents the installation of unsigned files.

> **Note:** Once you have set altered the Driver Signing setting, you must set it as the default setting or the setting will revert to the previous default setting on the next system reboot. To set the new settings as the default setting, select the **MAKE THIS ACTION THE SYSTEM DEFAULT** check box on the **Driver Signing Options** dialog box.

2.3.2 System File Checker

Windows XP Professional also has a System File Checker (SFC), which is a command-line tool that you can use to check the digital signature of files. SFC can be used from a command prompt. The syntax of the SFC tool is:

```
Sfc [/scannow] [/scanonce] [/scanboot] [/revert] [/purgecache] [/cachesize=x]
```

TABLE 2.1: *System File Checker Optional Command-line Switches*

Switch	Description
/scannow	Used to perform an immediate scan of all protected system files
/scanonce	Used to perform a scan of all protected system files only on the next system reboot
/scanboot	Used to perform a scan of all protected system files every time the system reboots
/revert	Causes the SFC settings to be returned to the default settings
/purgecache	Purges the file cache
/cachesize=*x*	Sets the file cache size

2.3.3 The File Signature Verification Utility

Windows XP Professional also has a File Signature Verification utility, ***sigverif***, that allows you to view the file's name, its location, its modification date, its type, and its version number.

2.3.4 Device Diver Rollback

In addition to protecting you from driver-related trouble by warning you when you try to install an unsigned driver that has not been certified as compatible with Windows XP, Windows XP Professional also allows you to uninstall an updated driver and restore the previously installed version of the driver. This can be done in Safe Mode, if necessary. In other words, if you experience system problems after updating a device driver, you can roll back to the previous instaled version of the driver.

To roll back a driver:

- Click on the **START** button
- Click on **CONTROL PANEL**
- Open **SYSTEM**
- Click on the **HARDWARE** tab
- Click on **DEVICE MANAGER**.
- Expand the **hardware category** to which the device driver belongs
- Right-click the **device driver**
- Click **PROPERTIES**
- On the **Device Properties** dialog box, click on the **DRIVER** tab
- Click **ROLL BACK DRIVER**.
- In the dialog box, click **YES**
- Click **OK**

If no backed-up driver is available, then Driver Rollback is not available for the selected device. This could be because the device driver was not updated or the previous version of the device driver was inactive or dysfunctional. Windows XP Professional only backs up device drivers that are active and functional. Also, when you roll back to an unsigned device driver, Windows XP Professional will prompt you before

overwriting the newer driver. Windows XP Professional will not you prompt when you roll back to a signed device driver.

Note: Driver Rollback is not available for Printers because the drivers are not configured through Device Manager; they are configured through the Printers and Faxes folder.

2.4 Configuring Display Settings

Windows XP Professional allows you to configure the appearance of your desktop and how your monitor displays information. Windows XP Professional also allows you to install and simultaneously use up to ten monitors. These monitors will require their own video adapter cards.

Note: You can use either **PCI or AGP** video adapter cards to support additional monitors but **not ISA** video adapter cards.

To install additional monitors:

- Switch off your computer and open the computer's case
- Insert the additional PCI or VGA video adapter card into a free slot
- Plug your additional monitor into the video adapter card
- Close the computer's case and boot the computer
- Windows XP Professional will detect the video adapter card and will install the appropriate drivers
- Open the **CONTROL PANEL**
- Open **DISPLAY**
- Click on the **SETTINGS** tab
- Select the **EXTEND MY WINDOWS DESKTOP ONTO THIS MONITOR** check box
- Click on the monitor icon that you want top use as an additional monitor
- Select the color depth and resolution for the secondary display

You can repeat this procedure for every additional display you want to use.

TABLE 2.2: *Troubleshooting Display Problems*

Problem	Solution
You cannot see any display on the secondary monitors	Activate the device in the Display Properties dialog box. Check that the correct video adapter driver has been installed. Switch the order of the adapters in the slots. The primary display adapter should be installed in the either PCI slot 0 or 1.
The Extend My Windows Desktop Onto This Monitor check box is unavailable.	Select the secondary display rather than the primary one in the Display Properties dialog box.

	Confirm that the secondary display adapter is supported. Confirm that Windows XP Professional can detect the secondary display.
An application fails to display on the secondary display.	Run the application in full-screen mode, if it is a DOS-based application, or maximized, if it is a Windows-based application.
A DOS-based application opens but the display area is scrambled. The monitor functions correctly when you run Windows-based applications.	Some legacy DOS applications can only run in 256 indexed color mode. You should therefore set the video adapter to 256 colors.
You want to configure a non-Plug and Play video adapter to use 16-bit color and 1024 x 768 resolution. The color setting for the video adapter is set to 16 colors and 640 x 480 resolution, and you cannot change that setting.	Windows has installed a standard video adapter driver. Install a driver that is compatible with Windows XP Professional.

2.5 Configuring System Settings

In Control Panel you can configure the operating system settings to optimize system performance. In the **SYSTEM PROPERTIES** dialog box you can configure Performance Options, Environment Variables, and Startup and Recovery settings. In **Performance Options** you can set the operating system to be optimized for applications or background services and you can set the size of the Windows XP Professional paging file. The minimum paging file size for Windows XP Professional is 2 MB. The default or **recommended paging file size** is equal to 1.5 times the total amount of RAM. You might want to use a larger paging file or multiple paging files if you run a large number of applications simultaneously. In **Startup and Recovery** you can specify the default operating system and the length of time that the list of operating systems must be displayed before the default is loaded.

2.6 Configuring the Desktop Environment

In Windows XP Professional you can use the CONTROL PANEL to configure your computer for multiple languages and locations or locale. This can be configured through the REGIONAL OPTIONS program in the CONTROL PANEL. You can also set **ACCESSIBILITY** options that make Windows XP Professional easier to use for people with disabilities.

In the **REGIONAL OPTIONS** program of the Windows XP Professional Control Panel, you can configure your computer for multiple **languages and locations**. You can select multiple languages on the **GENERAL** tab of the REGIONAL OPTIONS dialog box by selecting the check box of each language that you want your computer to support. REGIONAL OPTIONS also allow you to configure your computer to use multiple locations or locales. The **GENERAL** tab indicates the current locale setting and the **INPUT LOCALE** tab allows you to add additional locales to your computer.

Note: If you select more than one input locale and select the **ENABLE INDICATOR ON TASKBAR** checkbox on the INPUT LOCALE tab of the REGIONAL SETTINGS program, you can change the input locale by clicking on the **input locale indicator** on the taskbar.

2.7 Configuring Accessibility Options

In Windows XP Professional you can use the **ACCESSIBILITY OPTIONS** program in CONTROL PANEL to configure accessibility options. You can configure Keyboard, Sound, Display, Mouse, and General Accessibility options.

- On the **KEYBOARD** tab you can configure:
  - **FilterKeys** causes the keyboard to ignore brief or repeated keystrokes. This option also allows you to configure the keyboard repeat rate, which is the rate at which a key continuously held down repeats the keystroke. This is a check box selection, so it is either on or off. You can configure FilterKeys by clicking Settings to activate the Settings For FilterKeys dialog box
  - **StickeyKeys** Turning on StickyKeys allows you to press a multiple key combination, like Ctrl+Alt+Delete, one key at a time. This is useful for people who have difficulty pushing more than one key at a time. This is a check box selection, so it is either on or off. You can configure StickyKeys by clicking Settings to activate the Settings For StickyKeys dialog box
  - **ToggleKeys** You can also configure ToggleKeys in the Keyboard tab. Turning on ToggleKeys causes the computer to make a high-pitched sound each time the Caps Lock, Num Lock, or Scroll Lock keys are switched on. Turning on ToggleKeys also causes the computer to make a low-pitched sound each time these three keys are turned off.
- On the **SOUND** tab you can configure:
  - **Sound Sentry** allows you to configure Windows XP Professional to generate visual warnings when your computer makes a sound.
  - **ShowSounds** allows you to configure Windows XP Professional programs to display captions for the speech and sounds they make.
- On the **DISPLAY** tab you can configure:
  - **High Contrast** allows you to configure Windows XP Professional to use color and fonts designed for easy reading.
  - **Cursor Options** allow you to set the blink rate and the width of the cursor.
- On the **MOUSE** tab you can configure:
  - **MouseKeys** allows you to configure Windows XP Professional to control the mouse pointer with the numeric keypad on your keyboard this enables the keyboard to perform mouse functions. You can also configure the pointer speed and acceleration speed.
- On the **GENERAL** tab you can configure:
  - **SerialKeys** allows you to configure Windows XP Professional to support an alternative input device (also called an augmentative communication device) to your computer's serial port.

Unlike Windows 2000 in which accessibilty options were not made permanent, but reverted back to to the standard settings automatically after a specified period of inactivity, Windows XP Professional requires you to set this option on the **GENERAL** tab.

2.8 Configuring Hard Disks

2.8.1 Disk Storage Types

Windows XP Professional provides support for two types of disk storage: **basic storage**, which uses basic disks and is the standard storage type; and **dynamic storage**, which uses dynamic disks. Basic disks can be divided into up to four partitions that can either be **primary partitions** or **extended partitions**. You can have multiple primary partitions but only one extended partition. You can create multiple primary partitions to which enables you to **dual boot** between Windows XP Professional and other operating systems such as Windows 98. One of the primary partitions must be set in **fdisk** as the **active partition** as the **boot files** required to start the operating systems must be located on the active partition.

> **Note:** If you are going to dual boot between Windows XP Professional and **Windows 95**, **Windows 95 OSR2**, **Windows 98**, or **Windows Millennium Edition**, the primary partition must be formatted with the **FAT** or **FAT32** file system as Windows 9*x* must reside on the primary partition and cannot access partitions that have been formatted with the NTFS file system.

Basic disks can be converted to dynamic storage from which **dynamic volumes** can be created. Windows XP Professional supports three types of dynamic volumes: **simple volumes**, which are created from disk space on a single physical disk and is not fault tolerant; **spanned volumes**, which can contain disk space from up to 32 physical disks and are also not fault tolerant; and **striped volumes**, which can combine the free space from up to 32 physical disks into one logical volume.

You can convert a dynamic disk back to a basic disk; however, all volumes must be deleted before the conversion. Therefore you should backup the data on the dynamic disk before converting it back to a basic disk.

To convert a dynamic disk to a basic disk:

- Backup any data that you wish to retain.
- In **Disk Management**, right-click the dynamic disk that you want to convert.
- Click **Convert To Basic Disk**.

> **Note:** When you **add** a disk to the computer it is added as **basic storage**. You can convert from basic storage to dynamic storage at any time without loss of data. However, there must be at least **1 MB** of unallocated space on the hard disk to perform this conversion. Furthermore, all data will be lost when you revert from dynamic storage back to basic storage.

2.8.2 Configuring File Systems

Windows XP Professional supports the **FAT**, **FAT32** and **NTFS** file systems. A computer can contain a combination of file systems but each file system must be located on a separate partition or volume.

> **Note:** MS-DOS, Windows 3.1, Windows 95, Windows 98 and Windows Millennium Edition cannot access data on NTFS formatted disks.

The NTFS file system used by Windows 2000 and Windows XP Professional is **version 5**. This is a new version of NTFS that has been introduced with Windows 2000 and has new features that were not available in NTFS version 4 used by Windows NT 4.0. Windows NT 4.0 cannot therefore fully support all the features of NTFS version 5. NTFS version 5 offers a number of benefits that include:

- File compression
- File and folder level security
- File encryption using Encrypting File System (EFS)
- Disk quotas
- NTFS permissions

Note: You can **convert** a disk from the FAT and FAT32 file to NTFS at any time without data loss by using the ***convert*** command from a command prompt and using the ***fs:/ntfs*** switch. When you format the data on the disk is lost.

2.8.3 Encrypting File System (EFS)

EFS is a feature that was introduced with Windows 2000 and can be used to encrypt files and folders on NTFS volumes. When a user encrypts a file, only that user will be able to use the file. They can use the encrypted file without having to decrypt the file first. EFS can be implemented from Windows Explorer or from the command prompt using the **Cipher** command. The syntax for the cipher command is:

```
cipher [/e | /d] [/s:folder_name] [/a] [/i] [/f] [/q] [/h] [/k] [file_name [...]]
```

For a list of Cipher command switches see Table 2.3.

- EFS is only supported on **NTFS version 5**
- **Compressed files** cannot be encrypted using EFS
- **System files** cannot be encrypted
- Encrypted files cannot be **shared**
- Encrypted flies or folders that are moved or copied to partitions or volumes that are not formatted with the NTFS file system will become decrypted
- Files and folders on network computers can be encrypted if you have the necessary access **permissions** to the network computer's NTFS volume and if file encryption is enabled on the network computer.

TABLE 2.3: *Command-line Switches for the Cipher Command*

Switch	Description
/e	Encrypts the specified folders and marks them so that files that are added later will be encrypted.
/d	Decrypts the specified folders. Files that are added to the folder will no longer be encrypted.
/s:*folder*	Performs the specified operation on folders in the given folder and all subfolders

/a	Performs the specified operation on files and folders.
/i	Continues performing the specified operation even after errors have occurred.
/f	Forces the encryption operation on all specified files, even those that are already encrypted.
/q	Reports only the most essential information.
/h	Displays files with the hidden or system attributes.
/k	Creates a new file encryption key.
File_name	Specifies a pattern, file, or folder.

2.8.3.1 Recovering an Encrypted Folder or File

If the owner's private key is unavailable due to disk failure or any other reason, a designated recovery agent can open the file by using his or her own private key. The default recovery agent is the Administrator account for the local computer. If the recovery agent designation changes, then access to the file is denied. For this reason, it is recommended that you keep recovery certificates and private keys until all files that are encrypted by using those recovery certificates and private keys have been updated. One or more users, typically administrator-level accounts, can be designated as data recovery agents through Local Policy on stand-alone computers or through Group Policy in a domain. Data Recovery Agent (DRAs) are issued recovery certificates with public and private keys that are used for EFS data recovery operations. By default, in a domain, the EFS recovery policy designates the highest-level administrator account as the DRA on the first domain controller installed in the domain. Different DRAs can be designated by changing the EFS recovery policy, and different recovery policies can be configured for different parts of an enterprise. In Windows 2000, DRAs were required to implement EFS. In Windows XP, they are optional. Microsoft recommends that all stand-alone or domain environments have at least one designated DRA.

2.8.3.2 Backing Up and Restoring Encrypted Files or Folders

Encrypted files and folders remained encrypted when you back them up. Backup files remain encrypted when transferred across the network or when copied or moved onto any storage medium, including non-NTFS volumes. If you restore backup files to NTFS volumes in Windows 2000 or Windows XP, they remain encrypted. Along with providing effective disaster recovery, backups can also be used to securely move files between computers and sites. Opening restored, encrypted files is no different from decrypting and opening any other encrypted files. However, if files are restored from backup onto a new computer, or at any location where the user's profile, and thus the private key that is needed to decrypt the files, is not available, the user can import an EFS certificate and private key. After importing the certificate and private key, the user can decrypt the files. A data recovery agent can also be used to decrypt a file for the user, if the user is unable to decrypt the file.

2.8.4 Volume Mounting

The Disk Management tool can be used to mount local drives to an **empty folder** on an NTFS volume. This empty folder becomes the mount point. When a physical disk is mounted to a folder, it is assigned a **drive path** rather than a drive letter. The Administrator can identify and manage volume mount points by using the *mountvol.exe* command-line tool. To mount a drive:

- Open **MY COMPUTER**
- Open **CONTROL PANEL**
- Open **ADMINISTRATIVE TOOLS**
- Click on the **COMPUTER MANAGEMENT**
- Expand **STORAGE**
- Open **DISK MANAGEMENT**
- Right-click the partition or volume you want to mount
- Click **CHANGE DRIVE LETTER AND PATH**
- Click **ADD**
- Type the path to the *Empty Folder*

2.8.5 File Compression

Windows XP Professional supports file and folder level compression. Compressed files can be read and written to by any Windows-based or MS-DOS-based application without first having to be uncompressed by another program. When you access a file via a Windows-based or MS-DOS-based application, NTFS automatically decompresses the file. When you save or close the file again, NTFS compresses it again. Therefore NTFS allocates **disk space** based on the **uncompressed file size** and not on the compressed file size.

2.8.5.1 Copying and Moving Compressed Files and Folders

- When copying a file within an NTFS volume, the file inherits the compression state of the target folder.
- When moving a file or folder within an NTFS volume, the file or folder retains its original compression state.
- When copying a file or folder to another NTFS volume, the file or folder inherits the compression state of the target folder.
- When moving a file or folder to another NTFS volume, the file or folder inherits the compression state of the target folder. Because Windows XP Professional treats a move as a copy and then a delete, the files inherit the compression state of the target folder.
- When moving or copying a file or folder to a **FAT volume**, Windows XP Professional automatically uncompresses the file or folder. This is because Windows XP Professional only supports file and folder compression on NTFS volumes.
- When moving or copying a compressed file or folder to a **floppy disk**, Windows XP Professional automatically uncompresses the file or folder, as floppy disks are formatted with the FAT file system. Floppy disks cannot support the NTFS file system and NTFS file compression is only supported on NTFS volumes.

2.8.6 Disk Quotas

Disk Quotas can be used by administrators to control how much disk space is allocated to users on NTFS volumes and can be allocatedon a **per-user** basis or a **per-volume** basis. The user is charger for every file that they **own** and the **uncompressed file size** is used to calculate their disk quota usage. The Administrator can set the **disk quota level** and the **disk quota warning level** on the **QUOTA** tab of the **PROPERTIES**

dialog box for the **DISK** (SEE FIGURE 2.1). When the disk quota level is set, a warning is sent to the user indicating that they have almost reached their disk quota. When a use exceeds their disk quota, they receive an error message stating that **the disk is full**. When this occurs the user must either:

- Delete some of their files
- Have someone else take ownership of some of their files
- Have the administrator increase their disk quota.

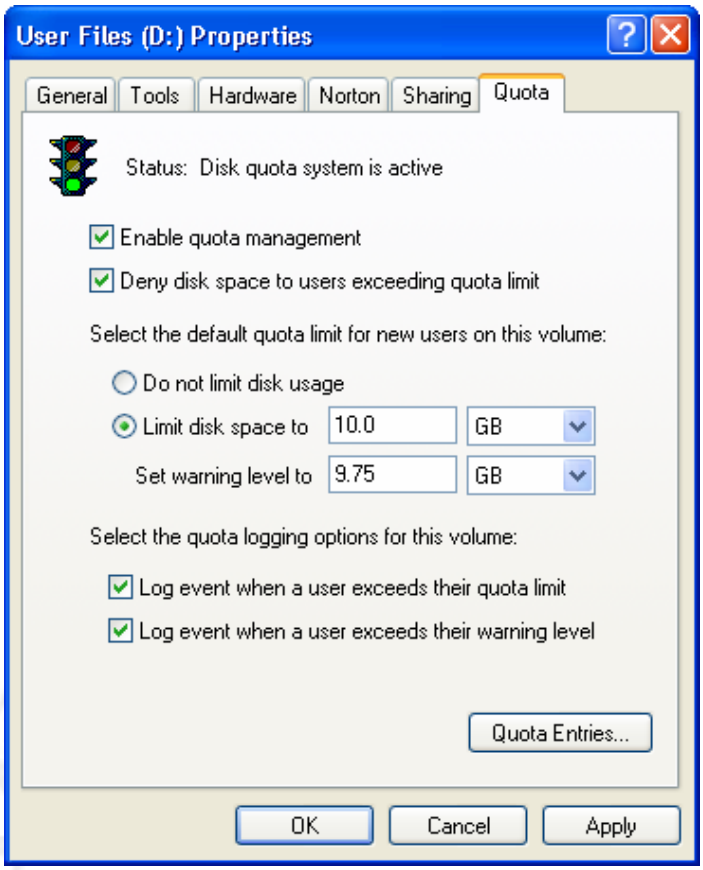


Figure 2.1: *The Quota Tab of the Properties Dialog Box*

2.8.7 Using Disk Defragmenter

Windows XP Professional saves files and folders in the first available space on a hard disk and not necessarily in an area of contiguous space. This results in file and folder fragmentation. When the hard disk contains a large percentage of fragmented files and folders, it takes longer to gain access to them because it requires several additional reads to access all the parts of the file or folder. Creating new files and folders also takes longer because the available free space on the hard disk is scattered, thus the computer saves a new file or folder in various locations on the hard disk.

The process of consolidating fragmented files and folders is called *defragmenting*. You can use Disk Defragmenter to defragment a hard drive. Disk Defragmenter locates fragmented files and folders and moves each piece of the file or folder to one location so that each file or folder occupies a single, contiguous space on the hard disk. This re-optimizes your computers. By consolidating files and folders, Disk Defragmenter also consolidates free space, making it less likely that new files will be fragmented. Disk Defragmenter can defragment FAT, FAT32, and NTFS volumes.

To open Disk Defragmenter:

- Click on **START**
- Point to **PROGRAMS**
- Point to **ACCESSORIES**
- Point to **SYSTEM TOOLS**
- Click **DISK DEFRAGMENTER**

Defrag.exe, a command-line version of Disk Defragmenter is also available in Windows XP Professional. You can use the command-line version in a batch process that is to be executed when the disk is not in use. To use *Defrag.exe*:

- At a command prompt, change to the disk that you want to defragment.
- Type defrag <*volume*> (where volume is the driver letter or mount point). Additional switches can be appended to the command. (See Table 33.3)
- To exit the command prompt window, type exit.

TABLE 2.4: *Defrag.exe Command-line Switches*

Switch	Function
/a	Analyze only.
/f	Force defragmentation even if free space is low.
/v	Verbose output.
/?	Display a list of Defrag.exe switches.

2.8.8 Backing Up and Restoring Data

Performing regular back ups of the data on hard disks prevents **data loss** due to disk drive failures, power outages, virus infections, and other such incidents. If data loss occurs, and you have performed regular backup jobs, you can restore the lost data.

2.8.8.1 Windows Backup

Windows XP Professional provides **Backup And Recovery Tools**. This includes the Backup Wizard, which you can use to easily back up and restore data. To launch Backup

- Click on the **START** button
- Point to **PROGRAMS**
- Point to **ACCESSORIES**
- Point to **SYSTEM TOOLS**
- Click **BACKUP**

Alternatively:

- Click on the **START** button
- Click **RUN**
- Type **ntbackup** in the text box
- Click **OK**

You can use Backup to back up data manually or you can schedule regular unattended backup jobs. You can back up data to a file or to a tape. Files can be stored on hard disks, removable disks, and recordable compact discs and optical drives.

To successfully back up and restore data on a Windows XP Professional computer, you must have the appropriate permissions and user rights

- **All users** can back up their own files and folders, and files for which they have the Read, Read & Execute, Modify, or Full Control permission.

- **All users** can restore files and folders for which they have the Write, Modify, or Full Control permission.
- By default, members of the **Administrators and Backup Operators** groups have the **Backup Files and Directories**, and the **Restore Files and Directories** user rights and can therefore back up and restore all files regardless of the assigned permissions.

2.8.8.2 Backup Types

Backup Wizard provides five types of backup that define which data is backed up. Some backup types use backup **markers**, also known as archive bits, which mark a file as having changed. When a file changes, an attribute is set on the file that indicates that the file has changed since the last backup. When you back up the file, this **clears** or resets the attribute.

- **Normal** – backs up all selected files and folders and does not rely on markers to determine which files to back up. During a normal backup, any existing marks are cleared and each file is marked as having been backed up. Normal backups speed up the restore process because the as the files are the most current therefore you do not need to restore multiple backup jobs.
- **Copy** – backs up all selected files and folders without looking for or clearing markers.
- **Incremental** – only backs up selected files and folders that have a marker and then **clears** the markers. Thus, if you did two incremental backups in a row on a file and nothing changed in the file, the file would not be backed up the second time.
- **Differential** – only backs up selected files and folders that have a marker but does not clear markers. Thus if you did two differential backups in a row on a file and nothing changed in the file, the entire file would be backed up each time.
- **Daily** – backs up all selected files and folders that have changed during the day and does not look for or clear markers.

2.8.8.3 Restoring Data

To restore data, you must select the backup sets, files, and folders to restore. You can use the Restore Wizard to restore data.

2.9 Configuring Power Management on Portable Computers

Mobile users have special needs for managing the power used by their computers, especially when running the computer on batteries. You can reduce the power consumption of your computer devices or of your entire system by choosing a power-saving scheme, or by adjusting the individual settings in a power scheme. To gain access to power option properties, such as power schemes, click Start, click Control Panel, click Performance and Maintenance, and then click Power Options.

Windows XP Professional supports a power management technology called Advanced Configuration and Power Interface (ACPI). ACPI enables Windows XP Professional to manage the power state of both portable and desktop computers in response to input from the user, applications, or device drivers. Windows XP Professional also includes support for portable computers that use Advanced Power Management (APM). ACPI compatible computers automatically support APM.

To reduce the power consumption of a workstation or mobile computer, you can choose a power scheme. A power scheme is a collection of settings that manages the power usage of the computer. Power schemes

provide users with the ability to balance their computer's battery life and performance in a way that best meets their needs.

TABLE 2.5: *Windows XP Professional Power Schemes*

Power Scheme	Description
Home/Office Desk	Maintains constant power to the hard disk and system when the computer is plugged in
Portable/Laptop	Turns off all settings after 5 to 30 minutes of inactivity.
Presentation	Maintains constant power to the monitor, the hard disk and system when the computer is plugged but only to the monitor when the computer is running on batteries.
Always On	Maintains constant power to the system when the computer is plugged in or running on batteries
Minimal Power Management	Maintains constant power to the hard disk and system when the computer is plugged in
Max Battery	Maintains constant power to the hard disk when the computer is plugged in.

3. Configuring the Network

Windows XP Professional supports both Workgroup Networks and Domain-Based Networks. **Workgroup Networks** are also referred to as Peer-to-Peer networks and are the simplest type of network. They are ideal for networks of less than ten computers and supports file and print sharing. **Domain-Based Networks** are common to large companies and benefit from centralized administration. This results in the implementation of stronger security models with users requiring a user account to logon access network resources.

3.1 Creating Network Connections

In Windows XP Professional you can create number of network connections. These include local area network (LAN) connections, remote connections, Virtual Private Network (VPN) connections and direct connections. All these connections are created in the **NETWORK AND INTERNET CONNECTIONS** folder.

3.1.1 Local Area Network (LAN)

A **Local Area Network** is also referred to as an intranet and has client support, such as Client for Microsoft Networks and Client Services for NetWare; services, such as Files and Printer Sharing; and user network protocols. A network **protocol** is a set of rules and conventions for computers use to communicate over a network. Windows XP Professional supports:

- ***TCP/IP***, which is the default protocol and is installed automatically in Windows XP Professional;
- ***NetBEUI*****,** which is a nonroutable protocol suited for small networks of less than ten computers;
- ***AppleTalk***, which allows a Windows XP Professional-based computer to communicate on Apple Macintosh networks;
- ***NWLink (IPX/SPX)***, which allows a Windows XP Professional-based computer to communicate on Novell NetWare networks; and
- ***DLC***, which is a nonroutable protocol that allows a Windows XP Professional-based computer to communicate to an IBM host.

> **Note:** The AppleTalk protocol requires a Windows 2000 Server that is configured with Windows 2000 Services to function properly.

You can also specify the **protocol binding** order to optimize network performance by placing the protocol that is used the most at the top of the protocol bindings list. The computer will then attempt to use this protocol first when a user attempts to make a connection to a server.

3.1.2 Remote Connections

Remote connections allow mobile computer users to dial into their corporate LAN and are also used to establish a connection to the Internet via an Internet Service Provider (ISP).

3.1.2.1 Remote Access Protocols

Windows XP Professional uses several Remote Access Protocols to allow clients to access Remote Access Servers.

- **PPP** enables remote access clients and servers to operate together in a network. For example, clients running Windows XP Professional can connect to remote networks through any server that uses PPP. Similarly, computers running other remote access software can also use PPP to dial in to a computer running Windows XP Professional configured with an incoming connection. This is the most commonly used remote access protocol.
- Serial Line Internet Protocol (**SLIP**) enables Windows XP Professional–based computers to connect to a SLIP server. SLIP is most commonly used with Telnet, and is not suitable for most modern remote access applications. Windows XP Professional does not include a SLIP server component.
- **RAS** is an older protocol used by Microsoft. Client computers running Windows XP Professional use the RAS protocol to connect to remote access servers running Microsoft Windows NT 3.1, Microsoft Windows for Workgroups, Microsoft MS-DOS, or LAN Manager.

3.1.2.2 Security for Remote Connections

Windows XP Professional uses authentication and authentication protocols to ensure network security. **Authentication** refers to the process in which the computer or network system checks a user's name and password against an authoritative database and only grants access if the user name and password match those in the database. **Authentication protocols** are used to transmit and receive user names and passwords. Windows XP Professional supports a number of authentication protocols:

- **PAP** is the least secure authentication protocol and transmits passwords in plain text, i.e. unencrypted. This is used when two computers cannot negotiate a more secure form of authentication.
- **SPAP** is a proprietary authentication protocol used by Shiva clients to dial in to computers running Windows 2000 Server and by Windows XP Professional clients to dial in to Shiva servers.
- **CHAP** resolves the problem of transmitting passwords in clear text by negotiating a secure form of encrypted authentication by using Message Digest 5 (MD5), which is a challenge-response hashing scheme. You should use CHAP when you have clients that are not running Microsoft operating systems
- **MS-CHAP** uses the same type of authentication but uses MD4 as its hashing method. You can use MS-CHAP for clients running Windows NT version 4.0 and later, or Microsoft Windows 95 and later.
- **MS-CHAP v2** is more advanced than CHAP and MS-CHAP and uses mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving data. You can use MS-CHAP v2 for dial-up clients running Windows 2000 or later, or for VPN clients running Windows NT 4.0 or Windows 98 or later
- **EAP** is an extension of PPP, which is the basis for PPTP, works with dial-in, PPTP and L2TP clients, and allows additional authentication methods with PPP. These include smart cards, public key authentication and certificates

3.1.3 Virtual Private Network (VNP)

Virtual Private Networks (VNP) use a tunneling protocol to secure a private network that is established across a public network. Windows XP Professional supports two tunneling protocols that can be used to create a VNP connection:

- **Point-to-Point Tunneling Protocol (PPTP)**, which is a TCP/IP protocol that can encapsulate TCP/IP, IPX/SPX, or NetBEUI protocols. PPTP tunnels must be authenticated by using the same authentication mechanisms as PPP connections; and

- **L2TP**, which is a combination of PPTP and Layer 2 Forwarding. L2PT does not provide data encryption but relies on **Internet Protocol Security (IPSec)**, which is group of services and protocol that supports the secured transfer of information across an IP internetwork.

IP Address

An IP address is a logical 32-bit address that identifies a TCP/IP host. Each network adapter card in a computer running TCP/IP must have a unique IP address, which has two parts: a network ID that identifies all hosts on the same physical network, and a host ID that identifies a host on the network. An IP Address of 192.168.1.66 indicates that the network ID is 192.168.1, and that the host ID is 66.

Subnet Mask

Subnet mask is used to subnets that divide a large network into multiple physical networks connected with routers. A subnet mask blocks out part of the IP address so that TCP/IP can distinguish the network ID from the host ID. When TCP/IP hosts try to communicate, the subnet mask determines whether the destination host is on a local or remote network. To communicate on a network, the computers must have the same subnet mask.

Default Gateway

The default gateway is a device on a local network that stores network IDs of other networks in the enterprise or Internet. To communicate with a host on another network you must configure an IP address for the default gateway. TCP/IP sends packets for remote networks to the default gateway, which forwards the packets to other gateways until the packet is delivered to a gateway connected to the specified destination.

3.2 IP Addressing

3.2.1 Configuring automatic IP Addressing

In Windows XP Professional client computer can obtain automatically obtain an IP address from a DHCP server or through Automatic Private IP Addressing.

3.2.1.1 DHCP Addressing

If the network has a server running the Dynamic Host Configuration Protocol (DHCP Service, it can automatically assign TCP/IP configuration information to the client computers if the client computers are configured as DHCP clients. You can then configure any client running Windows XP Professional, Windows 2000, Windows 95, and Windows 98 to obtain TCP/IP configuration information automatically from the DHCP Service. This can simplify administration and ensure correct configuration information**.**

3.2.1.2 Automatic Private IP Addressing

Windows XP Professional supports a new mechanism for automatic address assignment of IP addresses for simple LAN-based network configurations called **Automatic Private IP Addressing (APIPA).** This mechanism is an extension of dynamic IP addressing and enables the configuration of IP addresses without using static IP address assignment or installing the DHCP Service.

On a computer running Windows XP Professional you must configure a network LAN adapter for TCP/IP and click **Obtain an IP Address Automatically in the Internet Protocol (TCP/IP)** Properties dialog box for the Automatic Private IP Addressing feature to function properly.

APIPA can be used to set up IP configuration to allow network communication on a single subnet and is also used when the client computer cannot contact the DHCP server for IP address configuration. APIPA uses an addressing range from **169.254.0.1 through 169.254.255.254** and a subnet mask of **255.255.0.0.**

3.2.2 Configuring Static IP Addressing

By default, client computers running Windows XP Professional, Windows 2000, Windows 95, or Windows 98 obtain their IP configuration information automatically from the DHCP Service. However you should assign a static IP address to certain network computers, such as the computer running the DHCP Service. If the DHCP Service is not available, you can configure TCP/IP to use a static IP address. For each network

adapter card that uses TCP/IP in a computer, you can configure an IP address, subnet mask, and default gateway

3.2.3 Testing TCP/IP Configuration

After you configure the TCP/IP configuration, you must restart the computer, and use the *ipconfig* and *ping* command-prompt utilities to test the configuration and connections to other TCP/IP hosts and networks and to ensure that TCP/IP is functioning properly.

- ***Ipconfig*** can be used to verify the TCP/IP configuration parameters on a host. This can be used to determine whether the configuration is initialized, or whether a duplicate IP address exists on the network. Use the *ipconfig* command with the ***/all*** switch to verify configuration information.
- ***Ping*** can be used to test the computer's connectivity after you have verified the TCP/IP configuration. The *ping utility* is a diagnostic tool that you can use to test TCP/IP configurations and diagnose connection failures. You can use the ping utility to determine whether a particular TCP/IP host is available and functional.
- ***Tracert***. Traces the route that a packet takes to a destination. The tracert command displays a list of IP routers that are used to deliver packets from your computer to the destination, and the amount of time that the packet remained at each hop or the destination between two routers. If the packets cannot be delivered to the destination, you can use the tracert command to identify the last router that successfully forwarded the packets.
- ***Nslookup*** Nslookup is a command-line utility that you can use to query and troubleshoot your DNS installation.

  Name resolution errors can result if:
  - DNS client entries are not configured correctly.
  - DNS server is not running.
  - There is a problem with network connectivity.

  At a command prompt, type nslookup to view the host name and IP address of the DNS server that is configured for the local computer.

3.3 Name Resolution

Windows XP Professional supports the use of user-friendly domain names to represent the IP address of a host or a client. This however requires name resolution so that the computer can identify the IP address that the user-friendly name refers to. Windows XP Professional supports two types of name resolution: NetBIOS name resolution and host name resolution.

3.3.1 NetBIOS Name Resolution

Although Microsoft has phased out NetBIOS name resolution, it remains in Windows XP Professional for compatibility purposes. Two of the mechanisms implemented for NetBIOS name resolution are **Windows Internet Naming Service (WINS)**, which is a NetBIOS name server that stores NetBIOS names and their IP Addresses; and the LmHOSTS file, which is a static text file that contains a list of NetBIOS names and their corresponding IP addresses and is stored on the local computer.

3.3.2 Host Name Resolution

Windows XP Professional uses Domain Name Services (DNS) to resolve host names. DNS name servers resolve forward and reverse lookup queries. A forward lookup query resolves a user-friendly domain name to an IP address. A reverse lookup query resolves an IP address to a user-friendly domain name. A name server can resolve a query only for a zone for which it has authority. If a name server cannot resolve the query, it passes the query to other name servers that can resolve the query. The name server caches the query results to reduce the DNS traffic on the network.

DNS Zones

DNS uses *domain name space* is the naming. The DNS database is indexed by name; therefore, each domain must have a name. As you add domains to the hierarchy, the name of the parent domain is appended to its child domain. Consequently, a domain's name identifies its position in the hierarchy. Thus the domain name studyguide.testking.com identifies the studyguides domain as a child domain or subdomain of the testking.com domain and testking as a subdomain of the com domain. A discrete portion of the domain name space is represented as a zone. Zones provide a way to partition the domain name space into manageable sections.

3.4 Enabling and Configuring Internet Connection Firewall

A firewall protects a network against external threats from another network, including the Internet. Firewalls prevent an organization's networked computers from communicating directly with computers that are external to the network and prevent computers external to the network from communicating directly with the computers in the organization's network. All incoming and outgoing communication is routed through a proxy server outside the organization's network. Firewalls also audit network activity, recording the volume of traffic and information about attempts to gain unauthorized access. ICF is firewall software that is used to set restrictions on what information is communicated from your home or small business network to and from the Internet.

To enable and configure ICF:

- On the Desktop, click My Computer
- Click My Network Places
- Click View Network Connections. Windows XP Professional displays the Network Connections window.
- Click the dial-up, LAN, or high-speed Internet connection that you want to protect.
- Under Network Tasks, click Change Settings Of This Connection.
- Click on the Advanced tab
- Select the Protect My Computer And Network By Limiting Or Preventing Access To This Computer From The Internet check box. (To disable ICF, clear the this check box).
- To configure ICF click Settings

The Services tab allows you to specify the services running on your network that Iternet users can access. The Security Logging tab allows you to specify whether or not you want to log dropped packets and successful connections. It also allows you to set the size limit and location of the log file. By default, the log file is PFIREWALL.LOG and the size limit is 4096 KB. To enable security logging, select one or both of the following options: Log Dropped Packets and Log Successful Connections. To view the security log file, in the Security tab, click Browse. The ICMP tab allows you to select which requests for information from the Internet this computer will respond to. By default none of these check boxes are selected.

TABLE 3.1: *Configurable ICMP Options*

Option	Description
Allow Incoming Echo Request	Messages sent to the computer will be repeated back to the sender. This option is commonly used for troubleshooting, such as pinging a computer.
Allow Incoming Timestamp Request	Data sent to this computer can be acknowledged with a confirmation message indicating the time that the data was received.
Allow Incoming Mask Request	This computer will listen for and respond to requests for more information about the public network to which it is attached.
Allow Incoming Router Request	This computer will respond to requests for information about the routes it recognizes.
Allow Outgoing Destination Unreachable	Data sent over the Internet that fails to reach this computer because of an error will be discarded and acknowledged with a "Destination Unreachable" message explaining the failure.
Allow Outgoing Source Quench	When this computer's ability to process incoming data cannot keep up with the rate of a transmission, data will be dropped and the sender will be asked to slow down.
Allow Outgoing Parameter Problem	When this computer discards data it has received because of a problematic header, it will reply to the sender with a "Bad Header" error message.
Allow Outgoing Time Exceeded	When this computer discards an incomplete data transmission because the entire transmission required more time than allowed, it will reply to the sender with a "Time Expired" message.
Allow Redirect	Data sent from this computer will be rerouted if the default path changes.

If you enable any of the ICMP options, your network can become visible to the Internet and vulnerable to attack.

The following are some important ICF considerations:

- ICF is available in the Windows XP Professional 32-bit edition and the Windows XP Home Edition, but it is not available in the Windows XP Professional 64-bit edition.
- ICF should be enabled on your shared Internet connection if your network is using ICS to provide Internet access to multiple computers.
- ICF also protects a single computer that is connected to the Internet with a cable modem, a DSL modem, or a dial-up modem.
- ICF should not be enabled on VPN connections or on client computers; it will interfere with file and printer sharing.

3.5 Enabling Internet Connection Sharing

ICS allows you to connect multiple computers on your home or small business network to the Internet using one connection. One of the computers on your network connects to the Internet using a cable modem, DSL modem, or dial-up modem. You enable ICS on the computer that has the Internet connection and it becomes the ICS host. The other computers on the network then connect to the Internet through this connection.

Note: ICS is available in the Windows XP Professional 32-bit edition and the Windows XP Home Edition, but it is not available in the Windows XP Professional 64-bit edition.

To enable ICS:

- On the Start menu, click My Computer, click My Network Places, and then click View Network Connections. Windows XP Professional displays the Network Connections window.
- Click the dial-up, LAN, PPPoE, or VPN Internet connection that you want to share.
- Under Network Tasks, click Change Settings Of This Connection.
- In the Advanced tab, select the Allow Other Network Users To Connect Through This Computer's Internet Connection check box.
- To configure ICS and select the services running on your network that Internet users can access, click Settings.

3.6 Enabling and Configuring Network Bridge

Network Bridge allows you to connect LAN segments, groups of networked computers, without having to use routers or bridges. Network Bridge allows you to connect different types of network media. Before Network Bridge, if you were using more than one media type, you needed a different subnet for each media type. Packet forwarding would be required because different protocols are used on different media types. Network Bridge automates the configuration that is required to forward information from one media type to another.

Network Bridge uses the Institute of Electrical and Electronics Engineers (IEEE) Spanning Tree Algorithm (STA). STA provides an automated mechanism to ensure that the forwarding topology is loop free. You do not have to do any configuration to configure Network Bridge for STA.

To configure Network Bridge:

- On the Start menu, click My Computer, click My Network Places, and then click View Network Connections. Windows XP Professional displays the Network Connections window.
- Under LAN or High-Speed Internet, select each of the private network connections that you want to make part of the bridge.
- Right-click one of the selected private network connections, and then click Bridge Connections.

3.7 Using the Network Setup Wizard

The Network Setup Wizard is another one of the home and small business components in Windows XP Professional. You first run the Network Setup Wizard on the computer that will be your ICS host computer. The Network Setup Wizard automatically enables and configures ICS and ICF for you. After you run the Network Setup Wizard on the ICS host computer, run it on each of the other computers in the network. All computers other than the ICS host computer are known as client computers. The wizard automatically configures all of the computers on the network so that they function properly in the network.

To run the Network Setup Wizard:

- On the Start menu, click Control Panel.
- In Control Panel, click Network And Internet Connections.
- Click Network Connections and under Pick A Task, click Set Up Or Change Your Home Or Small Office Network.

3.8 Connecting to a Novell NetWare Network

Windows XP Professional computers can use NWLink, Client Services for NetWare, and Gateway (and Client) services for NetWare to connect to a Novell NetWare-based server using IPX/SPX. These are provided on the Windows XP Professional Installation CD. An alternative is Novell Client for Windows NT/2000 which is distributed by Novell.

3.8.1 Configuring NWLink

The NWLink protocol allows Windows XP Professional computers to gain access to applications running on Novell NetWare-based servers. The configuration of NWLink involves three components: frame type, network number, and internal network number. When you install NWLink, Windows XP Professional automatically detects a **frame type**, which defines the way that the network adapter card formats data and should match the frame type on the NetWare server; and a **network number**, which must be unique for each network segment and all computers on a segment using the same frame type must use the same network number to communicate with one another. Windows XP Professional also provides a generic internal network number. However, you must manually specify an internal network number if you plan to run FPNW or IPX routing.

3.9 Connecting to a UNIX Network

Windows XP Professional provides various levels of support for UNIX connectivity.

At the basic level of support, UNIX servers can be regarded as an Internet resource. This is because UNIX uses some of the protocols for communicating that are also available in Windows XP Professional, such as Hypertext Transfer Protocol (HTTP), FTP (File Transfer Protocol), and Telnet. These protocols enable you to access files.

Print Services for UNIX is an add-on network component available in Windows XP Professional that provides access to UNIX line printer remote (LPR) printers.

Windows Services for UNIX 2.0 and Microsoft Interix are Microsoft programs that enable a wide range of interoperability, including the ability to:

- Connect to NFS (Network File System). NFS is the native file format for UNIX, equivalent to the NTFS File System in Microsoft Windows XP Professional.
- Run UNIX shell commands (operating system level commands).
- Run distributed applications on a network computer.

3.9.1 Configuring Interoperability with UNIX

A standard Windows XP Professional installation without any additional Microsoft or third-party software provides basic connectivity to UNIX. This level of connectivity involves utilizing the basic Internet standard Transmission Control Protocol/Internet Protocol (TCP/IP) services and utilities within the Windows XP Professional operating system and the services configured on the UNIX network. This can be viewed as either a temporary change or a permanent configuration of the workstation, as the user can transition between the two network environments. For access to run application and to print to UNIX-based printers, Windows XP Professional provides both print services for UNIX and full Telnet client and server software.

3.9.2 Telnet

Telnet is a TCP/IP protocol found in almost all UNIX environments. Telnet server and Telnet client software are installed as part of the standard Windows XP Professional installation. The Telnet client and the Telnet server work together to allow users to communicate with UNIX workstations and servers.

3.9.2.1 Telnet Client

The Telnet client allows you to connect to a UNIX server and interact with that server through a terminal window as if you were sitting in front of it. Typical uses of Telnet include e-mail, file transfer, and system administration (remotely issuing commands to the UNIX server). When you access a UNIX server running Telnet client, you cannot use applications that interact with the desktop on the UNIX server.

3.9.2.2 Telnet Server

The Telnet server is a connection point for Telnet clients. When Microsoft Telnet server is running on a computer running Windows XP Professional, users on other UNIX workstations running Telnet client software can connect to the computer running Windows XP Professional. When a Telnet client connects to the Windows XP Professional Telnet server, the user is asked to enter a user name and password. By default, only user name and password combinations that are valid on the local server can be used to log on to that server. Once logged on, a user is given a command prompt that can be used as if it had been opened in a command prompt window locally. By default, however, the user cannot use applications that interact with the Windows XP Professional desktop.

All members of the Administrators group can use Telnet. Access to the system through a Telnet server by other users is controlled by membership in the Telnet Clients group. By default, this group contains one entry, “Everyone.” If you want to restrict who can access the system using Telnet, remove “Everyone” from the Telnet Clients group and add the users or groups that you want to give Telnet access to the system. The Telnet server service is not started by default. To start the Telnet service:

- Click on the Start button
- Right-click My Computer
- Click Manage.

- In Computer Management, expand Services and Applications
- Click Services.
- In the details pane, right-click Telnet
- Click Start.

Note: The Telnet server included with Windows XP Professional supports a maximum of two Telnet clients at a time. If you need additional licenses, use Telnet server from the Microsoft Services for UNIX. Services for UNIX supports up to 63 Telnet clients at a time.

4. Setting up and Managing User Accounts

4.1 Types of User Accounts

User accounts are required for accessing local and network resources. Microsoft Windows XP Provides **three different types** of user accounts: local user accounts, which allows a user to log on to a specific computer to gain access to resources on that computer; domain user accounts, which allows a user to log on to the domain to gain access to network resources; and built-in user accounts, which allows a user to perform administrative tasks or to gain access to local or network resources.

Local User Accounts	• Enable users to log on and gain access to resources on a specific computer • Reside in Security Accounts Manager • Must be created on each computer in a workgroup
Domain User Accounts	• Enable users to log on to the domain to gain access to network resources • Reside in Active Directory
Built-in User Accounts Administrator and Guest	• Enable users to perform administrative tasks or gain temporary access to network resources • Reside in SAM (local built-in user accounts) • Reside in Active Directory (domain built-in user accounts)

4.1.1 Local User Accounts

A Local user account allows a user to log on at a local computer and gain access to resources only on the computer where you create the local user account. When you create a local user account, Windows XP Professional creates the account only in that computer's security database, which is called the **local security database**. After the local user account exists, the computer uses its local security database to authenticate the local user account, which allows the user to log on to that computer.

4.1.2 Domain User Accounts

A Domain user account allows a user to log on to the domain and gain access to resources on the **network**. The user provides his or her password and user name during the logon process. By using this information, Windows XP Professional authenticates the user and then builds an access token that contains information about the user and security settings. The access token identifies the user to computers running Windows XP Professional on which the user tries to gain access to resources and is provided for the duration of the logon session.

Active Directory

You create a domain user account in the Active Directory database on a domain controller. The domain controller replicates the new user account information to all domain controllers in the domain. After Windows XP Professional replicates the new user account information, any of the domain controllers in the domain tree can authenticate the user during the logon process.

4.1.3 Built-In User Accounts

Built-in user accounts are **automatically created** by Windows XP Professional. Two commonly used built-in user accounts are the Administrator user account and the Guest user account. Built-in user accounts can be renamed but cannot be deleted.

4.1.3.1 Administrator
The built-in Administrator user account is used for **computer management**. If your computer is part of a domain, the built-in Administrator user account is used to manage the domain configuration. Tasks done using the Administrator user account include creating and modifying user accounts and groups, managing security policies, creating printers, and assigning permissions and rights to user accounts to gain access to resources.

As a **security precaution**, you should create a user account that you use to perform nonadministrative tasks. You should log on by using the Administrator user account only when you perform administrative tasks.

4.1.3.2 Guest
The built-in Guest user account is used to give **occasional users** the ability to log on and gain access to local and network resources. By default the built-in guest user account is disabled in Windows XP Professional.

4.2 Creating User Accounts
4.2.1 Creating Local User Accounts
4.2.1.1 In User Accounts
You can use USER ACCOUNTS in CONTROL PANEL to create local user accounts on a **Windows XP Professional computer**. To create local user accounts:

- Click on the **START** button
- Open the **CONTROL PANEL**
- Open the **USER ACCOUNTS**
- Click on **CREATE NEW USER ACCOUNT**
- Provide the **User Name**
- Set the appropriate **Account Type**
- Click **CREATE ACCOUNT**

4.2.1.2 In Computer Management
You can also use Computer Management to create local user accounts on a **Windows XP Professional computer**:

- Click on the **START** button
- Open **CONTROL PANEL**
- Open **ADMINISTRATIVE TOOLS**
- Open **COMPUTER MANAGEMENT**
- Expand **LOCAL USERS AND GROUPS**
- Right-click the **USERS** folder
- Click **NEW USER**
- Provide the **USER NAME** and a **PASSWORD**
- Set the appropriate **Account Setting**
- Click **CREATE**

4.2.2 Creating Domain User Accounts

You can use Windows 2000 Administrative Tools to create and administer domain user accounts. **Administrative Tools** are installed on a default controller by default but you can remotely manage a domain and its user accounts by installing the Windows 2000 Administrative Tools on a member server or a computer running Windows XP Professional. To create domain user accounts:

- Click on the **START** button
- Open the **CONTROL PANEL**
- Open **PERFORMANCE AND MAINTENANCE**
- Open the **ADMINISTRATIVE TOOLS**
- Open **ACTIVE DIRECTORY USERS AND COMPUTERS**
- Expand the **Domain** that you want to create a user account in
- Right-click the **folder** that will contain the user account
- Point to **NEW**
- Click **USER**
- Configure the **Required User Account Settings**
- Set the appropriate **Password Requirements**
- Click **CREATE**

4.2.3 Copying Domain User Accounts

When you copy an existing domain user account, most of the account properties are copied to the new domain user account. This **simplifies** the process of creating new user accounts by reducing the configuration required to create the new domain user account. To copy an existing domain user account:

- Click on the **START** button
- Open the **CONTROL PANEL**
- Open **PERFORMANCE AND MAINTENANCE**
- Open the **ADMINISTRATIVE TOOLS**
- Open **ACTIVE DIRECTORY USERS AND COMPUTERS**
- Click **USERS**
- Right-click the **User Account** that you want to copy
- Click **COPY**
- Provide the **Required Information** for the new **user account**
- Set the appropriate **Password Requirements**
- Click **NEXT**
- Click **FINISH**

4.3 Configuring Account Policies

4.3.1 Configuring Password Policy

Password Policy allows you to improve system security by controlling how passwords are created and managed. You can for example specify the maximum length of time a password can be used before the user has to change it. Requiring users to change their passwords regularly decreases the chances of an unauthorized person breaking into your computer. You can also specify a minimum password length and

maintain a history of the passwords that a user has used. The latter prevents a user from having two passwords and alternating between them. Table 4.1 lists the password policy options that you can configure.

TABLE 4.1: *Password Policy Options*

Option	Description
Enforce Password History	Prevent the user for specifying a password that they had used previously. Windows XP Professional can track up to 24 previously used passwords for each user. By default, this option is not enabled.
Maximum Password Age	Specifies the number of days a user can log on with a particular password before he or she is required to change the password. The default value is 42 days and can be set to 999 days.
Minimum Password Age	Specifies the number of days a user must keep a password before he or she can change it. The default is 0, which indicates that the password can be changed immediately. However, the minimum password age must be less than the maximum password age.
Minimum Password Length	Specifies the minimum number of characters required in a password. This value can range from 0 up to 14 characters inclusive. A value of 0 indicates that no password is required and is the default value.
Passwords Must Meet Complexity Requirements	Specifies that all passwords must meet the specified minimum password length; comply with the password history settings; contain capitals, numerals or punctuation; and cannot contain the user's account or full name.
Store Password Using Reversible Encryption For All Users In The Domain	This option enables Windows XP Professional to store a reversibly encrypted password for all users in the domain.

You can configure Password Policy on a computer running Windows XP Professional by using Group Policy or Local Security Policy.

- Click on the **START** button
- Point to **PROGRAMS**
- Point to **ADMINISTRATIVE TOOLS**
- Expand **ACCOUNT POLICIES**
- Click **PASSWORD POLICY**
- Right-click the **Password Policy Option** that you want to configure
- Click **SECURITY**
- Set the **Password Policy Option**
- Click **OK**

4.3.2 Configuring Account Lockout Policy

The Account Lockout Policy settings also allow you to improve the security on your computer. If you do not have an account lockout policy in place, an unauthorized user can repeatedly attempt to gain access to your computer. If, however, you have set an account lockout policy, the system will lock out the user account under the conditions you specify in Account Lockout Policy. These conditions are listed in Table 4.2.

TABLE 4.2: *Account Lockout Policy Options*

Setting	Description
Account Lockout Duration	Specifies the number of minutes that the account is locked out for. A value of 0 indicates that the user account is locked out indefinitely until the Administrator unlocks the user account.
Account Lockout Threshold	Specifies the number of invalid logon attempts it takes before the user account is locked out from logging on to the computer. A value of 0 indicates that the account will not be locked out.
Reset Account Lockout Counter After	Specifies the number of minutes to wait before resetting the account lockout counter.

4.4 Managing Users and User Accounts

4.4.1 Managing User Data

In addition to the My Documents folder, Windows XP Professional allows you to create home folders for users to store their personal documents. You can locate all users' home folders on a client computer, or in a shared folder on a file server, or in a central location on a network server.

Storing all home folders on a **file server** provides the following advantages:

- Users can gain access to their home folders from any client computer on the network.
- The backing up and administration of user documents is centralized.
- The home folders are accessible from a client computer running any Microsoft operating.

4.4.2 Using User Profiles

A user profile is used to store the user's desktop environment, application settings, and personal data. User profiles maintain consistency for users in their desktop environments by providing users with the same desktop environment they had the last time they logged on to the computer.

Windows XP Professional supports four types of user profiles:

- **Default User Profile**, which serves as the base for all user profiles;
- **Local User Profile**, which is created the first time that a user logs on at a computer and is specific to the local computer as it is stored on the computer;
- **Roaming User Profile**; and
- **Mandatory User Profile**.

4.4.2.1 Roaming User Profiles

An administrator can set up roaming user profiles to support users who work at **different computers**. This profile is stored on a network server so that the profile is available to user regardless of where the user logs on in the domain. When a user logs on, Windows XP Professional copies the roaming user profile from the network server to the client computer running Windows XP Professional at which the user logs on and consequently, the user always receives the appropriate desktop settings and connections.

When a user logs on, Windows XP Professional applies the roaming user profile settings to that computer. The first time that a user logs on at a computer, Windows XP Professional copies all documents to the local computer. Thereafter, when the user logs on to the computer, Windows XP Professional compares the locally stored user profile files and the roaming user profile files. It copies only the files that have changed since the last time the user logged on at the computer. This shortens the logon process.

When a user logs off from the network, Windows XP Professional copies changes that were made to the local copy of the roaming user profile back to the server where it is stored.

4.4.2.2 Mandatory User Profiles

A mandatory profile is similar to a roaming user profile except that it does not save any changes a user made to the profile when the user logs off from the network. It is thus a read-only roaming user profile. Windows XP Professional allows an administrator to assign one mandatory user profile to multiple users who require the same desktop settings. This means that when the administrator changes one profile, he or she changes the desktop environment for several users.

The ***Ntuser.dat*** file, which is a hidden file located in the folder that contains the profile, contains that section of the Windows XP Professional system settings that applies to the individual user account, and the user environment settings. By renaming the file to ***Ntuser.man*** the administrator makes the file read-only and thus mandatory.

4.5 Managing Users by Using Groups

An administrator can group a number of users together to **manage** user **access** to shared network resources. These groups are called user groups and can form the basis for assigning to users the required **permissions and rights** to access the network resources. When the administrator assigns permissions and rights to a group, those permissions are applied to all the members of the group. Users can be placed in multiple user groups and one user group can be placed in another user group. The latter is referred to as **nesting**. In a domain, user groups can be used to centralize user administration.

In a domain, Windows XP Professional supports different **types of groups** and scopes. In a Windows XP Professional domain, there are two types of user groups:

- **Security groups**, which are used to perform security-related duties; and
- **Distribution groups**, which are used by applications for non-security related functions.

5. Network Printing

Larger companies use network-interface print devices as network connections transfer data more quickly than printer cable connections. You can add a printer for a network-interface print device by using the Add Printer wizard. The main differences between adding a printer for a local print device and adding a printer for a network-interface print device is that for a typical network-interface print device, you provide additional port and network protocol information.

The default network protocol for Windows XP Professional is TCP/IP, which many network-interface print devices use. For TCP/IP, you provide additional port information in the Add Standard TCP/IP Printer Port wizard.

Printer Terminology

Printer: **A printer is the software interface between the operating system and the print device.**

Print Device: **A print device is the hardware device that produces printed documents.**

Printer Driver: **A printer driver is one or more files containing information that Windows 2000 requires to convert print commands into a specific printer**

Note: Like Windows 2000 Professional, Windows XP Professional only allows a maximum of 10 concurrent connections from other computers for file and print services and does not support Apple Macintosh computers or Norvell NetWare clients but does support UNIX computers. If you need to support more than 10 concurrent connections to a printer, you must install the printer on a Windows 2000 server.

5.1 Setting Up Client Computers

You need to set up client computers to use the printer device. All client computers require that a printer driver be installed. Windows XP Professional automatically downloads the printer drivers for client computers running Windows XP Professional, Windows 2000, Windows NT 4 and earlier, Windows 98, and Windows 95. Client computers running other Microsoft operating systems require installation of printer drivers. Client computers running non-Microsoft operating systems require installation of both printer drivers and the print service on the print server. Windows XP Professional, Windows 2000, Windows NT, Windows 98, and Windows 95 users only need to make a connection to the shared printer. The client computer automatically downloads the appropriate printer driver if a copy of it resides on the print server.

5.1.1 Using the Add Printer Wizard

Windows XP Professional, Windows 2000, Windows NT, Windows 98, or Windows 95 users can use the Add Printer Wizard to connect to a printer. The options that are available in the **Add Printer Wizard** that allow you to locate and connect to a printer vary depending on the operating system that the client computer is running.

- **Windows XP Professional** users can use the **Add Printer Wizard** to can make a connection to a printer by:
  - Using the UNC name (***print_server**printer_name***) to make connections by selecting **Type The Printer Name Or Click Next To Browse For A Printer** on the Locate Your Printer page of the **Add Printer Wizard**

- **Browsing the network** for the printer by selecting **Type The Printer Name Or Click Next To Browse For A Printer** on the **Locate Your Printer** page of the **Add Printer Wizard**, leaving the Name box blank, and clicking Next.
- Using the URL name on the Internet or your intranet by selecting **Connect To A Printer On The Internet Or On Your Intranet** on the **Locate Your Printer** page of the Add Printer Wizard.
- Searching the **Active Directory** directory services if the computer is a member of a domain.

- **Windows NT 4, Windows 98, and Windows 95** users can use the **Add Printer Wizard** to can make a connection to a printer by:
  - Using the UNC name; or
  - Browsing **Network Neighborhood** to locate the printer.

5.1.2 Downloading Printer Drivers

When Windows XP Professional, Windows XP Home Edition, Windows 2000, Windows NT, Windows 98, and Windows 95 clients first connect to a printer on the print server, the client computer automatically downloads the printer driver if the print server has a copy of the printer driver. Thereafter, these client computers running Windows XP Professional, Windows 2000 and Windows NT verify that they have the current printer driver every time they connect to the print. For these computers, you need only update the printer drivers on the print server. Client computers running Windows 98 and Windows 95 do not check for updated printer drivers. You must therefore manually install updated printer drivers on these computers.

5.2 Setting Up a Printer Pool

A printer pool is one printer that is connected to multiple print devices through multiple ports on a print server. Print devices should be identical but you can use print devices that use the same printer driver.

5.3 Setting Printer Priorities

Setting priorities between printers makes it possible to set priorities between groups of documents that all print on the same print device. Multiple printers point to the same print device, which allows users to send critical documents to a high-priority printer and noncritical documents to a lower-priority printer. The critical documents always print first. Point two or more printers to the same print device, i.e., the same port. The port can be either a physical port on the print server or a port that points to a network-interface print device.

5.4 Novell and UNIX Printers

Windows XP Professional provides Client Service for NetWare, a network software add-in that you can use to enable your computer to interoperate with NetWare servers. When installed on a computer running Windows XP Professional, Client Service for NetWare enables access to files on the NetWare server and printing to the NetWare printer. For computers to interoperate with each other, they must be running the same protocols. NWLink, a component of Client Service for NetWare, provides that interoperability. NWLink is an Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX)-compatible protocol that is automatically installed when you install Client Service for NetWare.

You can access NetWare printers depending on the methods of authentication. To connect to a NetWare printer using a Graphical User Interface (GUI):

- Click on the START button
- Click on Control Panel
- Click Printers and Other Hardware
- Click Add a Printer
- Click Next to start the Add Printer Wizard.
- On the Local or Network Printer page, click A network printer or a printer attached to another computer
- Click Next
- On the Specify a Printer page, click Connect to this printer, type the name of a printer in the following format: \\server_name\printer_name (where server_name is the name of the server to which you want to connect, and printer_name is printer to which you want to connect
- Click Next.

5.4.1 Installing a Printer Using LPR

In a mixed environment where printing services are distributed, users need to be able to print to any or all print devices. To enable printing to UNIX printers, you must install Print Services for UNIX, and then set up an LPR port and install the printer. The LPR port is best suited to servers that communicate with UNIX machines.

To install Print Services for UNIX:

- Click on the Start button
- Click Control Panel
- Click Add or Remove Programs
- Click Add/Remove Windows Components
- Scroll and select the Other Network File and Print Services check box
- Click the Details button to ensure Print Services for UNIX is highlighted
- Click OK
- Click Next
- Follow the wizard instructions.

A network-connected printer must have a card that supports line printer daemon (LPD) protocol for TCP/IP printing to work properly. To set up an LPR port and install the printer on a computer running Windows XP Professional:

- Click on the START button
- Click Control Panel
- Click Printers and Other Hardware
- Click Printers and Faxes
- Click Add a Printer
- Click Next
- On the Local or Network Printer page, click Local printer attached to this computer
- Clear the Automatically detect and install my Plug and Play printer check box
- Click Next

- On the Select a Printer Port page, click Create a new port
- Click LPR Port
- Click Next
- Provide the required information
- Follow the instructions in the wizard to finish installing the printer.

Note: Before you can add the LPR port, you must first install Print Services for UNIX

TABLE 5.1: *Services for Non-Microsoft Operating Systems Client Computers*

Client	Required Services
Macintosh	Services for Macintosh. This is not included not Windows XP Professional but is included with Windows 2000 Server.
UNIX	TCP/IP Printing, which is also called the LPD Service, is included with Windows 2000 Server but is not installed by default. It is not included with Windows XP Professional.
NetWare	File and Print Services for NetWare (FPNW), an optional add-on service for Windows 2000 Server, is not included with Windows XP Professional or Windows 2000 Server.

6. Shared Network Resources

6.1 Shared Files and Folders

You can **share resources** with other user on a network by sharing folders containing those resources. When you share a folder, you can **control access** to the folder by limiting the number of users who can simultaneously gain access to it, and you can also control access to the folder and its contents by **assigning permissions** to selected users and groups. Once you have shared a folder, users must connect to the shared folder and must have the appropriate permissions to gain access to it. In a Windows XP Professional **workgroup**, members of the built-in **Administrators** and **Power Users** groups can share folders on Windows XP Professional client computers and on the Windows 2000 stand-alone server which is part of the workgroup. In a Windows 2000 **domain,** the **Administrators** and **Server Operators** groups can share folders residing on any machines in the domain. The **Power Users** group is a local group and can share folders residing only on the stand-alone server or computer running Windows XP Professional where the group is located.

> **Note:** The **Power Users** group is a **local group** and can only share folders residing only on the stand-alone server or computer running Windows XP Professional where the group is located.

6.1.1 Shared Folder Permissions

- Shared folder permissions apply to **folders**, not individual files. Since you can apply shared folder permissions only to the entire shared folder, and not to individual files or subfolders in the shared folder, shared folder permissions provide less detailed security than NTFS permissions.
- Shared folder permissions are only applied to users who connect to the folder over the **network** and not to users who gain access to the folder at the computer where the folder is stored.
- Shared folder permissions can secure network resources on a **FAT** or **FAT32** volume, on which you cannot implement NTFS permissions.
- The default shared folder permission is **Full Control**, and it is assigned to the **Everyone group** when you share the folder.

TABLE 6.1: *Shared Folder Permissions*

Shared Folder Permission	Description
Read	Display folder names, filenames, file data, and attributes; run program files; and change folders within the shared folder.
Change	Create folders, add files to folders, change data in files, append data to files, change file attributes, delete folders and files, plus, it allows the user to perform actions permitted by the Read permission.
Full Control	Change file permissions, take ownership of files, and perform all tasks permitted by the Change permission.

You can also **allow** or **deny** shared folder permissions. Applying shared permissions to user accounts and groups affects access to a shared folder. Denying permission takes **precedence** over the permissions that you allow.

Multiple Shared Folder Permissions Combine: A user's **effective permissions** for a resource are the sum of the Shared Folder permissions that you assign to the individual user account and to all of the groups to which the user belongs. In other words, if a user has Read permission for a folder and is a member of a group with Change permission for the same folder, the user has both Read and Change permissions for that folder.

Denying Shared Folder Permissions Overrides Other Permissions: Denied permissions **take precedence** over any permissions that you may have granted the user accounts and groups. If you deny a shared folder permission to a user, the user will not have that permission, even if you allow the permission for a group of which the user is a member.

NTFS Permissions Are Also Required On NTFS Volumes: Shared folder permissions can be used to grant users access to files and folders on a FAT or FAT32 volume but not on an **NTFS volume**. On a FAT or FAT32 volume, you can grant users access to a shared folder as well as all of the files and subfolders contained in the shared folder. To grant users access to a shared folder on an NTFS volume, you must grant them the shared folder permission and the appropriate **NTFS permissions** for each file and folder that you want them gain access to.

Copied or Moved Shared Folders Are Not Shared: When you copy a shared folder, the original shared folder is still shared, but the copy is **not shared**. When you move a shared folder, it is no longer shared.

6.1.2 Combining Shared Folder Permissions and NTFS Permissions

Shared folder permissions provide limited security for resources. You gain the greatest flexibility by using NTFS permissions to control access to shared folders. Also, NTFS permissions apply whether the resource is accessed locally or over the network. Therefore, a strategy for providing access to resources on an NTFS volume is to share folders with the default shared folder permissions and then control access by assigning NTFS permissions. When you share a folder on an NTFS volume, both shared folder permissions and NTFS permissions combine to secure file resources.

6.1.3 Shared Application Folders

Applications that are installed on a network server and can be used by users from their client computers must be placed in shared application folders. The **advantage** of shared applications is that you do not need to install and maintain most components of the applications on each computer. The program files for the applications can be stored on the server, while configuration information for the applications can be stored on each client computer.

- You should create one shared folder for applications and **organize** all of your applications under this folder. When you combine all applications under one shared folder, you designate one location for **installing and upgrading** software.
- You should assign the **Administrators group** the **Full Control** permission for the applications folder so that they can **manage** the application software and control user permissions.
- You should **remove** the **Full Control** permission from the **Everyone group** and assign the **Read** permission to the **Users group**. This provides more security because the Users group includes only user accounts that you created, whereas the Everyone group includes anyone who has access to network resources, including the Guest account.

> **Note: Removing** a permission form a user account or a group differs from **Denying** the permission to that user or group. If you deny a shared folder permission to a user, the user will not have that permission, even if you allow the permission for a group of which the user is a member. If you remove a permission form a user account, the user may still have the permission by virtue of his or her membership to another group that has been granted that permission.

- You should assign the **Change** permission to groups that are responsible for **upgrading and troubleshooting** applications.
- You should create a **separate shared folder** outside your shared application folder for any application for which you need to assign **different permissions**. You can then assign the appropriate permissions to that folder.

6.1.4 Data Folders

A collective group of workers that work on a common project can use data folders to exchange public and working data over the network. **Working data folders** can be used by members of a team to access shared files. **Public data folders** are used by larger groups of users who all need access to common data.

6.1.5 Administrative Shares

Windows XP Professional automatically shares folders for administrative purposes. These shares are appended with a **dollar sign ($)**, which hides the shared folder from users who browse the computer. The root of each volume, the system root folder, and the location of the printer drivers are all hidden shared folders that you can gain access to across the network.

- The **root** of each volume on a hard disk is automatically shared, and the share name is the **drive letter** appended with a dollar sign ($). When you connect to this folder, you have access to the entire volume. You use the administrative shares to remotely connect to the computer to perform administrative tasks. Windows XP Professional assigns the **Full Control** permission to the **Administrators** group.
- The **system root folder**, which is *C:\Winnt* by default, is shared as **Admin$**. Administrators can gain access to this shared folder to administer Windows XP Professional without knowing in which folder it is installed. Only members of the Administrators group have access to this share. Windows XP Professional assigns the **Full Control** permission to the **Administrators** group.

- When you install the first **shared printer**, the ***systemroot*\ System32\Spool\Drivers folder** is shared as **Print$**. This folder provides access to printer driver files for clients. Only members of the **Administrators**, **Server Operators**, and **Print Operators** groups have the **Full Control** permission. The **Everyone group** has the **Read** permission.

> **Note:** You can hide additional shared folders by appending a dollar sign to the end of the share name. Only users who know the folder name will then be able to access it if they also possess the proper permissions to it.

6.2 Offline Files

Windows XP Professional allows users to work with network files when they are not connected to the network. This is called offline files. To make shared files available offline, copies of the files are stored in a portion of the user's hard disk. This portion is called a **cache**. Since the cache is on the user's hard disk, the user can access this cache regardless of whether it is connected to the network. By default, the cache size is set to **10 %** of the available disk space. To change the size of your cache

- Click on the **START** button
- Point to **PROGRAMS**
- Point to **ACCESSORIES**
- Open **WINDOWS EXPLORER**
- Click on the **TOOLS** menu
- Open **FOLDER OPTIONS**
- Click the **OFFLINE FILES** tab
- Select the **ENABLE OFFLINE FILES** check box
- Adjust the **AMOUNT DOSK SPACE TO USE FOR TEMPORARY OFFLINE FILES** slider

6.2.1 Enabling Offline Files

When you share a folder, you can allow others users to make the shared folder available for offline use on their computers. To do this

- Click on the **START** button
- Point to **PROGRAMS**
- Point to **ACCESSORIES**
- Open **WINDOWS EXPLORER**
- Browse to the **Shared Folder** you want to make available for offline use
- Right-click the **Shared Folder**
- Click the **PROPERTIES** on the popup menu
- Click on the **SHARING** tab
- Click on the **CACHING** tab
- Select the **ALLOW CACHING OF FILES IN THIS SHARED FOLDER** check box
- Select the **SETTINGS** you want to use

Note: You must enable the caching of files for offline access on the computer where the files reside on and not on the client computer that you want to have access to the files when the computer is offline.

The Caching Settings dialog box contains three caching options:

- **Manual Caching For Documents**. The files that someone using your shared folder specifies for offline access are the only files that are cached. This caching option is recommended for a shared network folder containing files that are accessed and modified by several people and is the default.
- **Automatic Caching For Documents**. Caches every file that someone opens from your shared folder and makes it available for offline use. Files that the user does not open are not cached and are therefore not available for offline use.
- **Automatic Caching For Programs**. Provides offline access to shared folders containing files that are read, referenced, or run, but that are not changed in the process. This setting reduces network traffic because offline files are opened directly without accessing the network versions in any way, and generally start and run faster than the network versions.

6.2.2 Offline File Synchronization

When a user has modified an offline file, the file on the network must be updated with the one on the user's computer. This updating occurs through a process called synchronization. Windows XP provides several options for setting when synchronization should occur. These are:

- Automatically at log on
- Automatically at log off
- Automatically at a specified time
- Automatically after the computer has been idle for a specified amount of time
- Manually at any time

7. Controlling Access to Network Resources

Windows XP Professional allows you to control who has access to network resources through permissions that are stored in an Access Control List.

7.1 Access Control List

NTFS stores an **access control list (ACL)** with every file and folder on an NTFS volume. The ACL contains a list of all user accounts and groups that have been granted access to the file or folder, as well as the type of access that they have been granted. When a user attempts to gain access to a resource, the ACL must contain an entry, called an **access control entry (ACE)**, for the user account or a group to which the user belongs. The entry must allow the type of access that is requested for the user to gain access. If the access control entry does not exist or the entry does not match the type of access the user requests, the user will not be granted access to the resource.

7.2 NTFS Permissions

7.2.1 NTFS Folder Permissions

You can control the access that users have to folders and to the files and subfolders that are contained within the folder by assign folder permissions to the users and user groups.

> **Note:** You require the NTFS file system to use NTFS File and Folder permissions.

There are six permissions that you can assign to users and user groups:

- **Read** Allows the user to see files and subfolders in the folder and view folder ownership, permissions, and attributes.
- **Write** Allows the user to create new files and subfolders within the folder, change folder attributes, and view folder ownership and permissions.
- **List Folder Contents** Allows the user to see the names of files and subfolders in the folder.
- **Read & Execute** Allows the user to browse through folders to reach other files and folders, even if the users do not have permission for those folders. It also allows the user to perform actions permitted by the Read permission and the List Folder Contents permission.
- **Modify** Allows the user to delete the folder and perform actions permitted by the Write permission and the Read & Execute permission.
- **Full Control** Allows the user to change permissions, take ownership, and delete subfolders and files. It also allows the user to perform actions permitted by all other NTFS folder permissions.
- **Deny** Denies a user account or group all access to a folder and denies the Full Control permission.

> **Note:** Administrators, owners of files or folders, and users with Full Control permissions can assign NTFS permissions to other users and groups.

7.2.2 NTFS File Permissions

You can control the access that users have to files by assigning file permissions to the users. The NTFS file permissions that you can assign are

- **Read** Allows the user to read the file, and view file attributes, ownership, and permissions.
- **Write** Allows the user to overwrite the file, change file attributes, and view file ownership and permissions.
- **Read & Execute** Allows the user to run applications. Also allows the user to perform the actions permitted by the Read permission.
- **Modify** Allows the user to modify and delete the file. It also allows the user to perform the actions permitted by the Write permission and the Read & Execute permission.
- **Full Control** Allows the user to change permissions and take ownership of the file. It also allows the user to perform the actions permitted by all the other NTFS file permissions.

> **Note:** NTFS file permissions take **priority** over NTFS folder permissions. A user or user group with access to a file will be able to gain access to the file even if he or she does not have access to the folder containing the file. A user can gain access to the files for which he or she has permissions by using the **full universal naming convention (UNC)** or local path to open the file from its respective application, even though the folder in which it resides will be invisible if the user has no corresponding folder permission. Without permission to access the folder, you will not see the folder, so you will not be able to browse for the file you want to access.

7.2.3 Multiple NTFS Permissions

You can assign multiple permissions to a user account and to each group that the user is a member of. The user can thus be granted multiple permissions on the basis of the user's group membership.

> **Note:** The **Deny** permission overrides all other file and folder permissions that the user may have been granted in other groups. This can effectively prevent a particular user access to a file or folder without having to remove the user from the group.

7.2.4 Cumulative Permissions

A user's **effective permissions** for a resource is the sum of the NTFS permissions that you assign to the individual user account and to all of the groups to which the user belongs. In other words, if a user has Read permission for a folder and is a member of a group with Write permission for the same folder, the user has both Read and Write permission for that folder.

7.2.5 The Deny Permission

Denying a permission overrides all instances where that permission is allowed. Even if a user has permission to gain access to the file or folder as a member of a group, denying permission to the user blocks any other permission that the user might have.

7.2.6 Setting NTFS Permissions

By default, when you format a volume with NTFS, the **Full Control** permission is assigned to the **Everyone group**. As all user groups that you create on the computer are automatically added to the Everyone group, all users have the Full Control permission. As a security precaution, you should change this default permission and assign other appropriate NTFS permissions to control the access that users have to resources.

7.2.7 NTFS Permissions Inheritance

By default, permissions that are assigned to a **parent folder** are inherited by and propagated to the subfolders and files that are contained in the parent folder. This is indicated on the Security tab in the Properties dialog box by a check mark in the **Allow Inheritable Permissions From Parent To Propagate To This Object** check box. You can however prevent permissions inheritance. To prevent a subfolder or file from inheriting permissions from a parent folder, clear the Allow Inheritable Permissions From Parent To Propagate To This Object check box. If you clear this check box, you are prompted to select one of the options that are described in Table 7.1.

> **Note:** The folder for which you prevent permissions inheritance becomes the **new parent folder**, and permissions that are assigned to this folder will be inherited by the subfolders and files that are contained within it.

TABLE 7.1: *Permission Inheritance Options*

Option	Description
Copy	Copy the permissions from the parent folder to the current folder and then deny subsequent permissions inheritance from the parent folder.
Remove	Remove the permissions that are inherited from the parent folder and retain only the permissions that you explicitly assign to the file or folder.
Cancel	Cancel the dialog box and restore the check mark in the Allow Inheritable Permissions From Parent To Propagate To This Object check box.

7.2.8 Assigning Special Access Permissions

The standard NTFS permissions generally provide all of the access control that you need to secure your resources. However, sometimes the standard NTFS permissions do not provide the specific level of access that you might want to assign to users. To create a specific level of access, you can assign NTFS special access permissions.

There are fourteen special access permissions. Two of them are particularly useful for controlling access to resources: Change Permissions and Take Ownership.

7.2.8.1 Changing Permissions

You can give other administrators and users the ability to change permissions for a file or folder without giving them the **Full Control** permission over the file or folder. In this way, the administrator or user cannot

delete or write to the file or folder but can assign permissions to the file or folder. To give administrators the ability to change permissions, assign **Change Permissions** to the Administrators group for the file or folder.

7.2.8.2 Taking Ownership

You can **transfer ownership** of files and folders from one user account or group to another user account or group. You can give someone the ability to take ownership of a file or folder. As an administrator, you can also take ownership of a file or folder.

Certain rules apply to taking ownership of a file or folder. These are:

- The **owner** of the file or folder, or any user with **Full Control** permission can assign the Full Control standard permission or the Take Ownership special access permission to another user account or group, allowing the user account or a member of the group to take ownership.
- An **administrator** can take ownership of a folder or file, regardless of assigned permissions. If an administrator takes ownership, the Administrators group becomes the owner and any member of the Administrators group can change the permissions for the file or folder and assign the Take Ownership permission to another user account or group.
- For **example**, if an employee leaves the company, an administrator can take ownership of the employee's files, assign the Take Ownership permission to another employee, and then that employee can take ownership of the former employee's files.
- The user or a group member with Take Ownership permission must **explicitly take ownership** of the file or folder

7.2.9 Copying and Moving Files and Folders

- When you **copy** files or folders from one folder to another folder, or from one volume to another volume, permissions change.
- When you **copy** a file within a single NTFS volume or between NTFS volumes:
  - Windows XP Professional treats it as a **new file**. As a new file, it takes on the permissions of the destination folder.
  - You must have **Write permission** for the destination folder to copy files and folders.
  - You become the **CREATOR OWNER**.

> **Note:** When you copy or move files or folders to **FAT** volumes or to a **floppy disk**, the folders and files lose their NTFS permissions because FAT volumes and floppy disks do not support NTFS permissions.

- When you move a file or folder within a single NTFS volume
  - The file or folder retains the original permissions.
  - You must have the Write permission for the destination folder to move files and folders into it.
  - You must have the Modify permission for the source file or folder. The Modify permission is required to move a file or folder because Windows XP Professional deletes the file or folder from the source folder after it is copied to the destination folder.
  - The owner of the file or folder does not change.
- When you move a file or folder between NTFS volumes

- The file or folder inherits the permissions of the destination folder.
- You must have the Write permission for the destination folder to move files and folders into it.
- You must have the Modify permission for the source file or folder. The Modify permission is required to move a file or folder because Windows XP Professional deletes the file or folder from the source folder *after* it is copied to the destination folder.
- You become the CREATOR OWNER.

8. Monitoring Resources and Performance

8.1 Monitoring Applications

You can use the **Applications** tab in **Task Manager** to view the applications running in current user's security context. This can be used to troubleshoot computer performance problems. On Applications tab you can:

- View the status of an application;
- Shut down a non-responding application;
- Switch to another application;
- Start a new application; and
- Identify the processes that are associated with a particular application.

8.2 Monitoring Processes

You can use the **Processes** tab to view a list of running processes and the total processor time and the amount of memory the process is using. The list that appears on the Processes tab includes all processes that run in their **own address space** and includes system services. Both the user and the system can initiate a process, but you can only end a process that has been initiated by a user.

Note: Some applications have more than one associated process. Therefore, when you use the Applications tab to close an application that is not responding, not all the associated processes will be closed. You should rather right click the application that is not responding, click **Go To Process**, then right click the highlighted process and click **End Process Tree**.

8.2.1 Using Process Measures to Identify Resource Usage

You can use the **Process** tab in **Task Manager** to identify the resources used by the applications that are running. Processes can be sorted by any measure, enabling you to view the processes in ascending or descending order for that particular measure.

8.2.2 Promoting and Demoting Process Priority

Each process running on a computer is assigned a base priority. The priority that a process is assigned determines the order in which it can gain access to system resources. Promoting the priority of a process can make it run faster. Demoting the priority of a process can make it run slower.

To view the base priority:

- Press **Ctrl-Alt-Delete**
- Click **Task Manager**
- Click on the **View** menu
- Click **Select Columns**
- Select **Base Priority** check box

- Click **OK**

To change the priority assigned to a process:

- Press **Ctrl-Alt-Delete**
- Click **Task Manager**
- Click on the **Process** tab
- Right-click the process
- Point to **Set Priority**
- Select the priority that you want to assign.

8.3 Monitoring System Performance

8.3.1 Using Task Manager

You use the **Performance** tab in **Task Manager** to monitor the current performance of your computer. The Performance tab shows overall computer performance and displays a dynamic overview of the computer's current performance, including a numeric display and graph of processor and memory usage.

CPU Usage displays the current processor usage, while the **CPU Usage History** graph shows the history of processor usage. **MEM Usage** displays the current memory usage, while the **Memory Usage History** graph shows a combined history of the information in the MEM Usage column on the Processes tab.

TABLE 8.1: *Performance Tab Performance Measures*

Process Measures	Description
Totals	The number of handles, threads, and processes running on the computer.
Physical Memory (in KB)	**Total**: Amount of installed physical RAM **Available**: Amount of physical memory available to processes **System Cache**: Amount of physical memory released to the file cache on demand.
Commit Charge (in KB)	**Total**: Size of virtual memory in use by all processes. **Limit**: Amount of virtual memory that can be committed to all processes without enlarging the paging file. **Peak**: Maximum amount of virtual memory used in the session. If the commit peak exceeds the commit limit, virtual memory is temporarily expanded to accommodate the new peak.
Kernel Memory (in KB)	**Total**: Sum of paged and nonpaged memory. **Paged**: Size of the paged memory pool allocated to the operating system. **Nonpaged**: Size of the nonpaged memory pool allocated to the operating system

8.3.2 Using the Performance Console

You can monitor system performance by using Performance Console and its counters. This can be used to determine the computer's efficiency and locate and resolve current or potential bottleneck problems.

The Performance Console contains a number of objects, each with its own set of counters. Table 8.2 describes a few of the available Performance Console objects.

TABLE 8.2: *Some Performance Console Objects*

Object Option	Description
Cache	Monitors the file system cache that is used to buffer physical device data
Memory	Monitors the physical and virtual memory
PhysicalDisk	Monitors a hard drive
Processor	Monitors processors

8.3.2.1 Adding Counters

To monitor the performance of an object, you must add the appropriate counter that is relevant to the aspects of the object you want to monitor. To add counters to an object in Performance Console:

- on the **START** button
- Point to **PROGRAMS**
- Point to **ADMINISTRATIVE TOOLS**
- Open **PERFORMANCE**
- Right-click the **COUNTERS**
- Click **ADD COUNTERS**
- In the **Performance Object** box, select the **OBJECT** for which you want to add counters.
- Select a **COUNTER** from the list
- Click **ADD**
- When you have selected the desired objects and counters, click **CLOSE**

TABLE 8.3: *Some Useful Performance Console Counters*

Counter	Description
Processor: %Processor Time	The percentage of time that the processor spends executing a non-idle thread. A count that is continuously above 75% indicates that the processor is causing a bottleneck and should be upgraded.
Memory: Pages/Sec	The number of pages that were not in RAM when requested or had to be moved to virtual memory to free up RAM. A count of up to 20 is acceptable.
PhysicalDisk: %Disk Time	The amount of time the disk drive is busy. A count of over 50% indicates a system problem.

PhysicalDisk: Disk Queue Length	The number of waiting I/O requests. A count of up to 2 is acceptable.

8.4 Monitoring Network Connectivity
Windows XP Professional also has a **Networking** tab in **Task Manager** that you can use to monitor statistics about network connections currently in use. Monitoring the activity of network connections will enable you to determine if a network connection is functioning properly. The **Networking** tab has three parts:

- Menus that enable users to configure views and options;
- Charts that show bytes per second through the network interface as a percentage of available bandwidth; and
- A table that lists measures for each network card.

8.5 Monitoring Event Logs
Windows XP Professional records events in three logs:

- System log, which contains events generated by the system components in Windows XP Professional;
- Application log, which contains events generated by applications; and
- Security log which records security events, such as valid and invalid logon attempts, and events related to resource use, such as creating, opening, or deleting files. An administrator can specify which events are recorded in the Security log.

You can use Event Viewer to view these logs.

To open Event Viewer:

- Click on the **Start** button
- Click **Control Panel**
- Click **Performance and Maintenance**
- Click **Administrative Tools**
- Double-click **Event Viewer**

8.5.1 Event Logs
Event logs allow you to monitor information about hardware, software, system problems, and security. These logs can also be used to provide a history of events.

8.5.2 System and Application Events
By monitoring system and application events you can identify and track resource use, system errors, and application errors. System events, which are automatically configured by Windows XP Professional, are recorded in the System log while application events, which are determined by the application developer, are recorded in the Application log. After events are recorded in these logs, you can view and analyze the logs to detect activities and events that require administrative consideration. Based on your analysis of the logs,

you may need address system problems or reallocate resources. You may also need to address changes in application configuration or system configuration.

There are three types of system and application events:

- **Information** Indicates information about the successful operations of applications, drivers, or services.
- **Warning** Indicates information about events that are not urgent, but may indicate a future problem with system operations.
- **Error** Indicates information about significant problems with system operations, such as loss of data or loss of functionality.

8.6 Audit Policies

An *audit policy* defines the types of security events that Windows XP Professional records in the security log on each computer.. Windows XP Professional writes events to the security log on the computer on which the event occurs and allows you to track the events that you specify.

You use Event Viewer to view events that Windows XP Professional has recorded in the security log. You can also archive log files to track trends over time.

When you plan an audit policy, you must determine what you want to audit and the computers on which to set up auditing. Auditing is turned off by default. The types of events that you can audit includes:

- Accessing files and folders
- Logging on and off
- Shutting down a Windows XP Professional computer
- Starting a Windows XP Professional computer
- Changing user accounts and groups
- Attempting to make changes to Active Directory objects if your Windows XP Professional computer is part of a domain

You can also determine whether to audit the success of events, the failure of events, or both. Tracking successful events can tell you how often Windows XP Professional or users access specific files, printers, or other objects, and you can use this information for resource planning. Tracking failed events can alert you to possible security breaches.

8.6.1 Configuring Auditing

For computers running Windows XP Professional, you set up an audit policy for each individual computer. Toset up and administer auditing you must have the **Manage Auditing And Security Log** user right for the computer on which you want to configure an audit policy or review an audit log. These rights are granted to the Administrators group by default. Furthermore, you can only audit files and folders to NTFS volumes.

8.6.2 Setting up Auditing

Setting up auditing is a two-part process:

1. **Set the audit policy.** The audit policy enables auditing of objects but doesn't activate auditing of specific objects.
2. **Enable auditing of specific resources.** You designate the specific events to audit for files, folders, printers, and Active Directory objects. Windows XP Professional then tracks and logs the specified events.

8.6.2.1 Setting an Audit Policy

The first step in implementing an audit policy is selecting the types of events you want Windows XP Professional to audit. You set audit policies for a local computer in the Group Policy snap-in, which can be accessed by using the Microsoft Management Console (MMC) console and adding the Group Policy snap-in. The types of events that Windows XP Professional can audit are:

- Account Logon Events
- Account Management
- Directory Service Access
- Logon Events
- Object Access
- Policy Changes
- Privilege Use
- Process Tracking
- System Events

8.6.3 Auditing Access to Files and Folders

You can set up auditing for files and folders on NTFS partitions to audit user access to files and folders. However, you must first set your audit policy to audit **object access**, which includes files and folders.

When you set your audit policy to audit object access, you enable auditing for specific files and folders and specify which types of access, by which users or groups, to audit.

8.6.4 Auditing Access to Printers

Audit access to printers to track access to sensitive printers. To audit access to printers, set your audit policy to **audit object access**, which includes printers. Enable auditing for specific printers and specify which types of access to audit and which users will have access.

Information about events that are monitored by an audit policy are contained in the security log on the computer on which the event occurred. You can use **Event Viewer** to view these events from any computer if you have administrative privileges for the computer where the events occurred. To view the security log on a remote computer, open the MMC console and point Event Viewer to a remote computer.

8.6.5 Locating Events

When you first start Event Viewer, it displays all events that are recorded in the selected log. You can use the Filter command to change what appears in the log and to locate selected events. You can also search for specific events using the Find command.

TABLE 8.4: *Options for Filtering and Finding Events*

Option	Description
Event Types	The types of events to view.
Event Source	The software or component driver that logged the event.

Category	The type of event, such as a logon or logoff attempt or a system event.
Event ID	An event number to identify the event. This number helps product support representatives to track events.
User	A user logon name.
Computer	A computer name.
From and To	The date ranges for which to view events (Filter tab only).
Restore Defaults	Clears any changes in this tab and restores all defaults.
Description	The text that is in the description of the event (Find dialog box only).
Find Next	Finds and displays the next occurrence defined by the Find Settings.

8.7 Archiving Logs

Archiving security logs allows you to maintain a history of security-related events. This allows you to track trends in Windows XP Professional by comparing logs from different periods. Viewing trends helps you determine resource use and plan for growth. You can also use logs to determine patterns of unauthorized resource access. Windows XP Professional allows you to control the size of the logs and to specify the action that it takes when a log becomes full.

If you want to archive, clear, or view an archived log, select the log you want to configure in Event Viewer, click the Action menu, and then click one of the options described in Table 8.5.

TABLE 8.5: *Options to Archive, Clear, or View a Log File*

Option	Do This
Archive the log	Click Save Log File As and then type a filename.
Clear the log	Click Clear All Events to clear the log. Windows XP Professional creates a security log entry stating that the log was cleared.
View an archived log	Click New Log View; add another view of the selected log.

Note: When the log file becomes full and you have specify the **Do Not Overwrite Events (Clear Log Manually)** action, Windows XP Professional stops. You can therefore use this configuration to ensure that Windows XP Professional only operates while auditing occurs.

8.8 Monitoring Access to Shared Folders

You can monitor access to shared folders to determine **how many** users are **currently connected** to each folder. You can also monitor open files to determine which users are gaining **access to the files**, and you can **disconnect** users from one or all **open files**.

8.8.1 Monitoring Shared Folders

You can use the **Shares** folder in either the **Computer Management** snap-in or the **Shared Folders** snap-in to view a list of all shared folders on the computer and to determine how many users are connected to each folder. To open the shares folder

- Open **MY COMPUTER**
- Open **CONTROL PANEL**
- Open **ADMINISTRATIVE TOOLS**
- Click on the **COMPUTER MANAGEMENT**
- Expand **SYSTEM TOOLS**
- Expand **SHARED FOLDERS**
- Click on **SHARES**

Note: You can use Shares folder in Computer Management to identify the **path** to all **shared folders** in the domain as well as the administrative shares on the local computer.

The **Computer Management** snap-in or **Shared Folders** snap-in can also be used to determine the maximum number of users that are permitted to gain concurrent or simultaneous access to a folder, and whether the maximum number of users that are permitted to gain concurrent access to a folder has been reached. This is one quick and easy way to troubleshoot connectivity problems. If a user cannot connect to a share, determine the number of connections to the share and the maximum connections allowed. If the maximum number of connections has already been made, the user cannot connect to the shared resource.

8.8.2 Modifying Shared Folder Properties

You can modify existing shared folders **properties** from the Shares folder clicking the **shared** folder, and then on the **Action** menu, click **Properties**. The **General** tab of the **Properties** dialog box shows you the share name, the path to the shared folder, and any comment that has been entered. The **General** tab also allows you to view and set a user limit for accessing the shared folder. The **Security** tab allows you to view and change the shared folders permissions.

8.8.3 Monitoring Open Files

The **Open Files** folder in either the **Computer Management** snap-in or **Shared Folders** snap-in can be used to view a list of open files that are located in shared folders and the users who are currently connected to each file. You can use this information to contact users so that you can notify them that you are about to shut down the system.

8.8.4 Disconnecting Users from Open Files

When you make changes to the NTFS permissions for a file that is currently opened by a user, the new permissions will not affect the user until he or she closes and then attempts to reopen the file as a user retains all permissions for a shared resource that Windows XP Professional assigned when the user connected to it. These permissions are evaluated again the next time that a connection is made.

Note: Disconnecting users from open files can result in **data loss**. To prevent data loss you should **notify** users that are connected to shared folders or files that there will be a disruption to the computer or resource availability.

8.8.5 Monitoring Network Users

You can also use the **Computer Management** snap-in or the **Shared Folders** snap-in to monitor which users are currently connected to shared folder resources on a server from a remote computer, and you can view the resources to which the users is connected. You can also disconnect users and send administrative messages to computers and users, including computers and users who are not currently connected to network resources from the **Computer Management** snap-in or the **Shared Folders** snap-in.

8.8.6 Monitoring User Sessions

You can use the **Computer Management** snap-in or the **Shared Folders** snap-in to identify which users have a connection to open files on a server and the files to which they have a connection. This information can be used to determine which users you should contact when you need to stop sharing a folder or shut down the server on which the shared folder resides. You can also disconnect one or more users to free idle connections to the shared folder, to prepare for a backup or restore operation, to shut down a server, and to change group membership and permissions for the shared folder.

8.8.7 Disconnecting Users

You can use the **Shared Folders** snap-in to disconnect one or all users that are connected though a network to a computer if:

- You have made changes to shared folder and NTFS permissions and want the changes to take immediate effect.
- You want to free idle connections on a computer so that other users can make a connection when you reach the maximum number of connections.
- You want to shut down a server.

Note: Disconnecting users from open files can result in **data loss**. To prevent data loss you should **notify** users that are connected to shared folders or files that there will be a disruption to the computer or resource availability.

8.8.8 Sending Administrative Messages to Users

You should send administrative messages to users who are currently connected to a computer on which network resources are shared when there will be a disruption to the computer or resource availability, such as when you are about to:

- Perform a backup or restore operation
- Disconnect users from a resource
- Upgrade software or hardware
- Shut down the computer

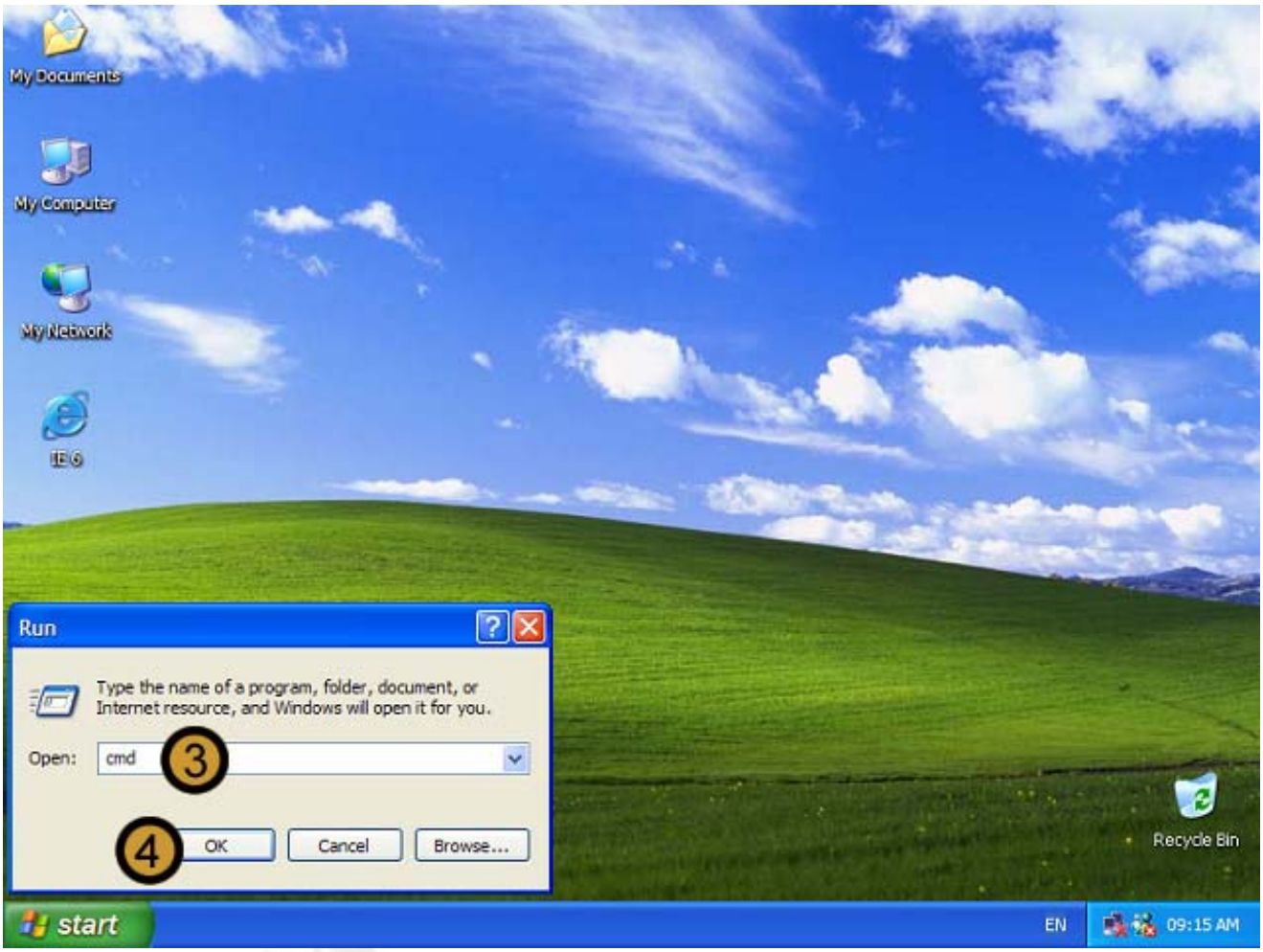
You can use the **Computer Management** snap-in or the **Shared Folders** snap-in to send administrative messages to users. By default, all currently connected computers to which you can send a message appear in the list of recipients. You can also add other users or computers that are not currently connected to resources on the computer to this list.

9. Practice Labs

9.1 Converting the hard drive to NTFS

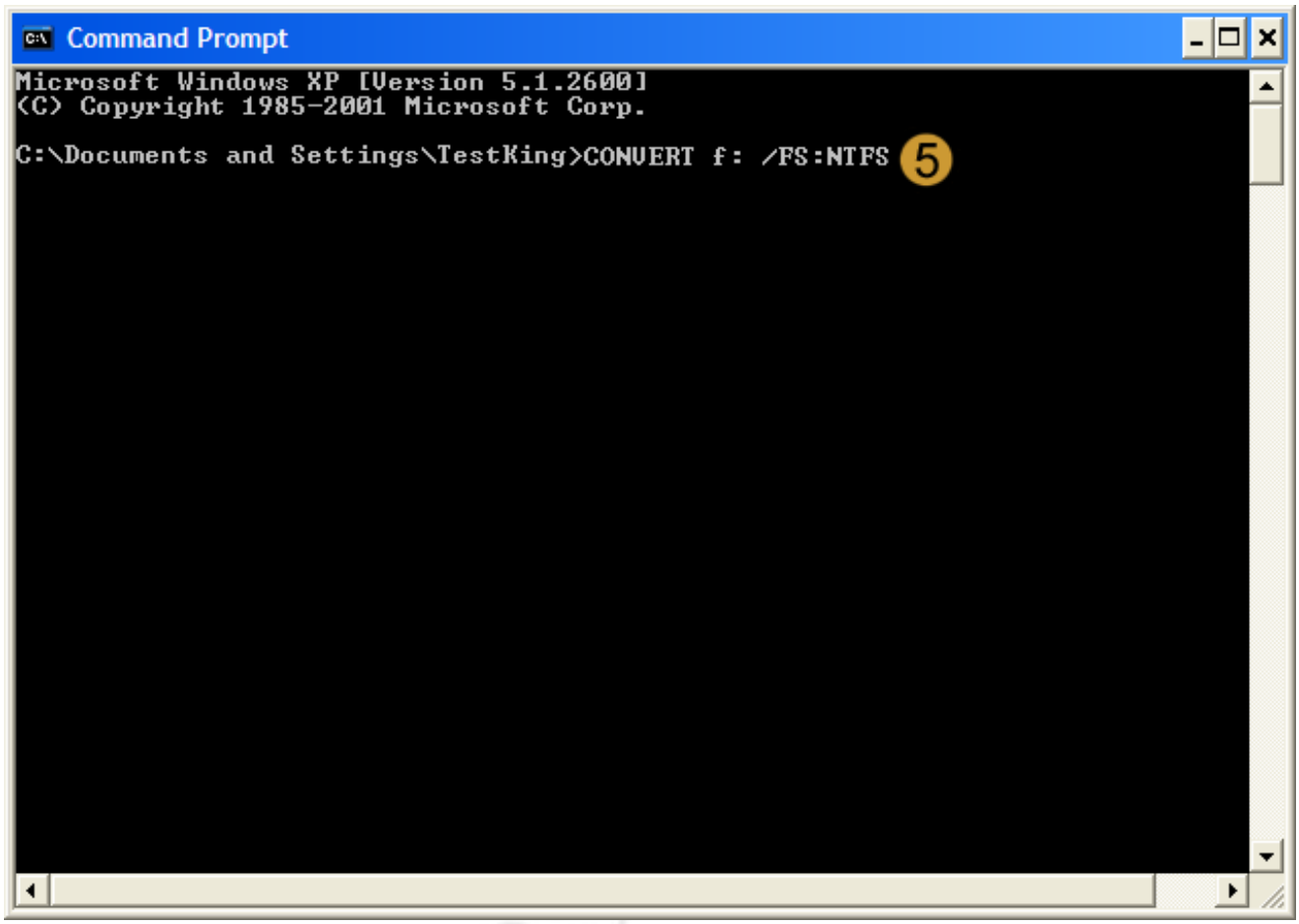
1. Click on the **START** button

2. Click on **RUN**



3. In the RUN dialog box, type **cmd**

4. Click **OK**

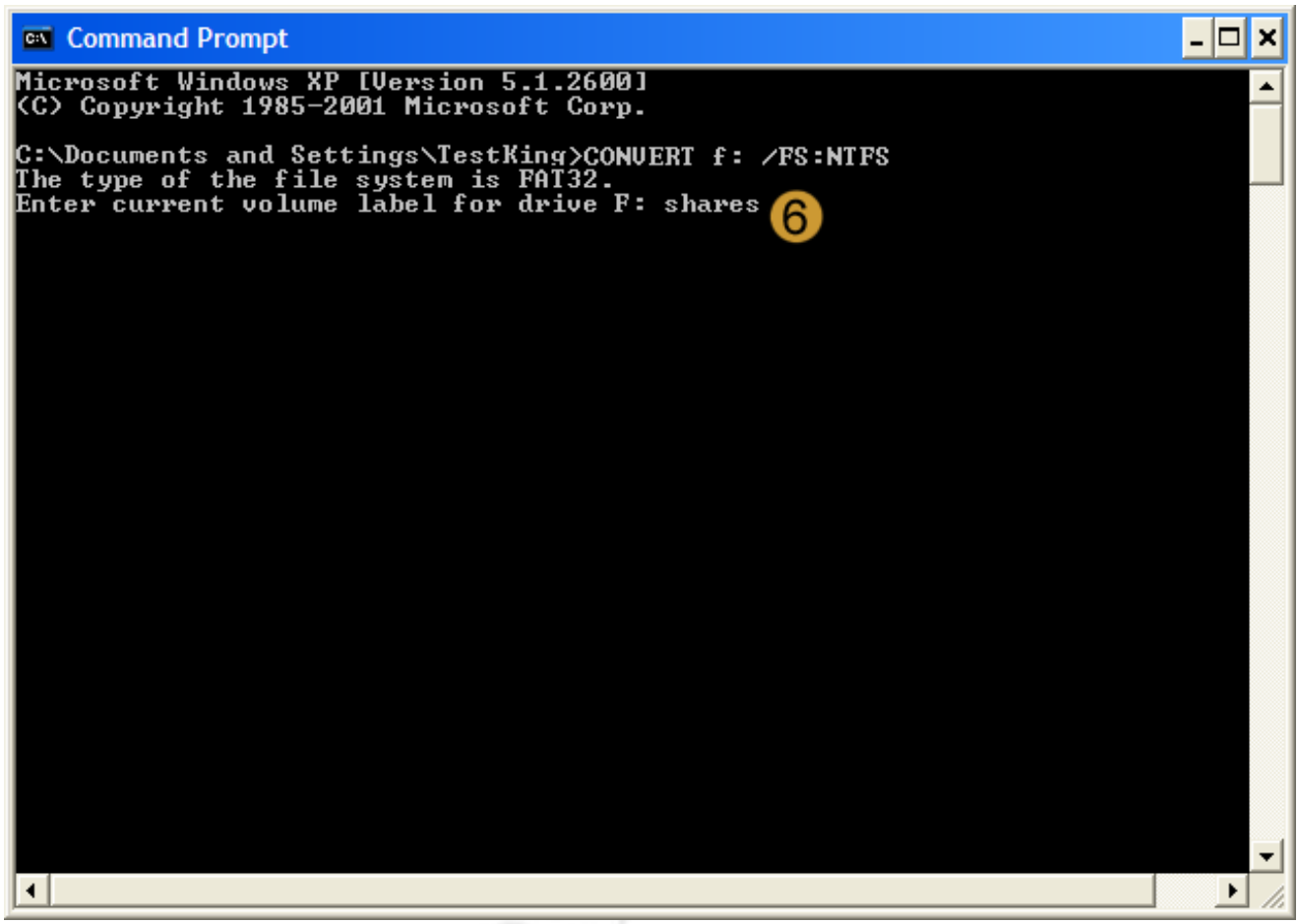


The COMMAND PROMP appears

5. At the COMMAND PROMPT, type **`convert <drive letter> /fs:ntfs`** and press **`Enter`**

In this example we will be converting the F drive. Therefore we have typed:
`convert f: /fs:ntfs`

Note: The Convert command-line utility does not support converting drives to FAT or FAT32. Therefore there is **no /fs:fat or /fs:fat32** command-line switches and we cannot convert a drive back to the FAT or FAT32 file system. To return the drive to the FAT of FAT32 file system we would have to **format** the drive. This would result in the data on the drive being erased.



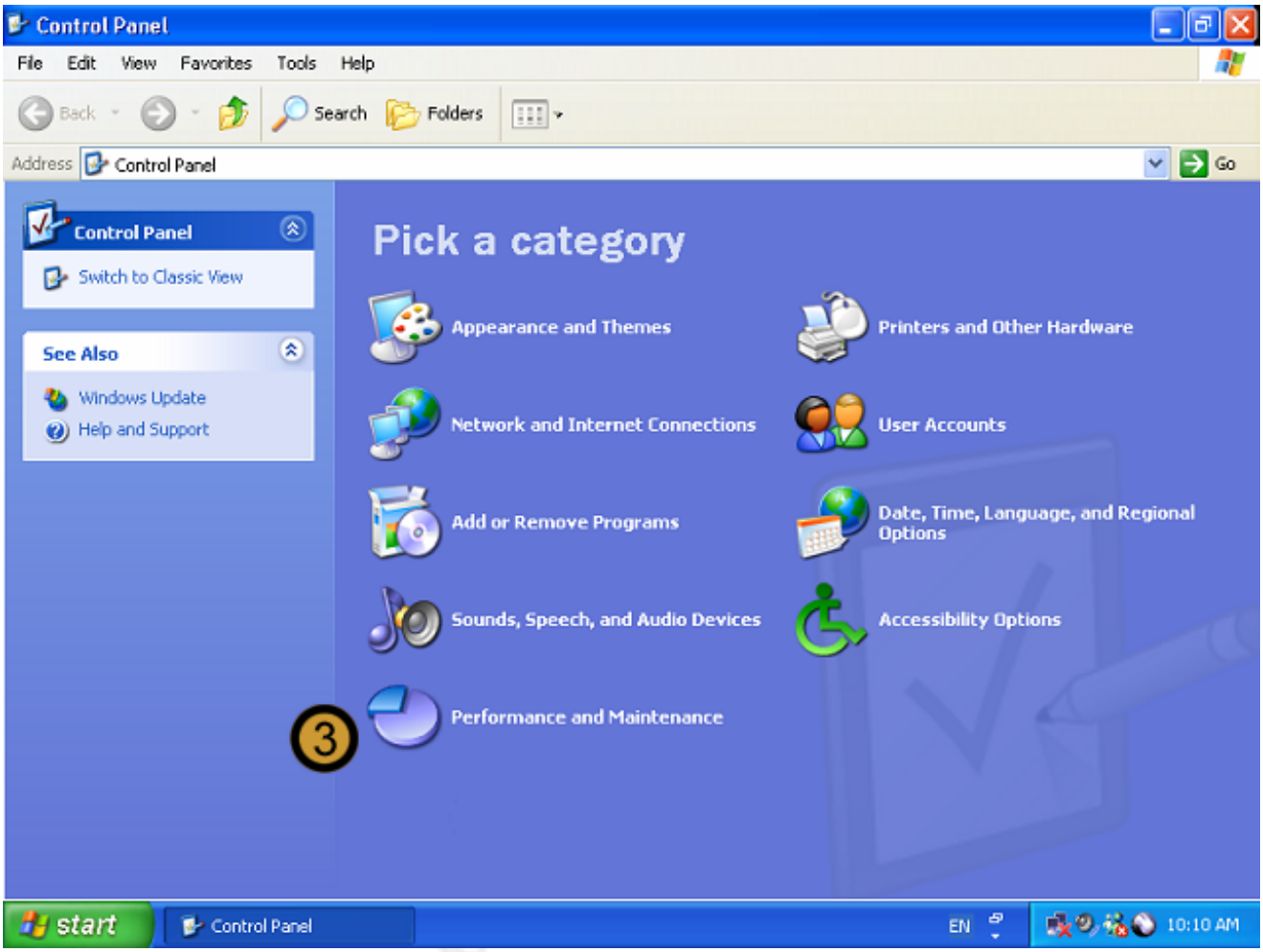
6. If the drive has a volume label, Windows XP Professional will ask you to enter it. Once you have entered the volume label, press **Enter**

Windows XP Professional converts the drive to the NTFS file system while keeping the integrity of the data on the drive in tact.

9.2 Configuring Dual Boot Options

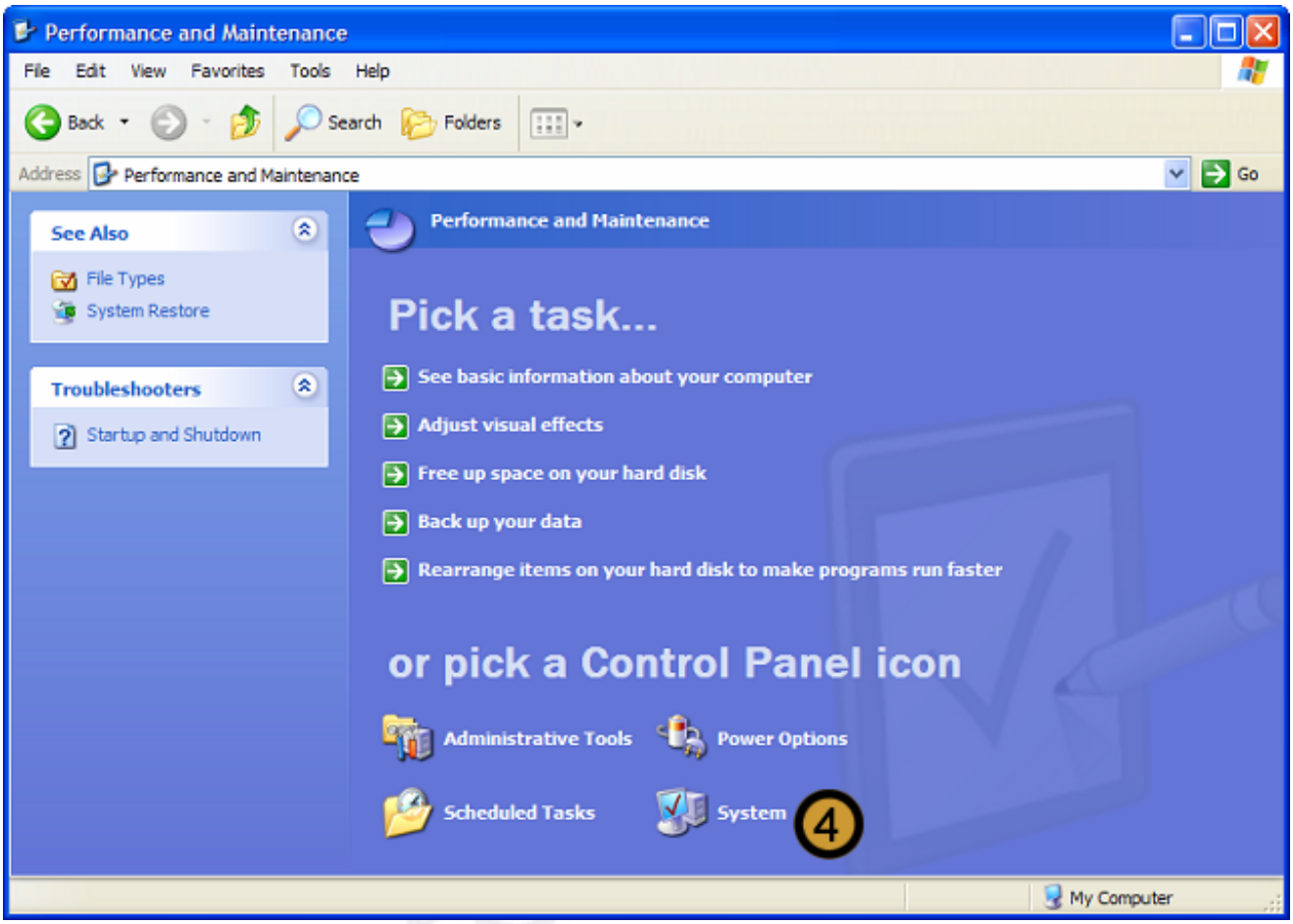
1. Click on the **START** button

2. Click on **CONTROL PANEL**

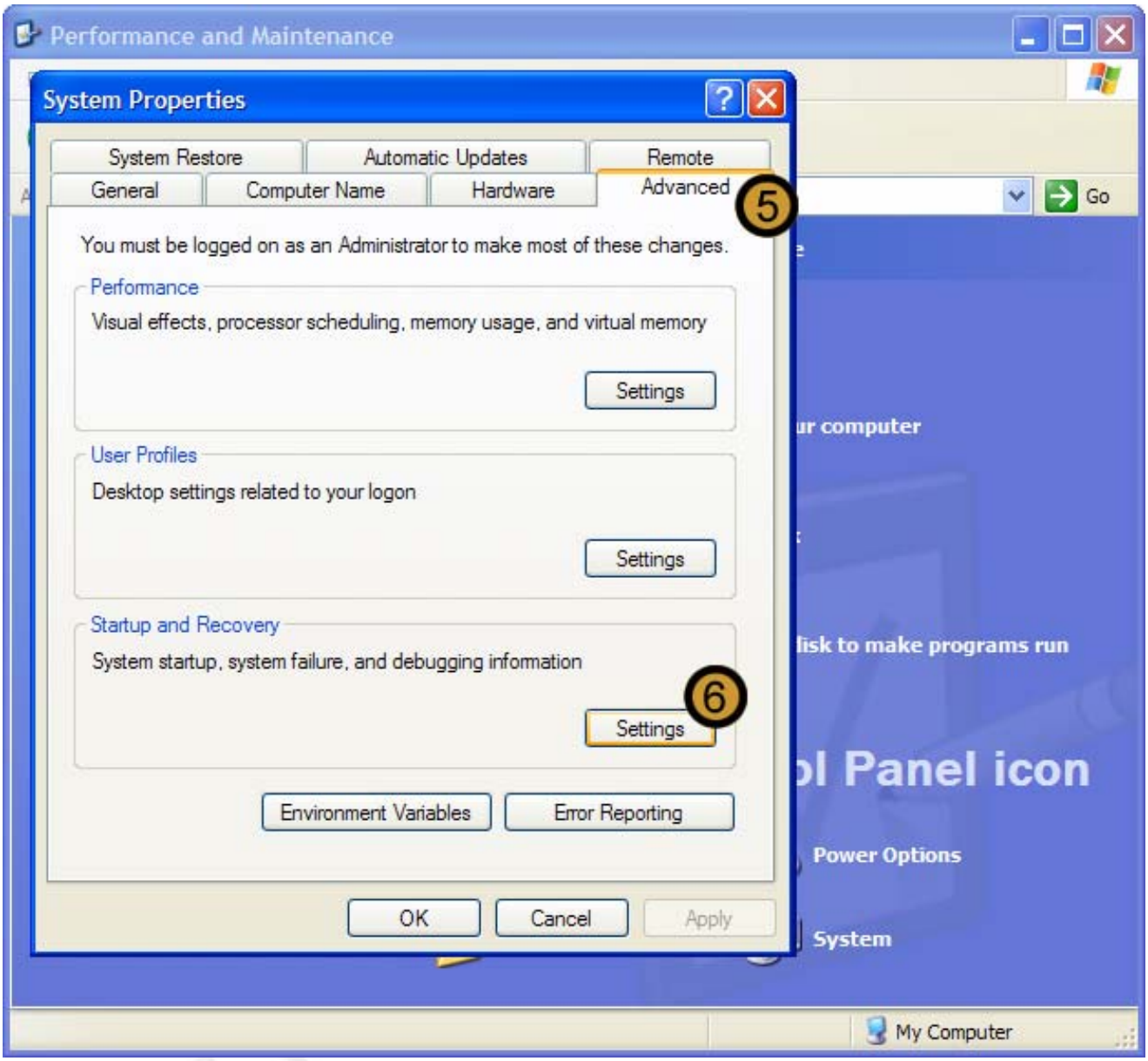


The **Control Panel** appears

3. In the CONTROL PANEL, click on the **PERFORMANCE AND MAINTENANCE** icon



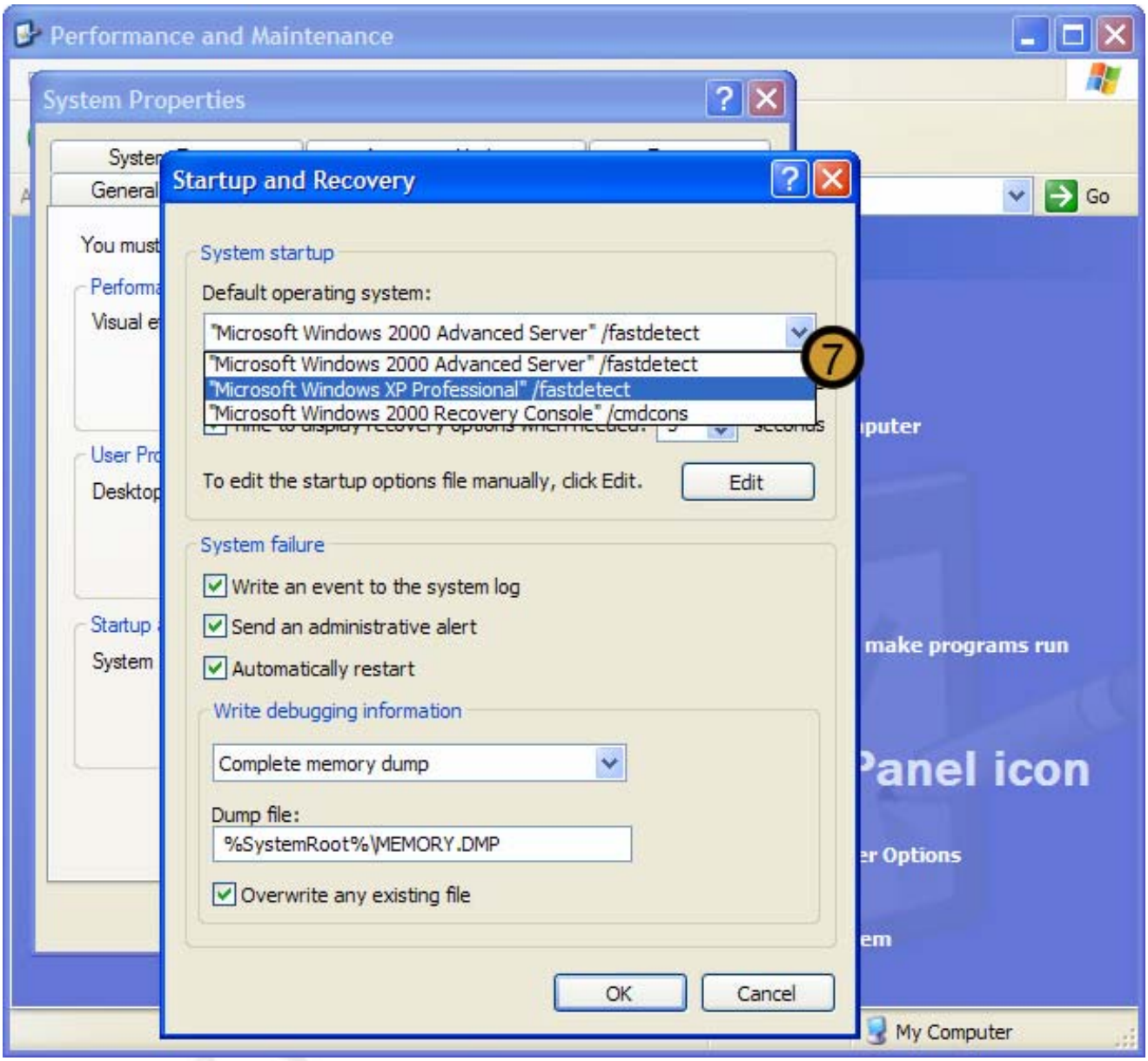
4. In PERFORMANCE AND MAINTENANCE, click **SYSTEM**



The SYSTEM PROPERTIES dialog box appears

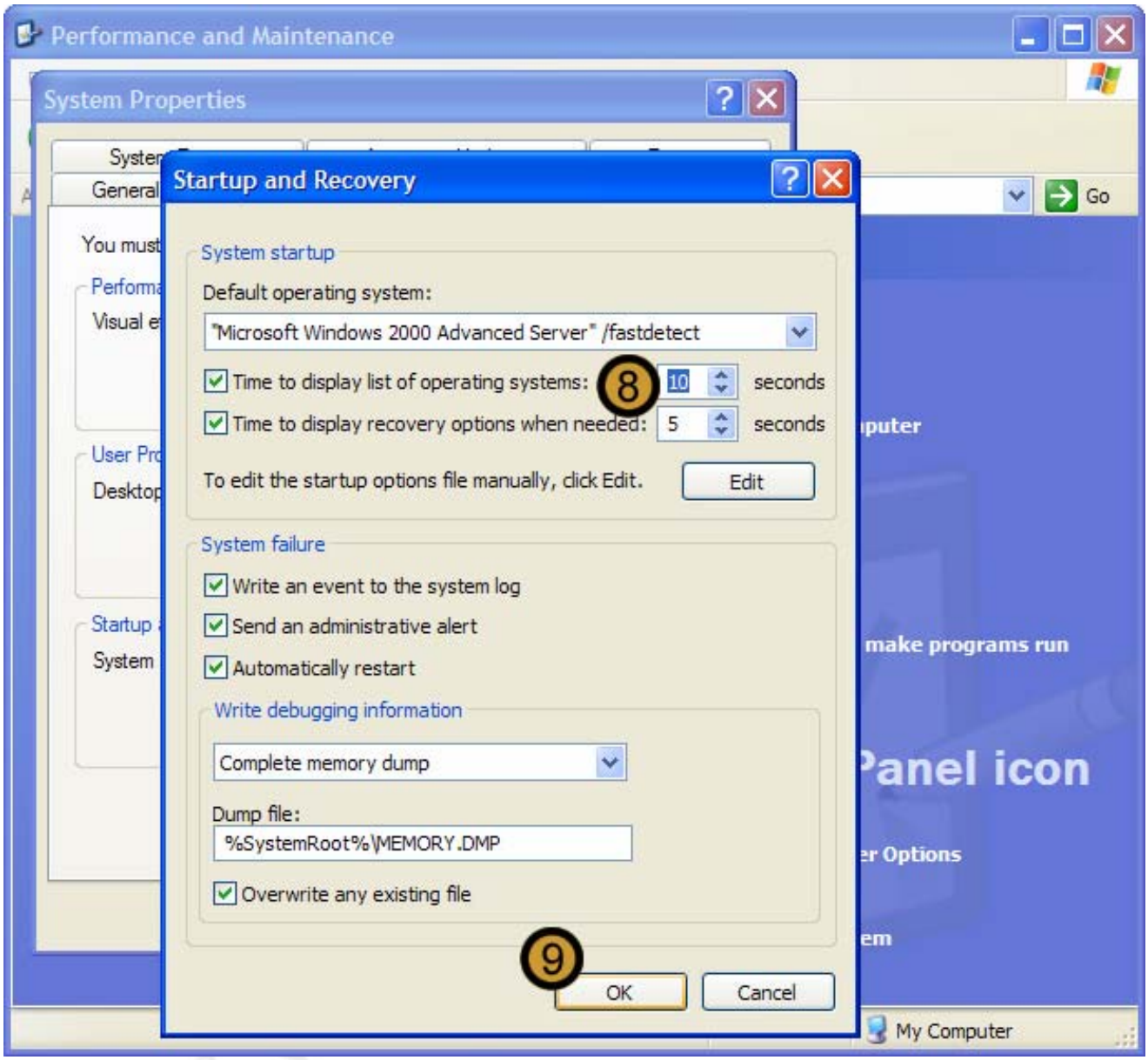
5. In SYSTEM PROPERTIES dialog box, click on the **ADVANCED** tab

6. In the STARTUP AND RECOVERY section of the SYSTEM PROPERTIES dialog box, click **SETTINGS**



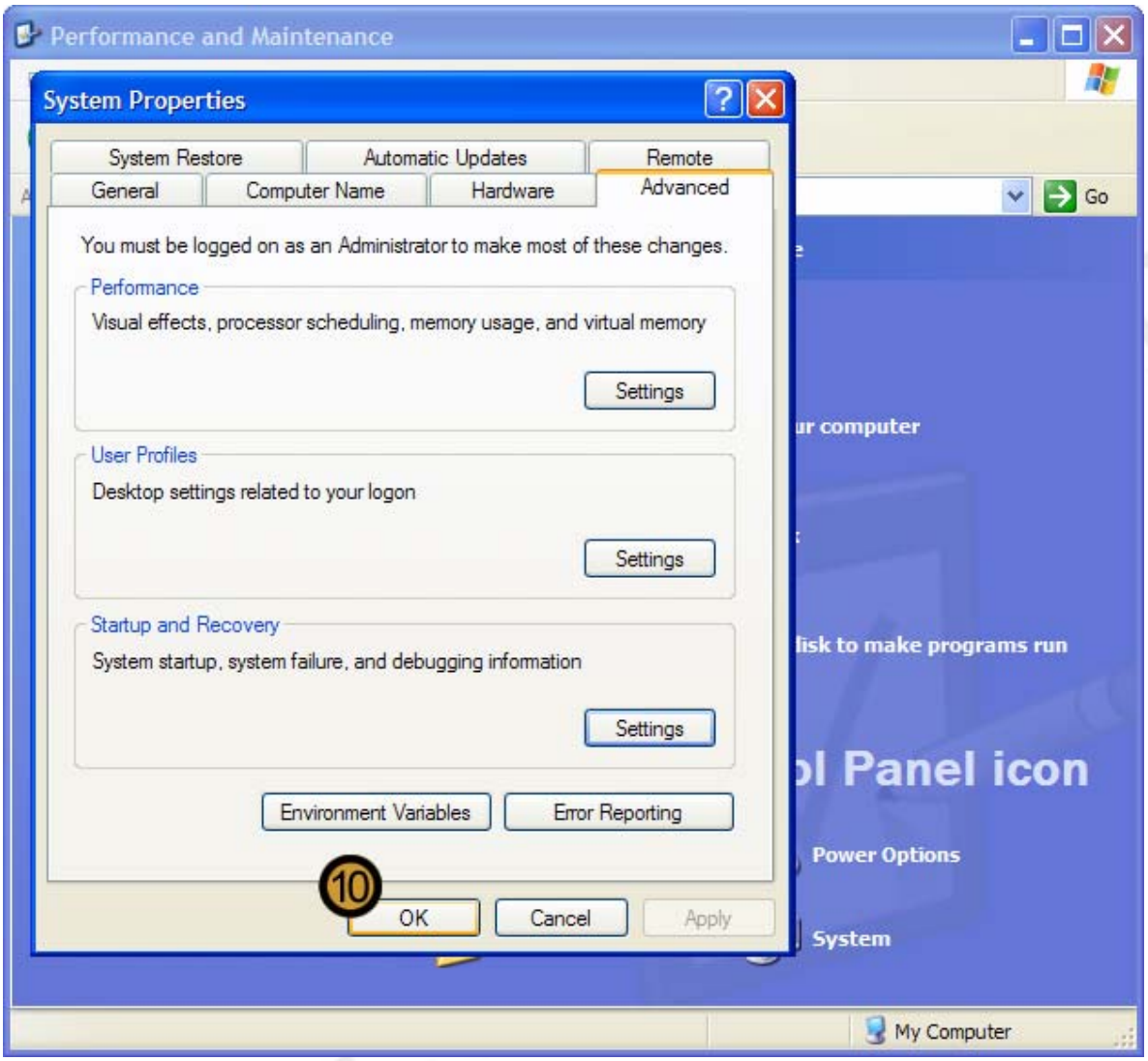
The STARTUP AND RECOVERY dialog box appears

7. In the STARTUP AND RECOVERY dialog box, click **DEFAULT OPERATING SYSTEM** drop down list and select the operating system that you want to set as the default operating system for the local computer.

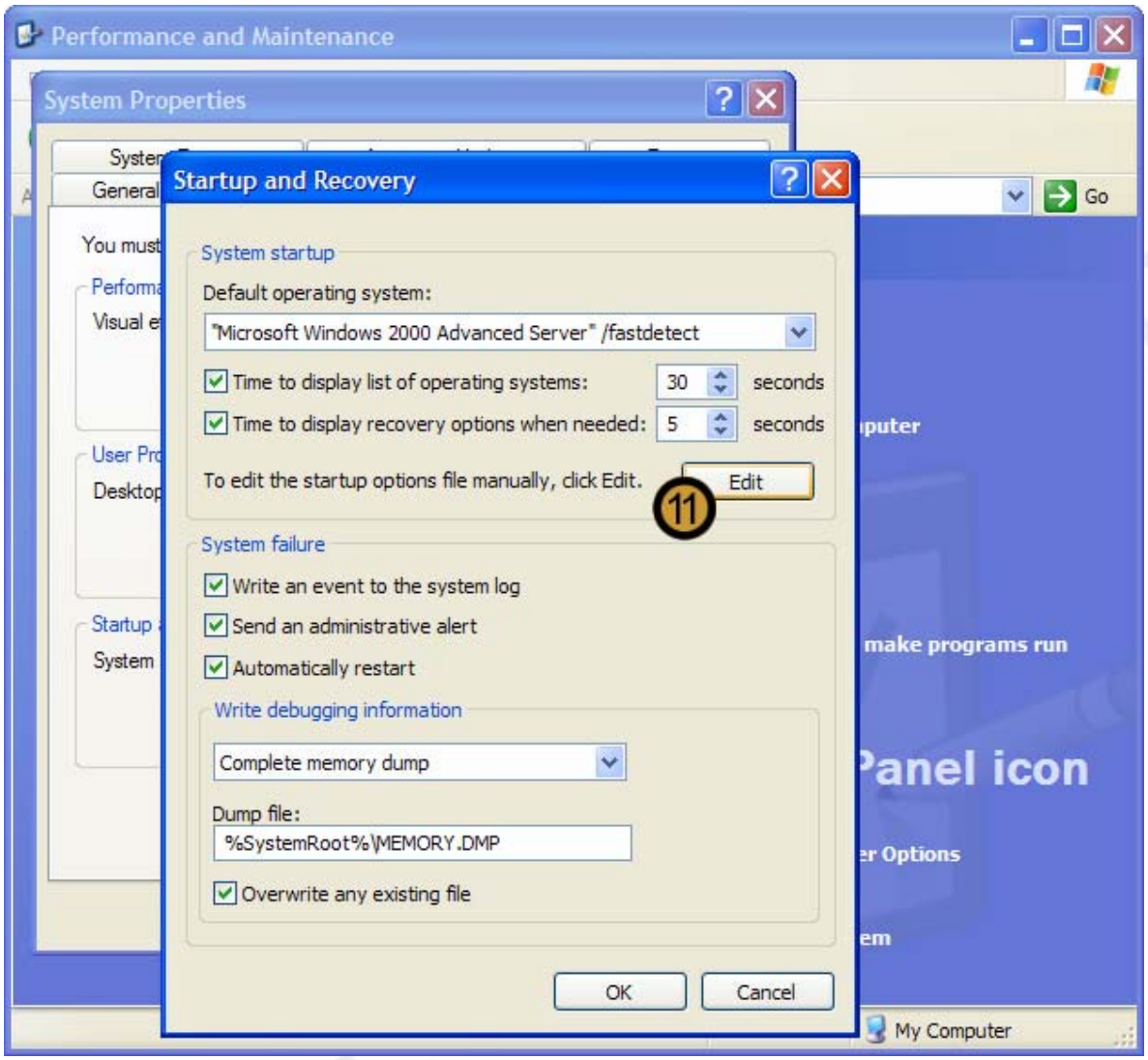


8. Set the **TIME TO DISPLAY LIST OF OPERATING SSYTEMS** option

9. Click **OK**

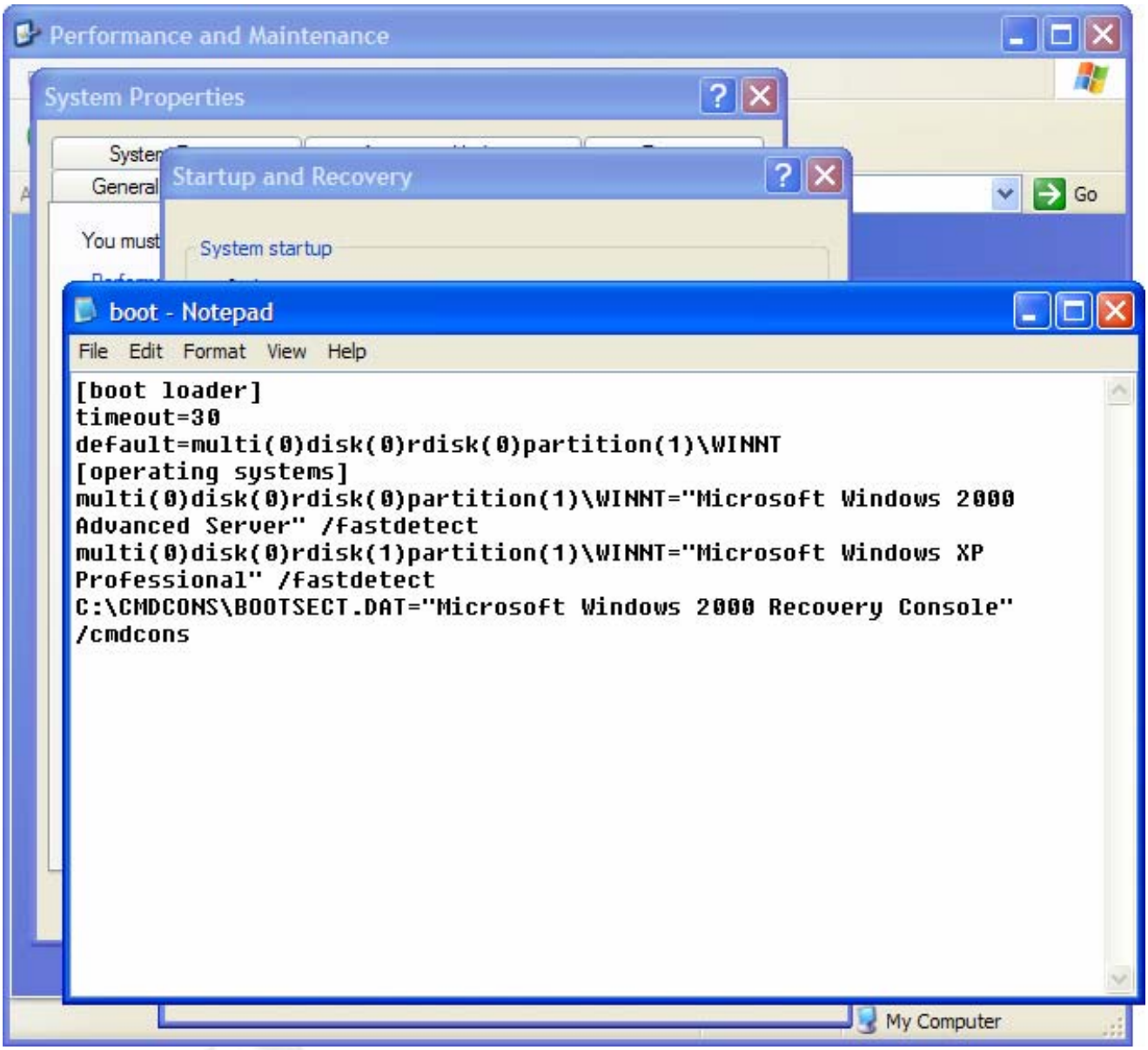


10. Close the SYSTEM PROPERTIES dialog box by clicking **OK**



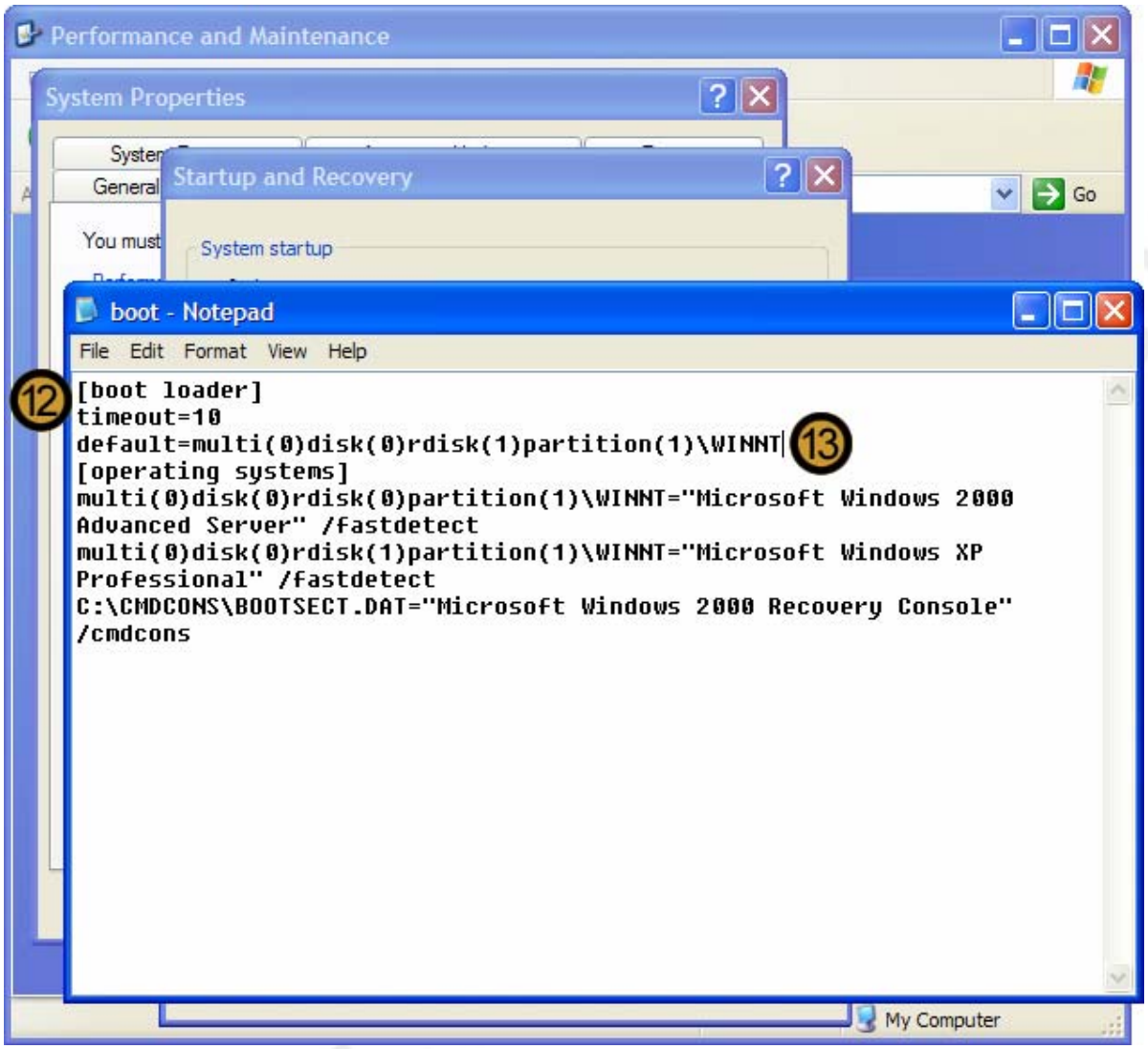
Alternatively, you could alter the dual boot options by manually editing the *boot.ini* file. To manually alter the options:

11. On the STARTUP AND RECOVERY dialog box, under the SYSTEM STARTUP section, click **EDIT**



Windows XP Professional opens the *boot.ini* file in Notepad

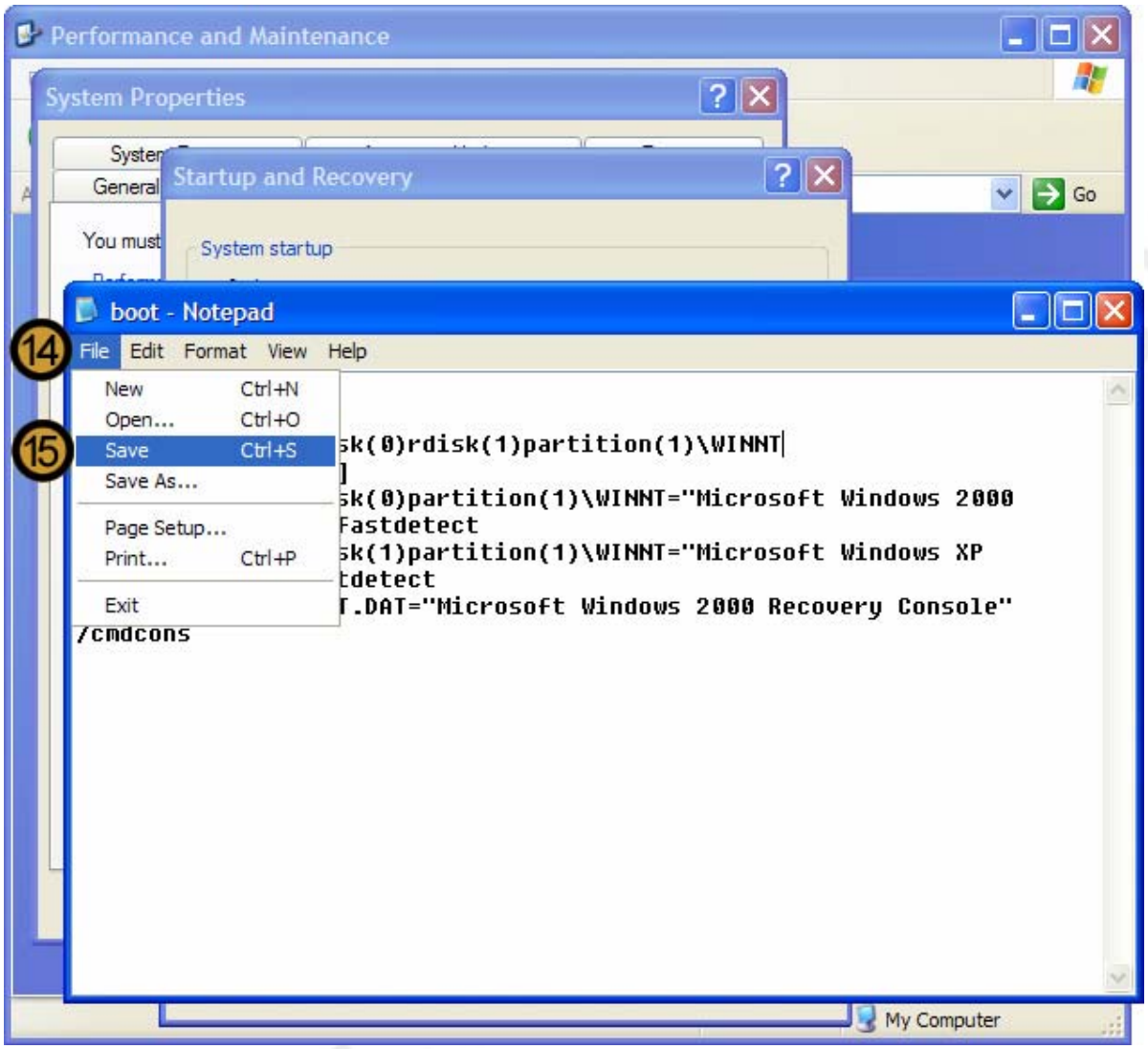
Note: The current default operating system is located by the ARC Path **`multi(0)rdisk(0)partition(1)`**. This is the lowest ARC Path and points the primary or system partition on the primary master hard drive.



12. In the **[boot loader]** section, set the **TIME TO DISPLAY LIST OF OPERATING SSYTEMS** option

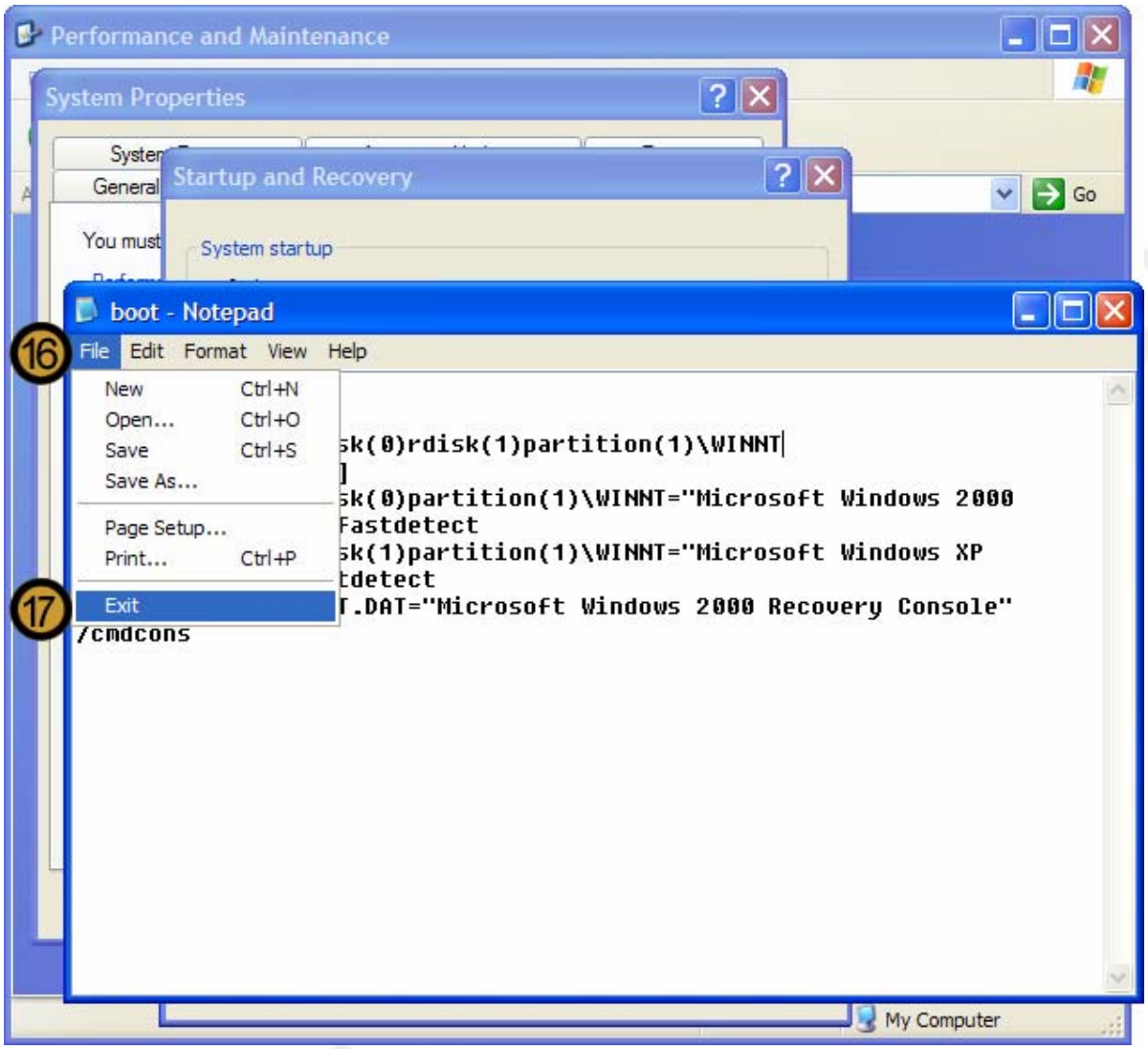
13. Set the correct ARC path to the operating system that you want to set as the default operating system on the local computer.

> **Note:** The new ARC Path: **`multi(0)rdisk(1)partition(1)`** points to the primary partition on the primary slave hard drive which is denoted by **`rdisk(1)`**.



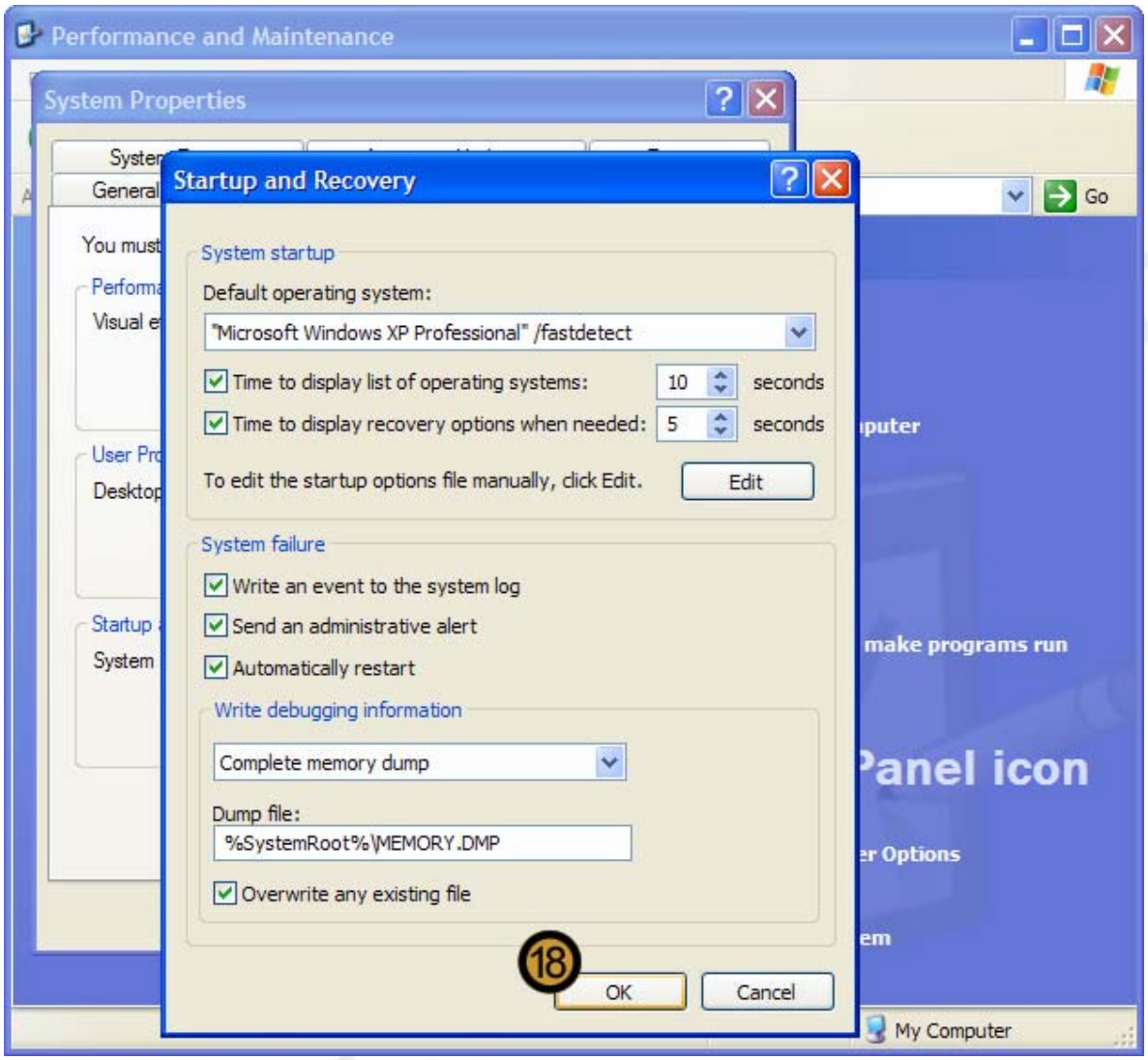
14. Click on the **FILE** menu

15. On the drop down menu, click **SAVE**

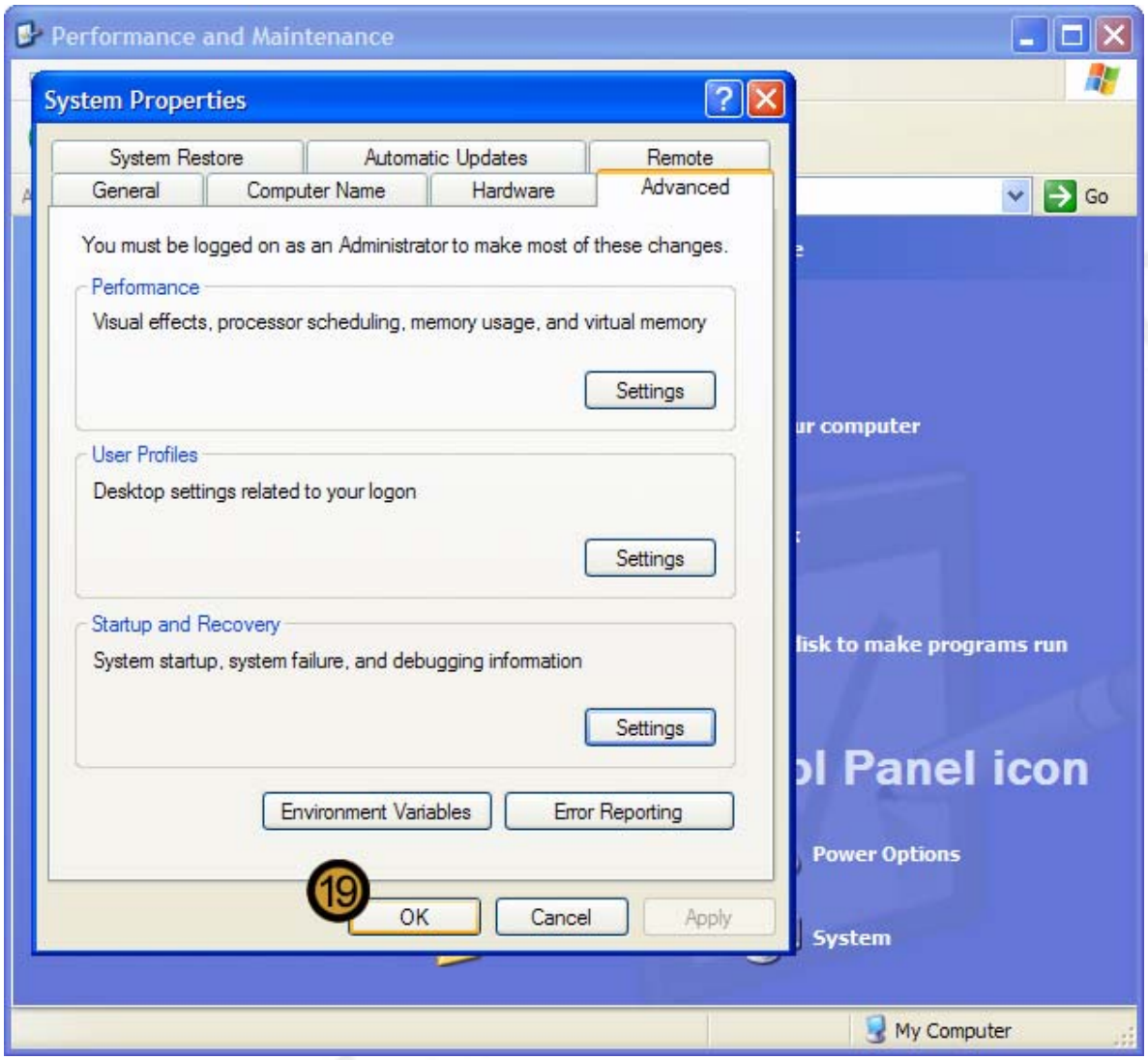


16. Click on the **FILE** menu again

17. Click **EXIT**



18. Close the STARTUP AND RECOVERY dialog box by clicking **OK**

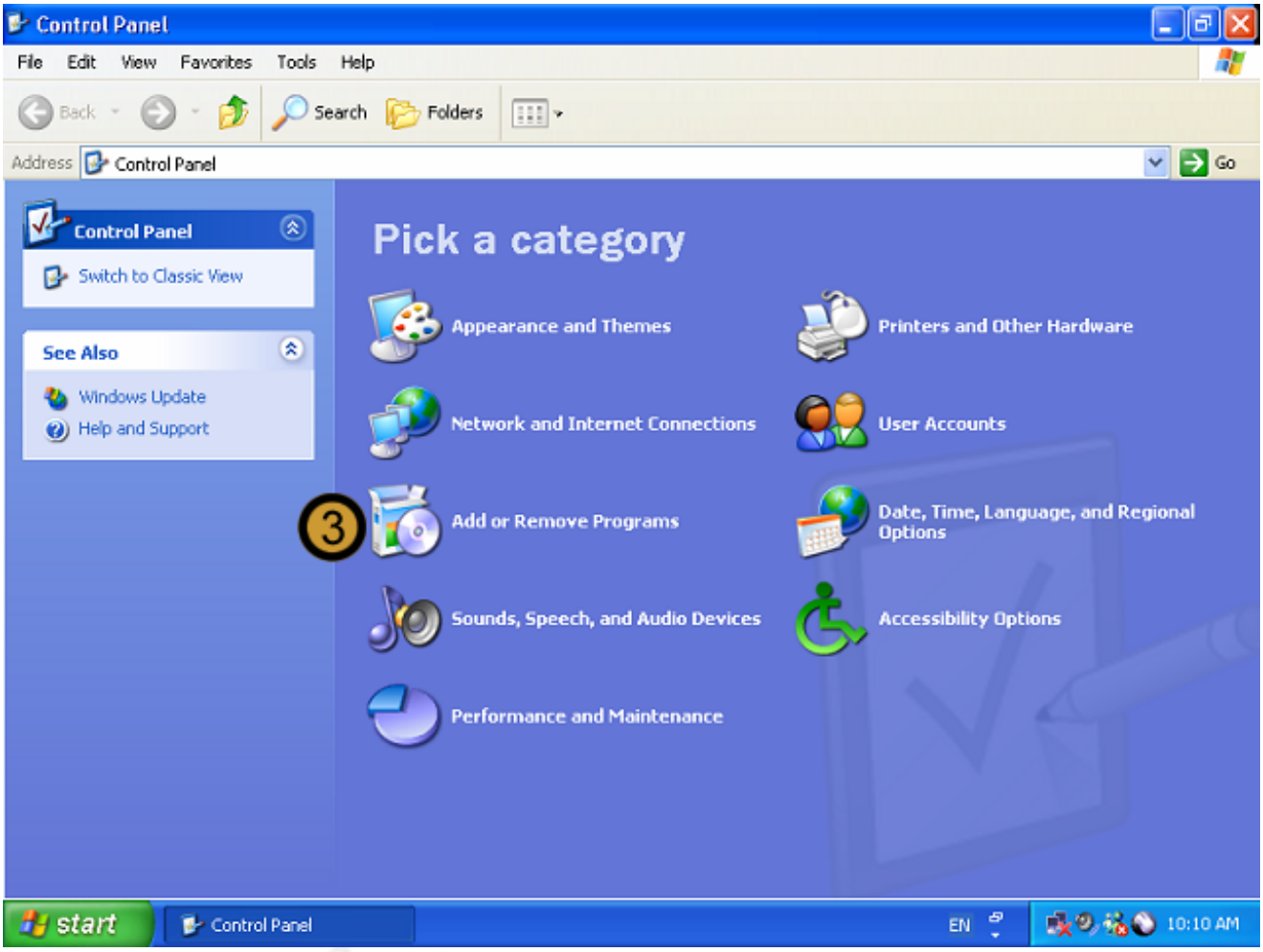


19. Close the STARTUP AND RECOVERY dialog box by clicking **OK**

9.3 Supporting Printing for UNIX clients
9.3.1 Installing Print Services for UNIX

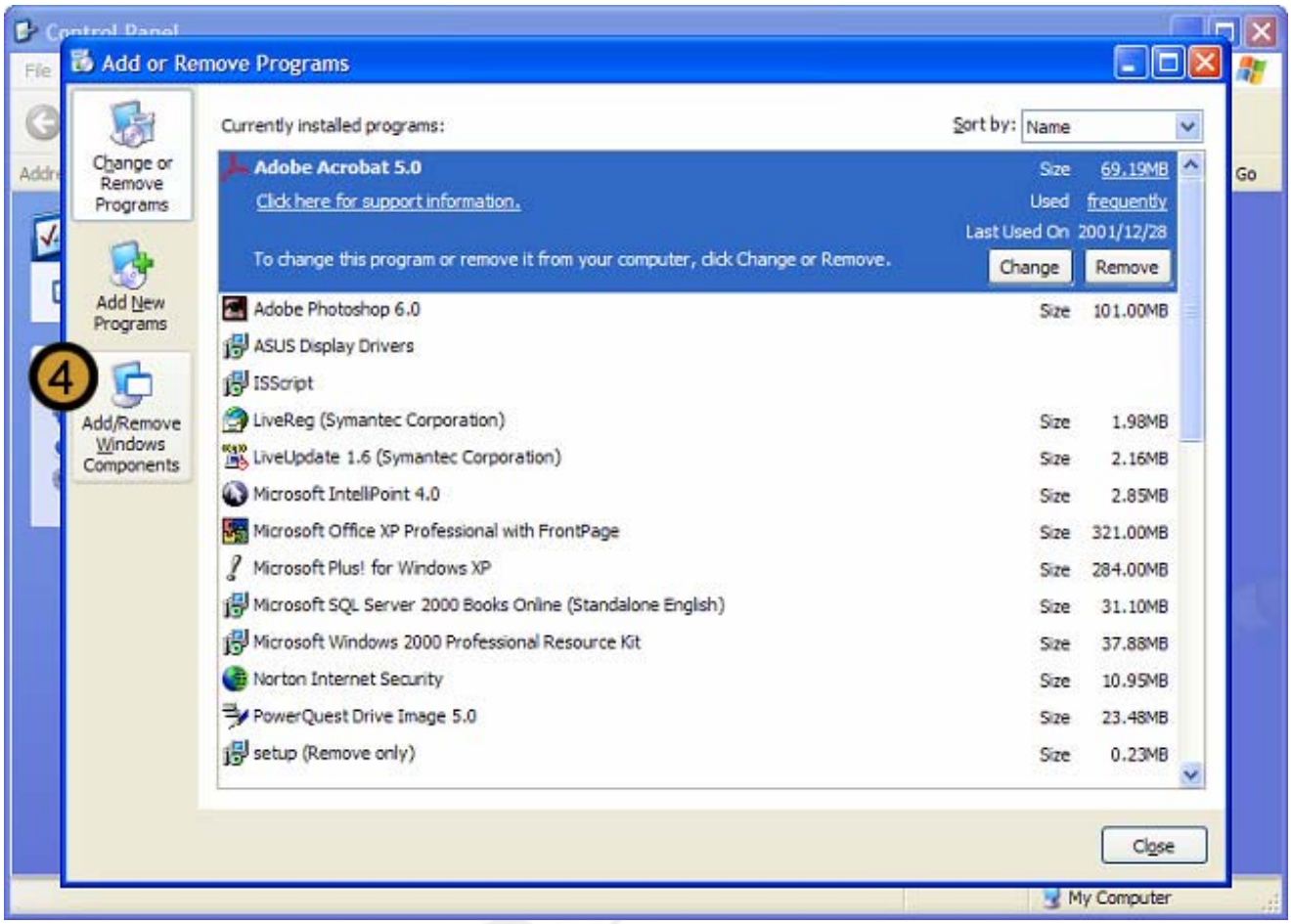
1. Click on the **START** button

2. Click on **CONTROL PANEL**



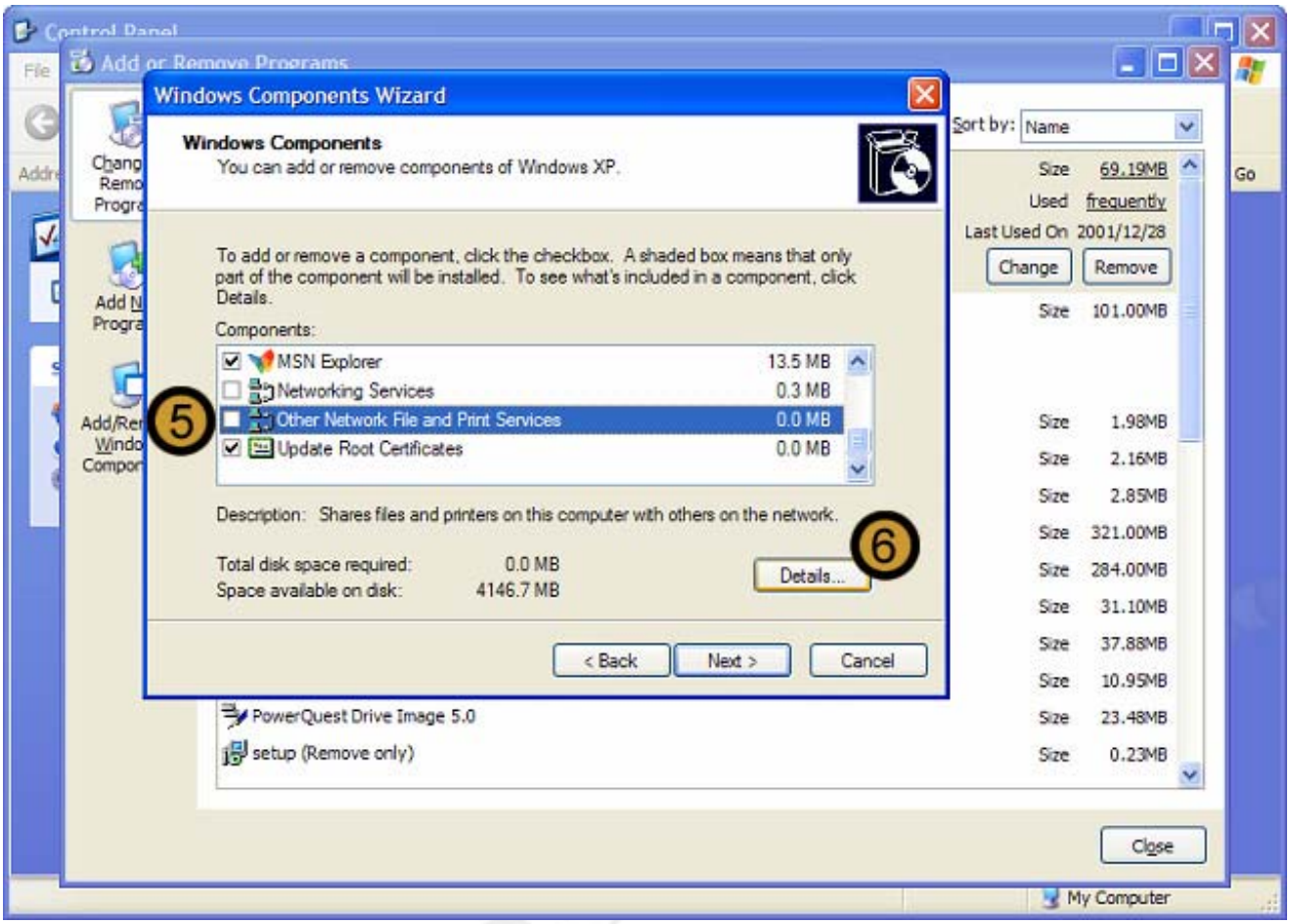
The Control Panel appears

3. In the CONTROL PANEL, click on the **ADD OR REMOVE PROGRAMS** icon



The ADD OR REMOVE PROGRAMS dialog box appears

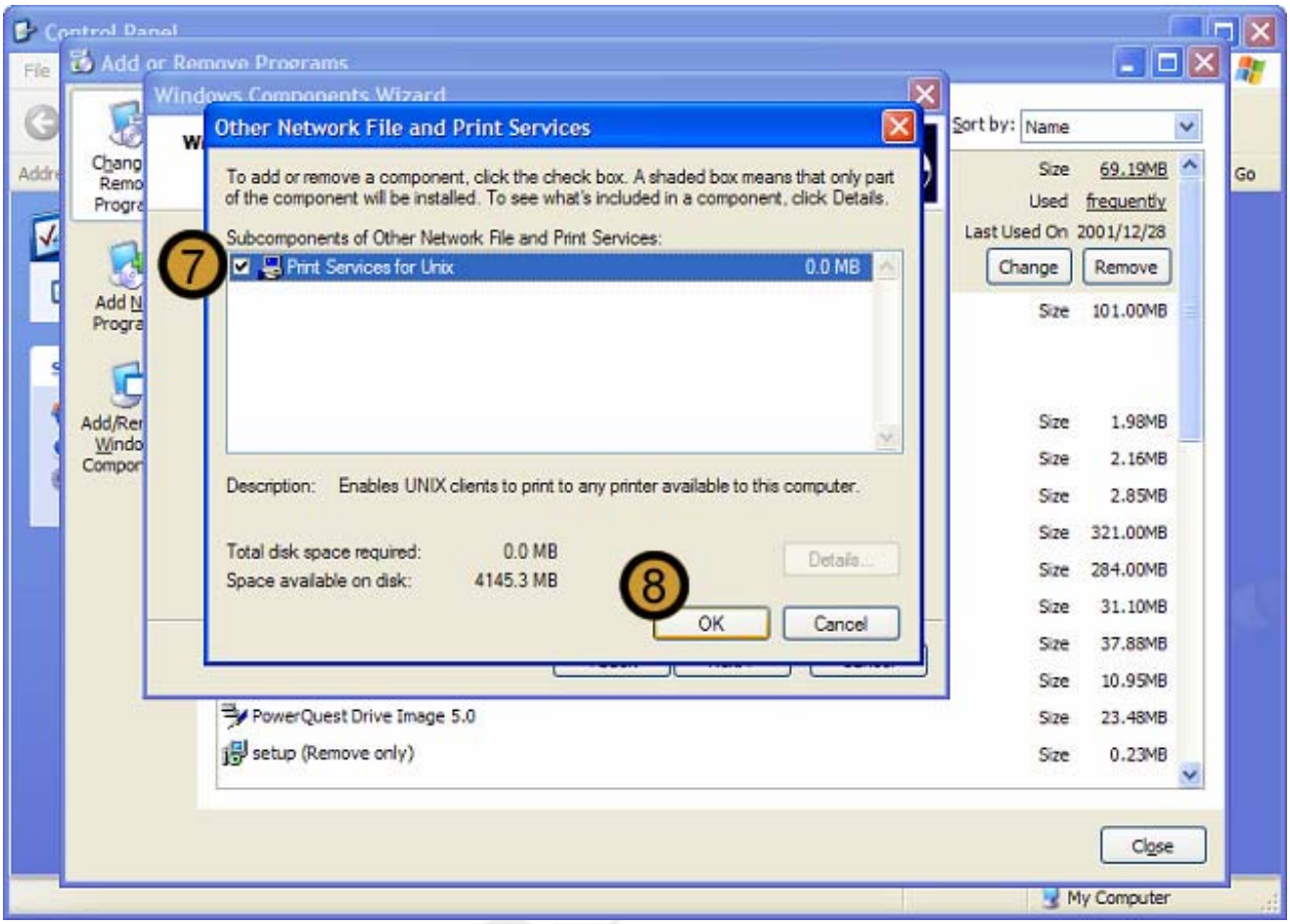
4. In the ADD OR REMOVE PROGRAMS dialog box, click **ADD/REMOVE WINDOWS COMPONENTS**



The WINDOWS COMPONENTS WIZARD appears

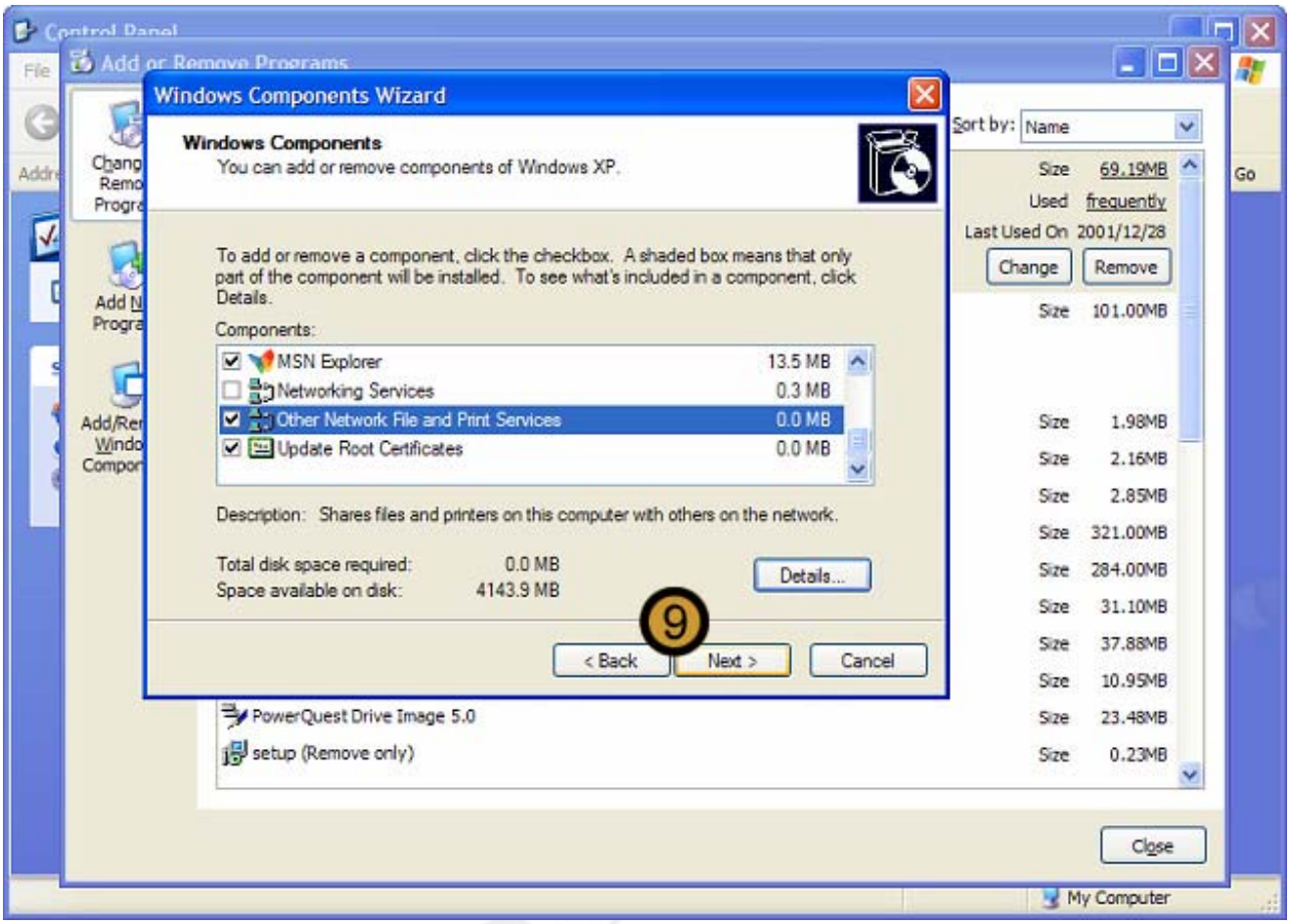
5. In the WINDOWS COMPONENTS WIZARD, scroll down and click on **OTHER NETWORK FILE AND PRINT SERVICES**

6. Click on **DETAILS**

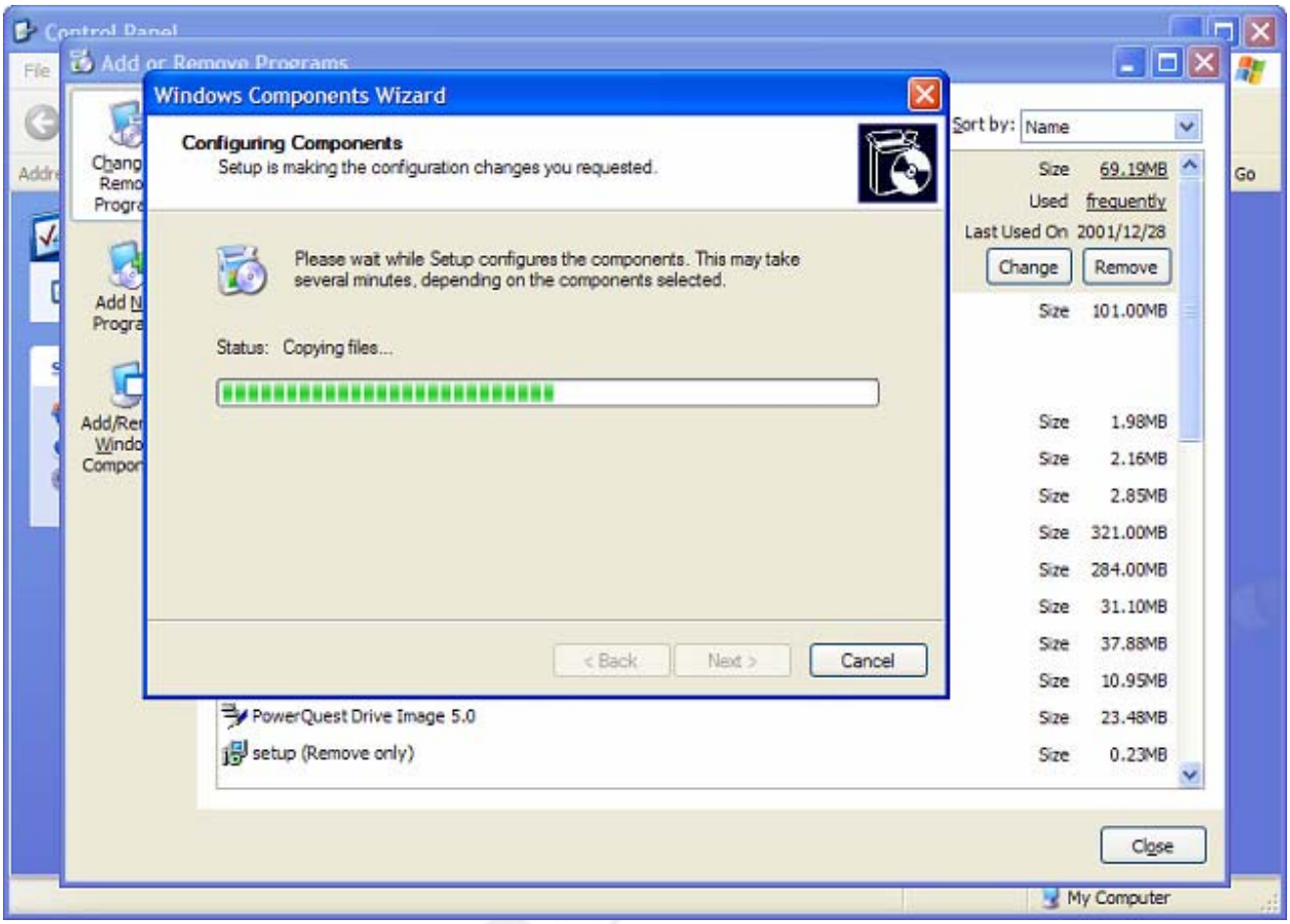


7. Select the **PRINT SERVICES FOR UNIX** check box

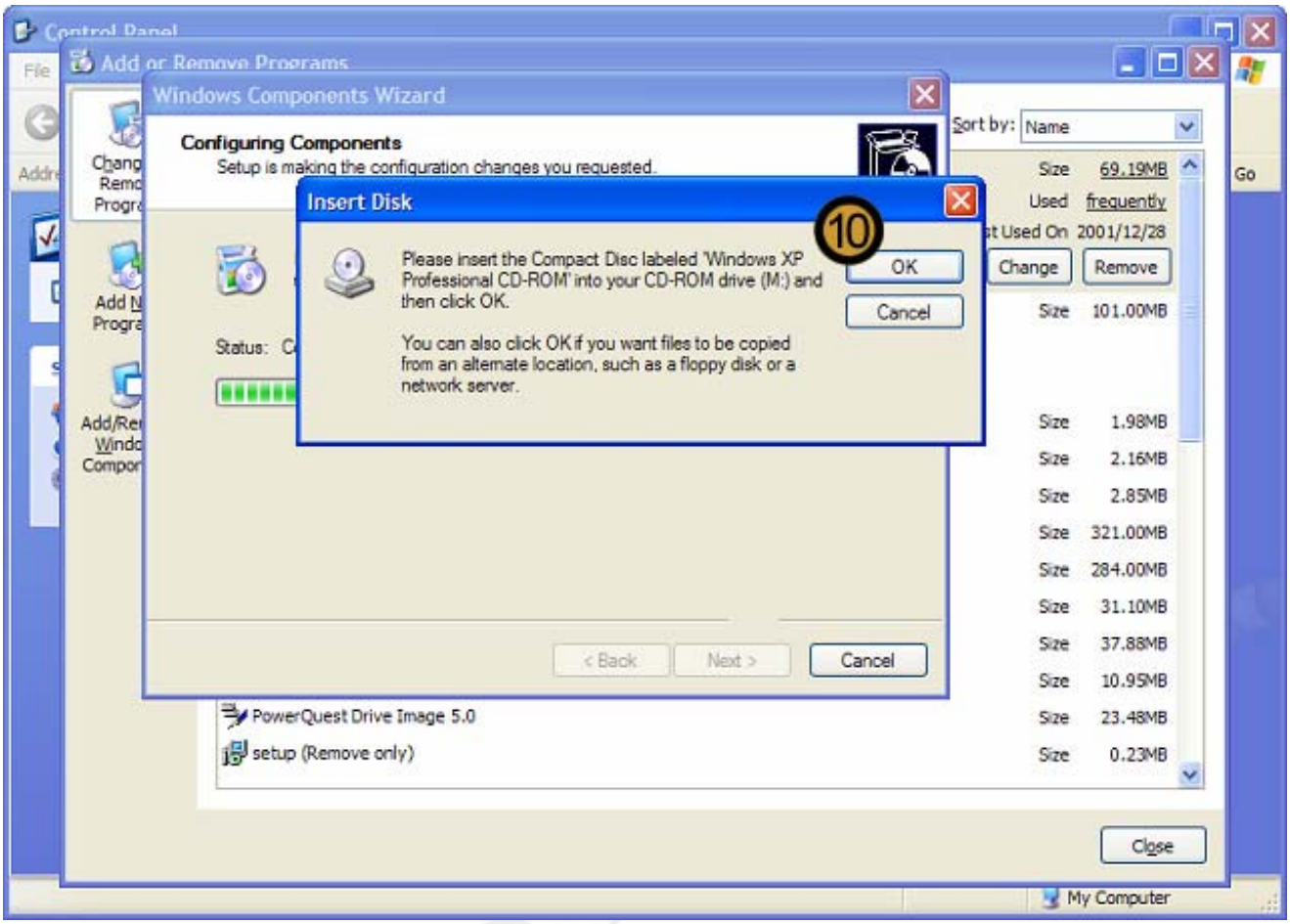
8. Click **OK**


Control Panel
Add or Remove Programs
Windows Components Wizard
Windows Components
You can add or remove components of Windows XP.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
MSN Explorer 13.5 MB
Networking Services 0.3 MB
Other Network File and Print Services 0.0 MB
Update Root Certificates 0.0 MB
Description: Shares files and printers on this computer with others on the network.
Total disk space required: 0.0 MB
Space available on disk: 4143.9 MB
Details...
9
< Back
Next >
Cancel
Sort by: Name
Size 69.19MB
Used frequently
Last Used On 2001/12/28
Change
Remove
Size 101.00MB
Size 1.98MB
Size 2.16MB
Size 2.85MB
Size 321.00MB
Size 284.00MB
Size 31.10MB
Size 37.88MB
Size 10.95MB
PowerQuest Drive Image 5.0
Size 23.48MB
setup (Remove only)
Size 0.23MB
Close
My Computer

9. Click **NEXT**

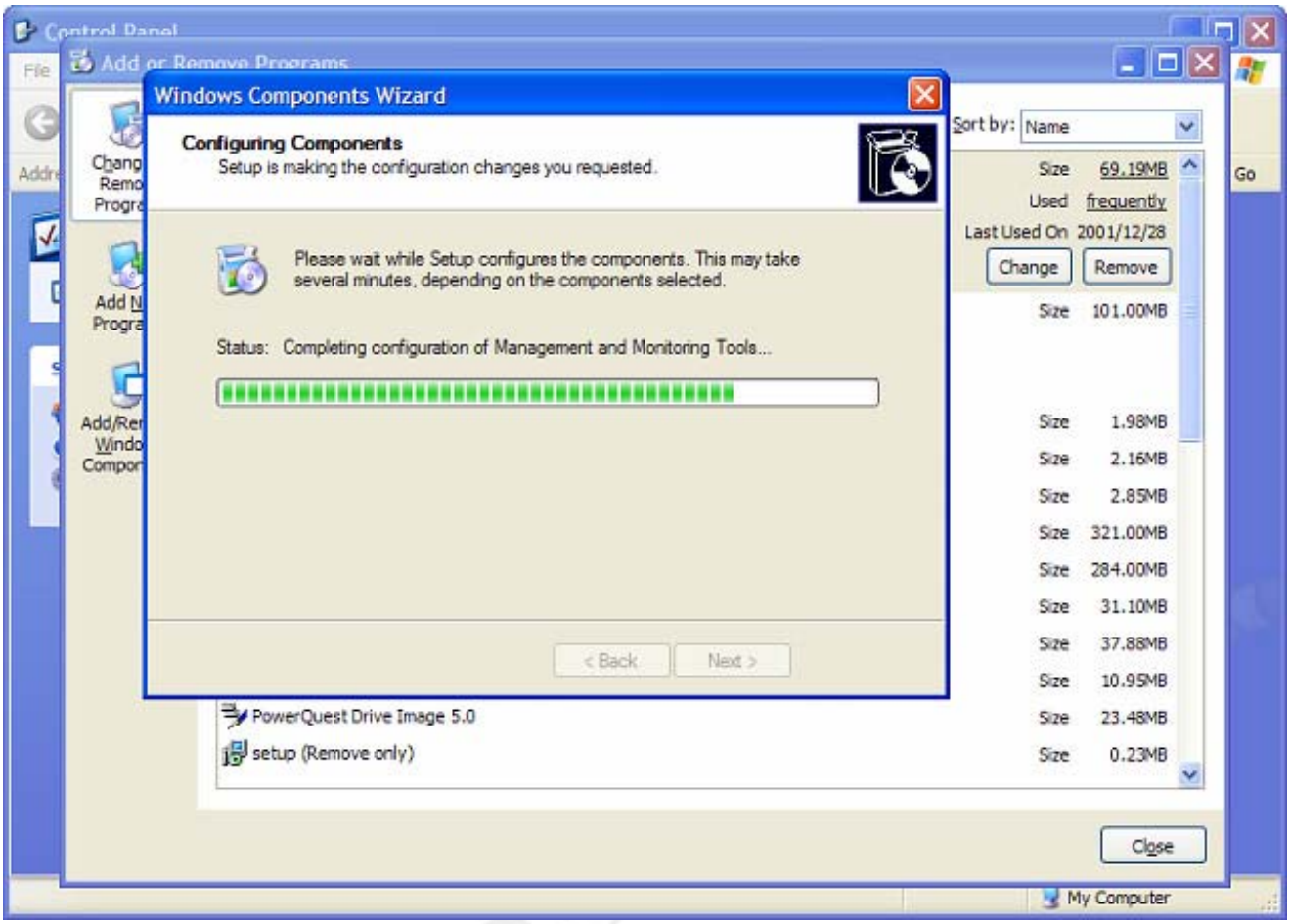


Windows XP Professional begins to install the Print Services for UNIX component



Windows XP Professional requires the Windows XP Professional Installation CD to complete the installation. If the CD is not in the CD-Rom drive, Windows XP Professional prompts you for it.

10. Insert the Windows XP Professional Installation CD in the CD-Rom drive and click **OK**



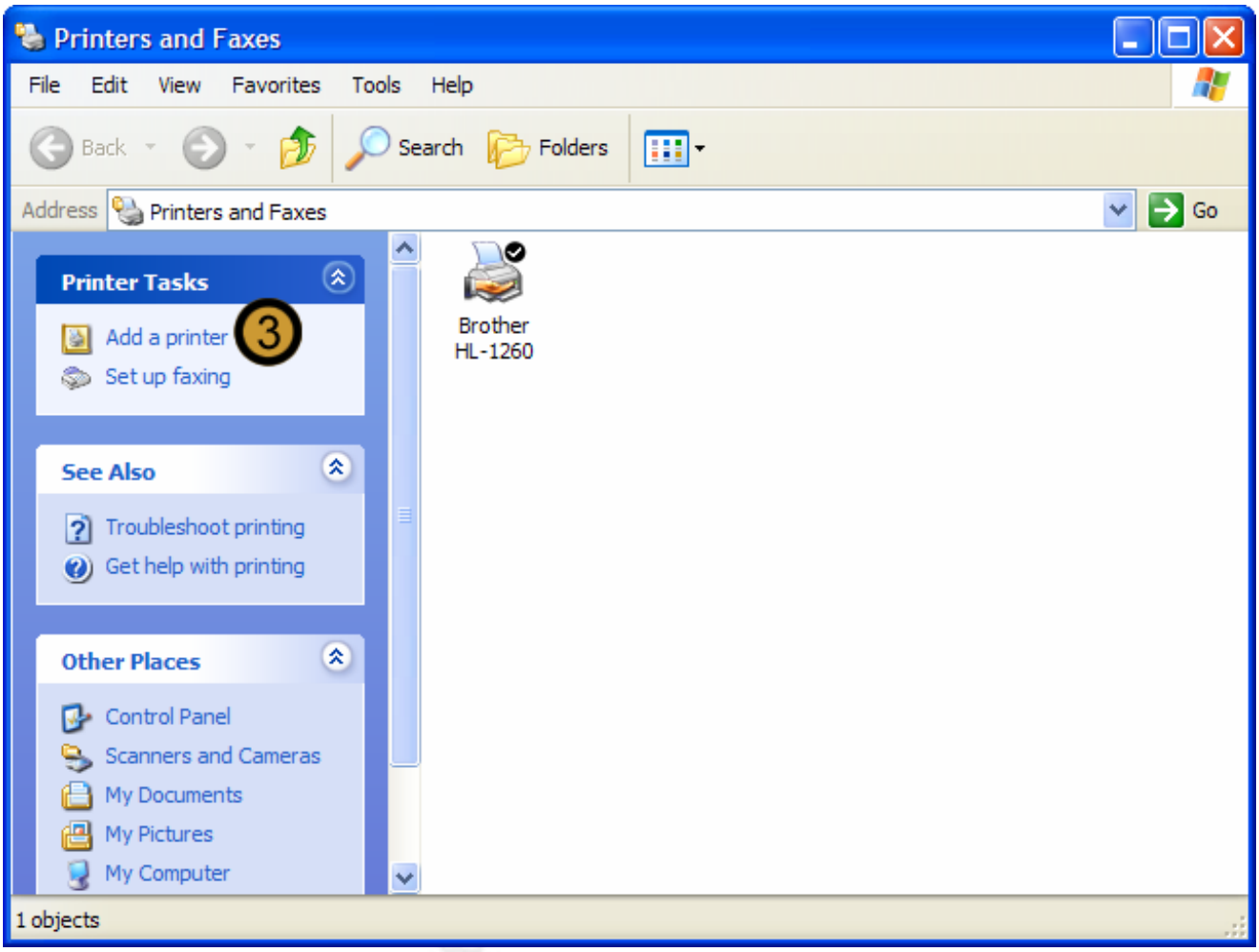
Windows XP Professional continues to install the Print Services for UNIX component

11. To complete the installation of the Print Services for UNIX component, click **FINISH**

9.3.2 Installing a Printer for UNIX clients

1. Click on the **START** button

2. Click on **PRINTERS AND FAXES**

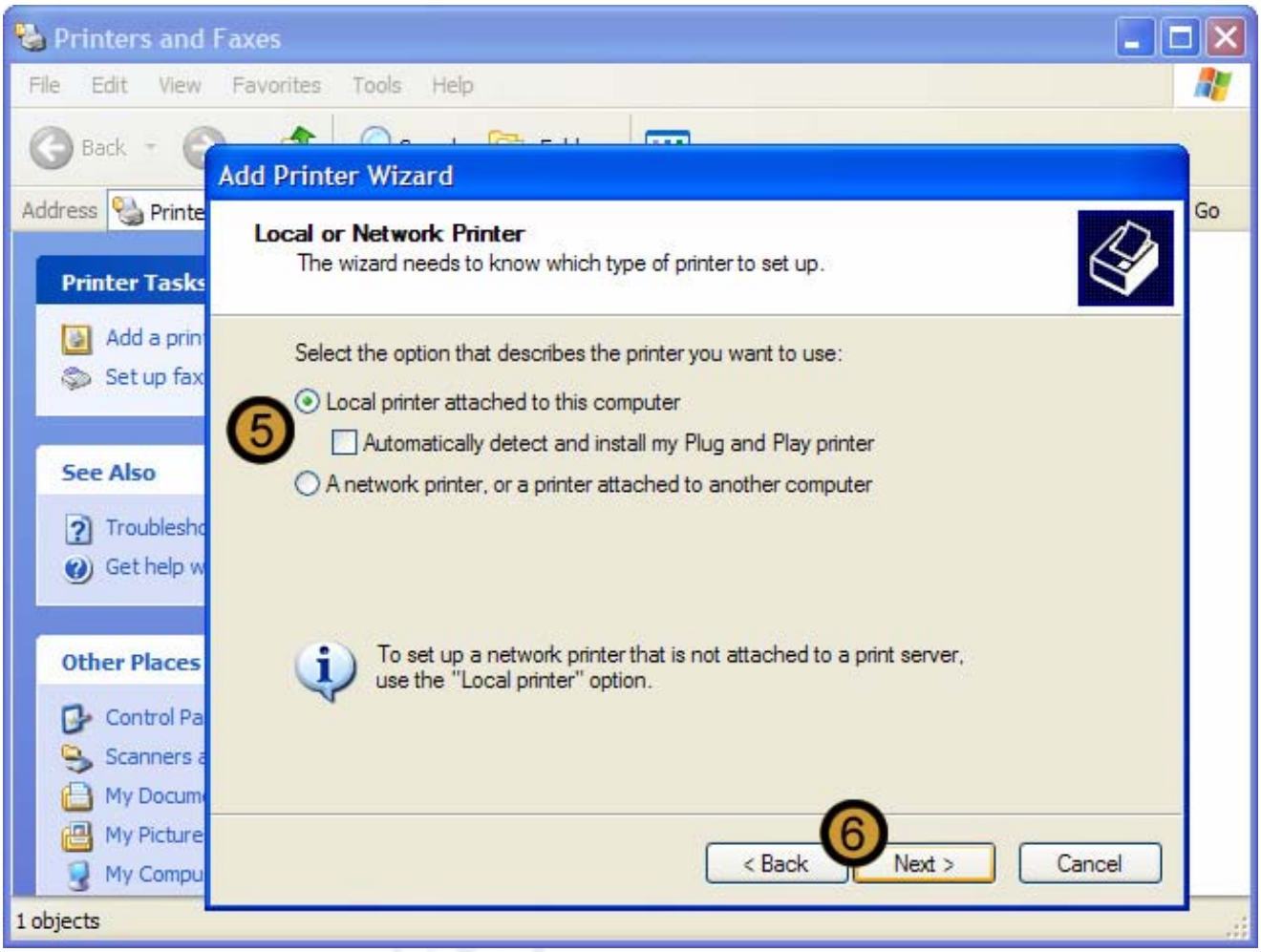


The PRINTERS AND FAXES folder appears

3. In the PRINTERS AND FAXES folder, click **ADD A PRINTER**

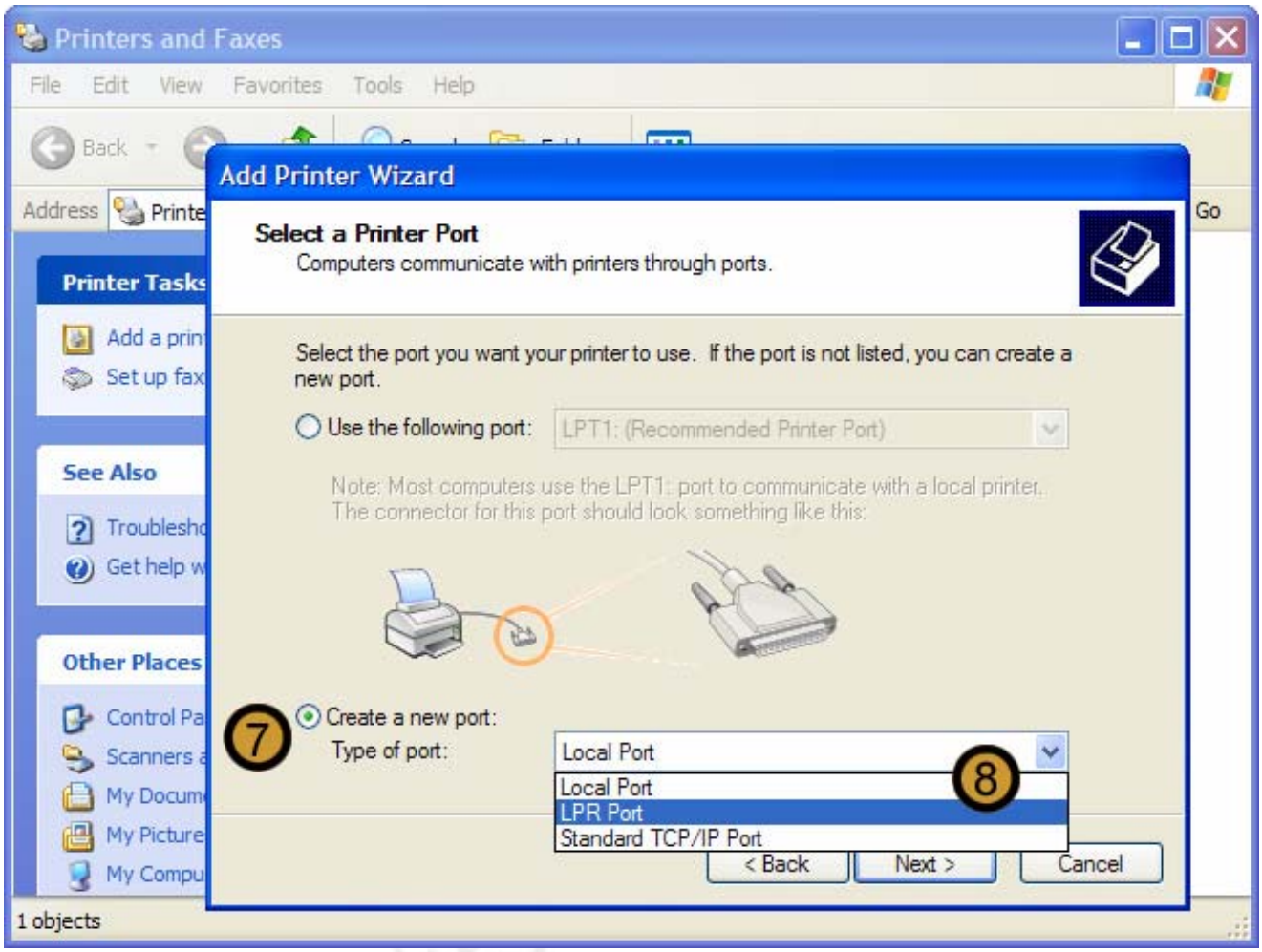
The ADD PRINTER WIZARD appears

4. In the ADD PRINTER WIZARD, click **NEXT** to begin the installation.



5. Clear the **AUTOMATICALLY DETECT AND INSTALL MY PLUG AND PLAY PRINTER** check box

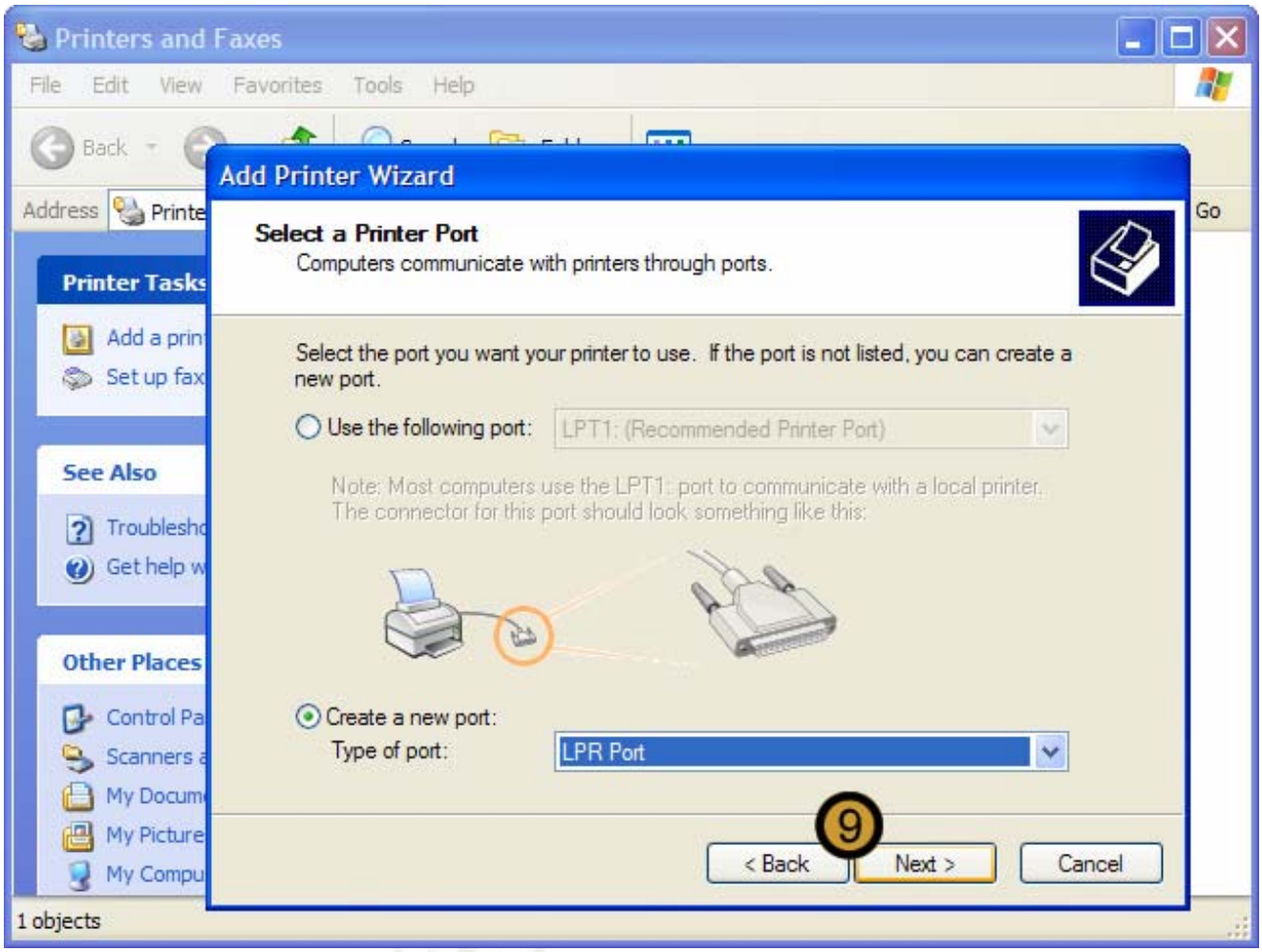
6. Click on **NEXT**



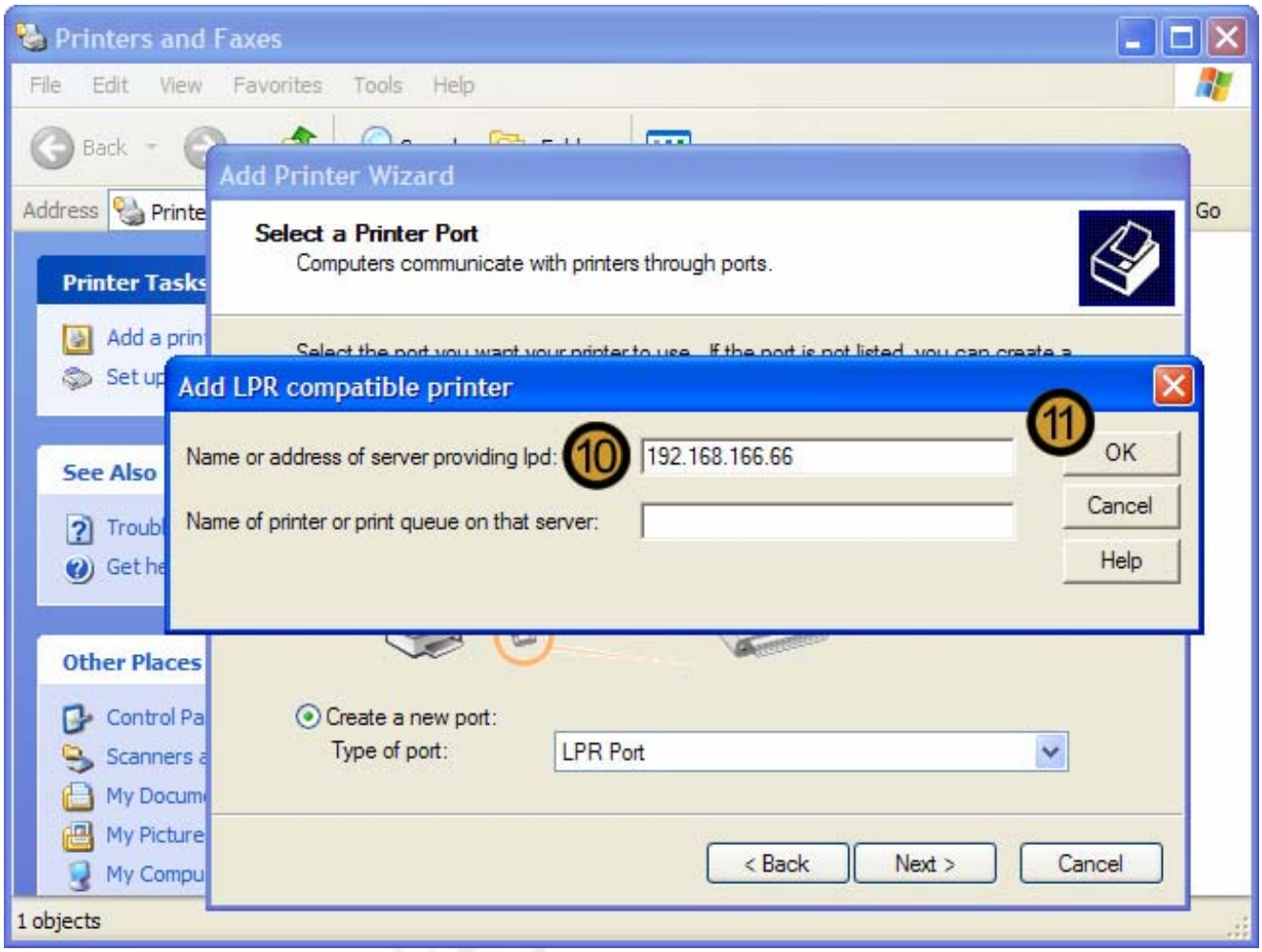
7. Select the **CREATE A NEW PORT** radio button

8. From the **TYPE OF PORT** drop down list, click on **LPR PORT**

Note: The **LPR Port** is only available after you have installed the **Print Services for UNIX** network component.



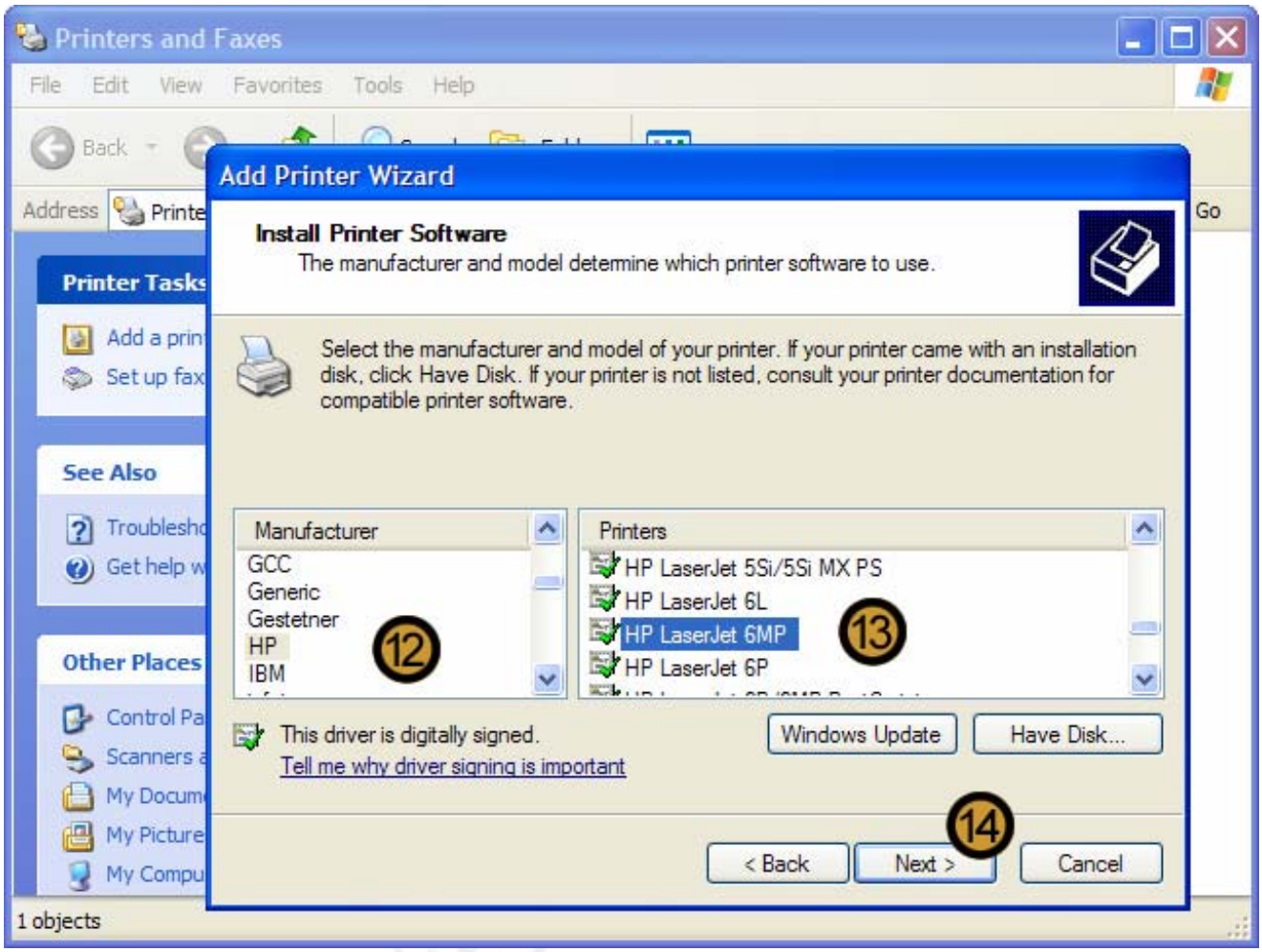
9. Once you have selected the LPR Port, click **NEXT**



The ADD LPR COMPATABLE PRINTER dialog box appears

10. In the ADD LPR COMPATABLE PRINTER dialog box, enter the name or IP address of the computer on which the Print Services for UNIX network component has been installed

11. Click **OK**

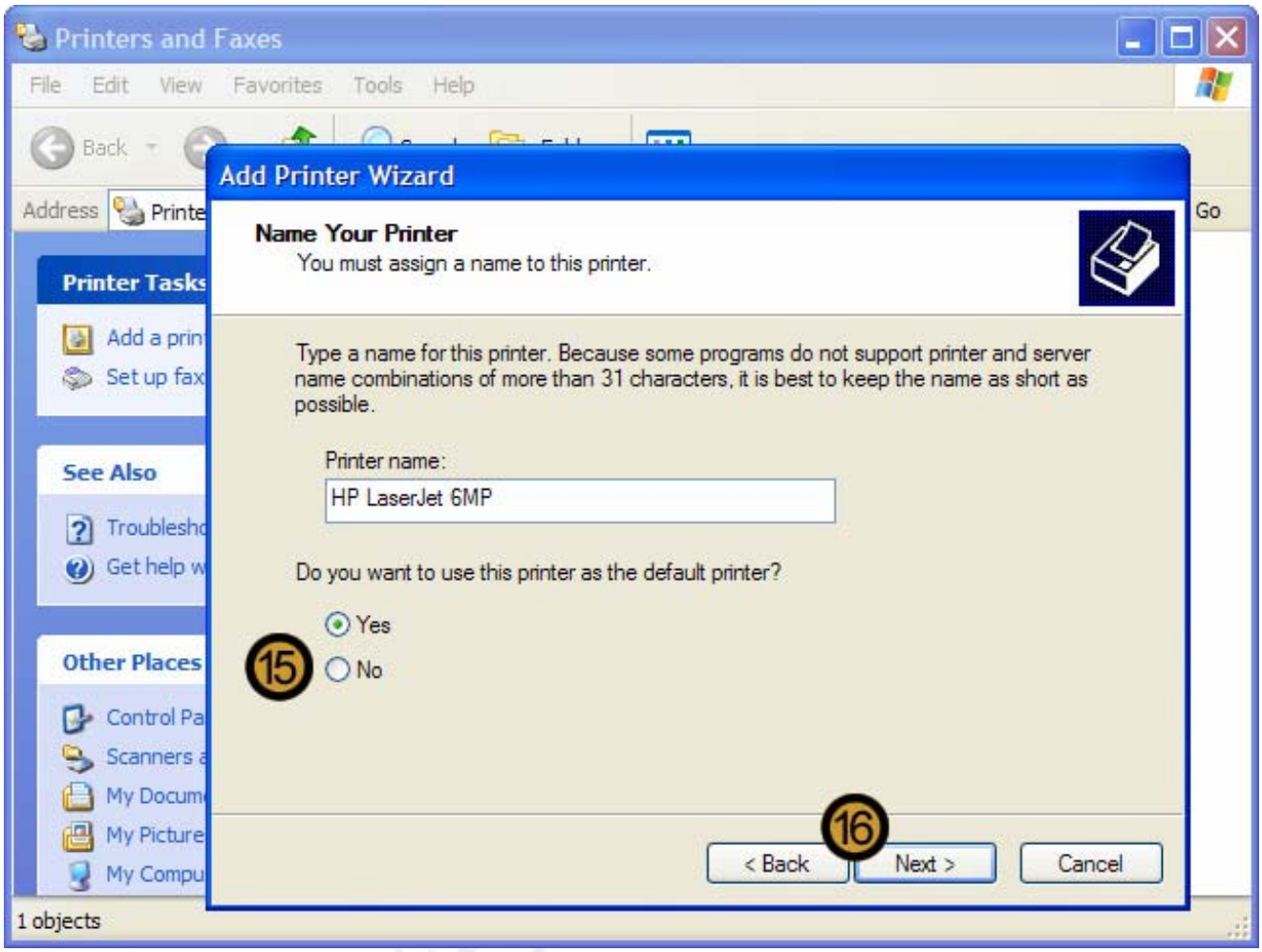


12. Scroll down to, and click on, the **Manufacturer** of the Print Device that you are installing.

13. Scroll down to, and click on, the **Printer Model** that you are installing.

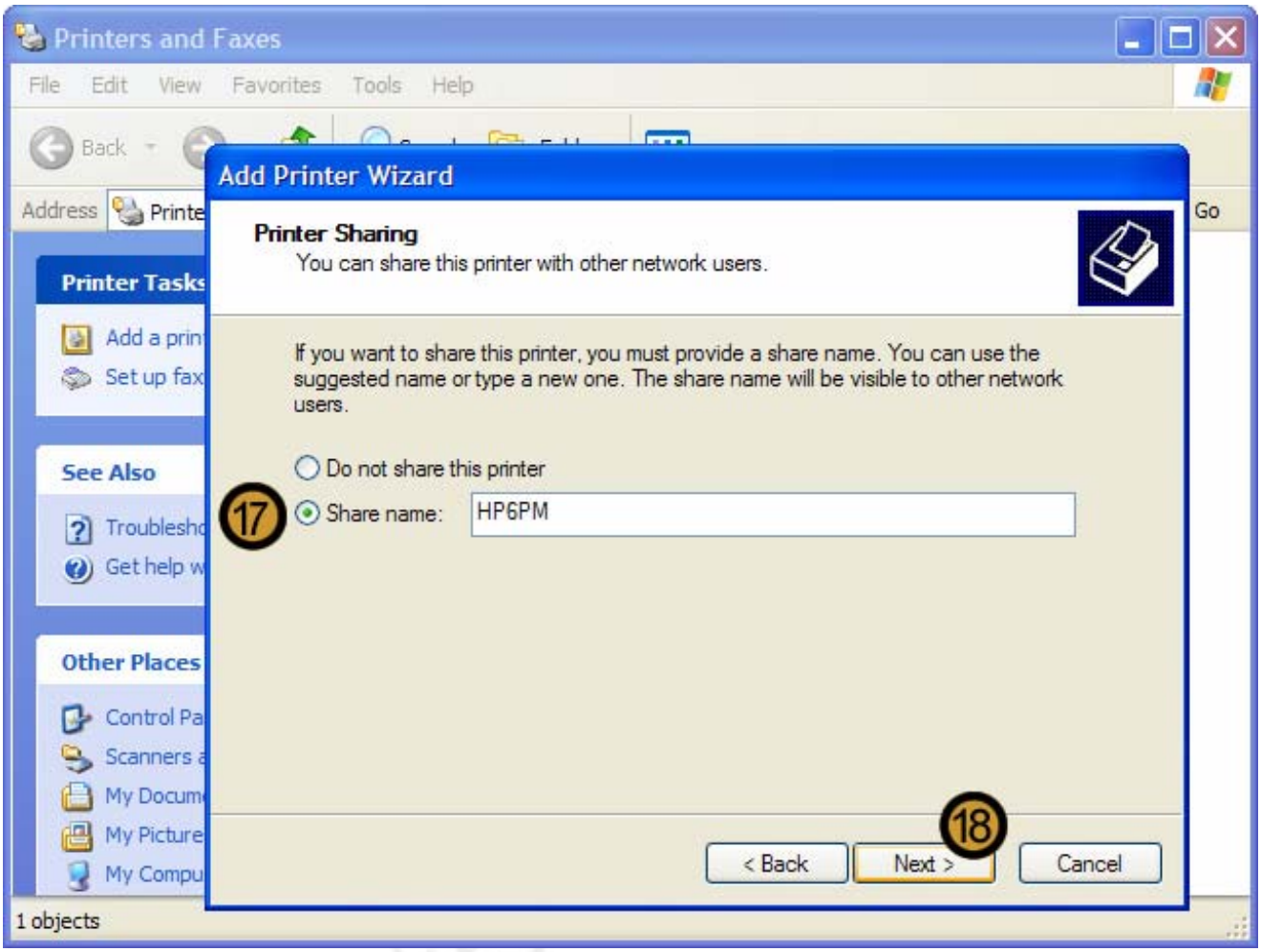
14. Click **NEXT**

If the correct printer model is not listed, you can click **HAVE DISK** to install the drivers that have been supplied with the device. This procedure is performed in section **9.5 Installing new hardware devices**.



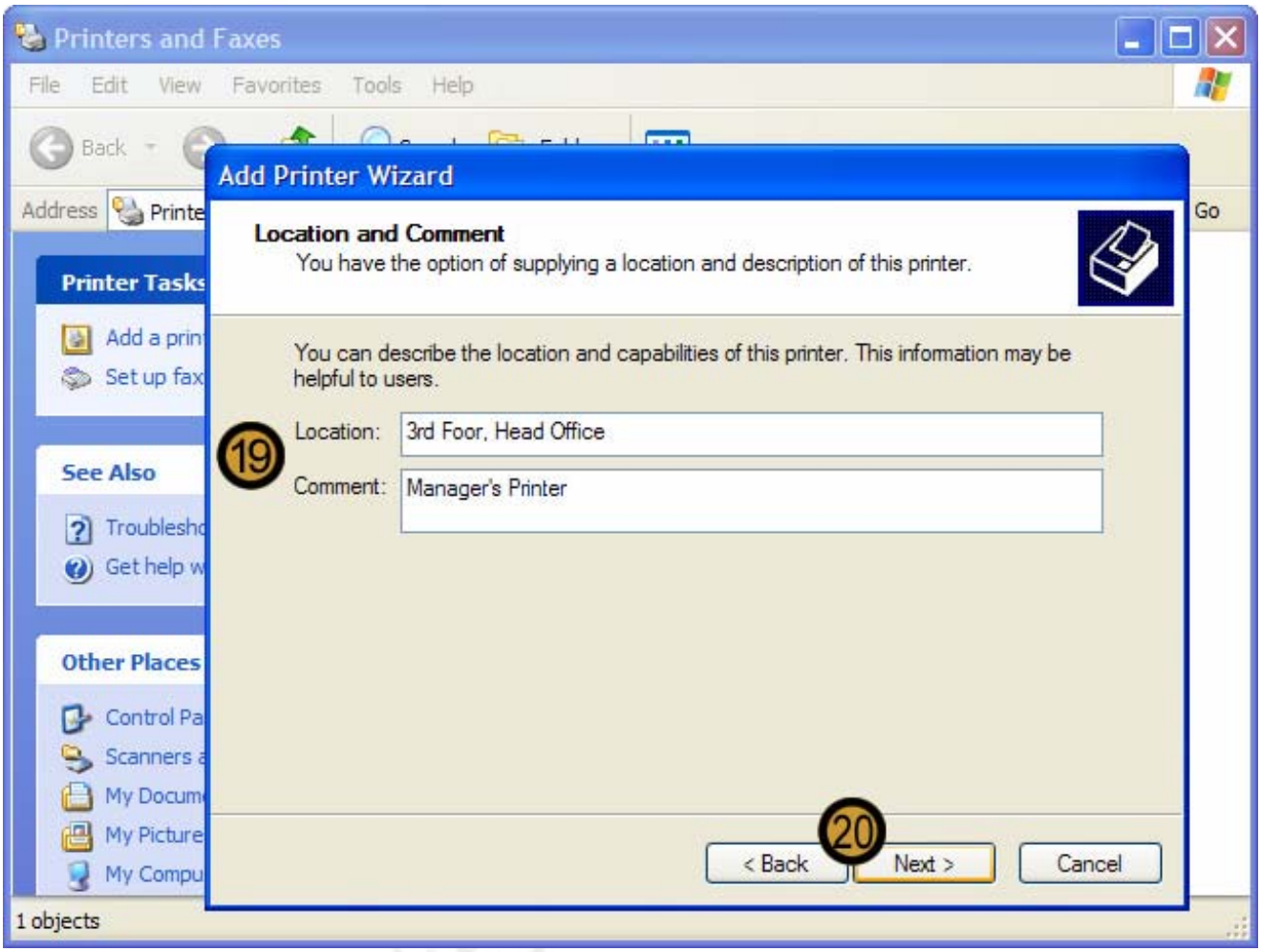
15. If you do not want to set the new printer to be the default printer on the local computer, select the **NO** radio button.

16. Click **NEXT**



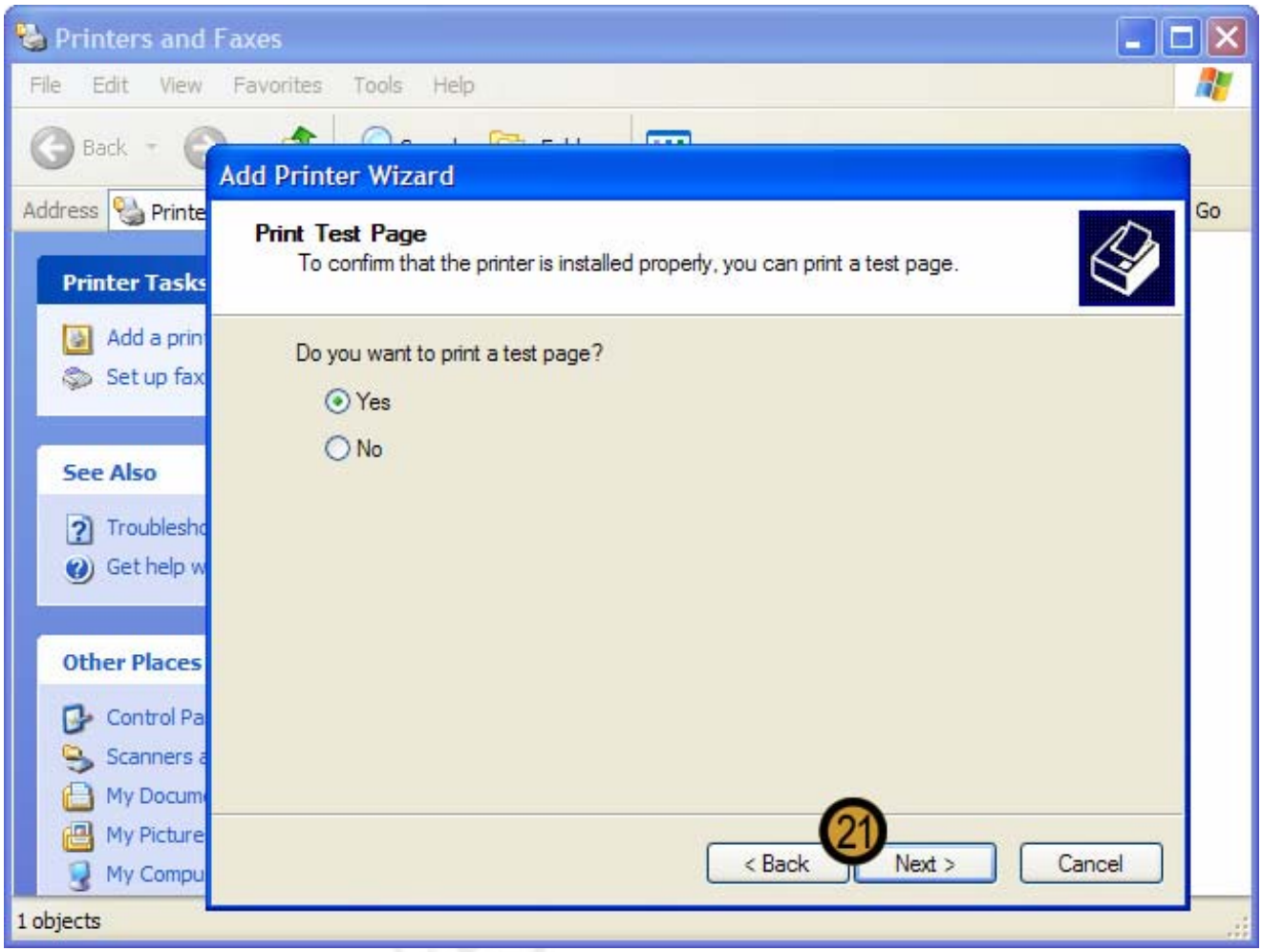
17. Provide a **Share Name** for the new printer

18. Click on **NEXT**

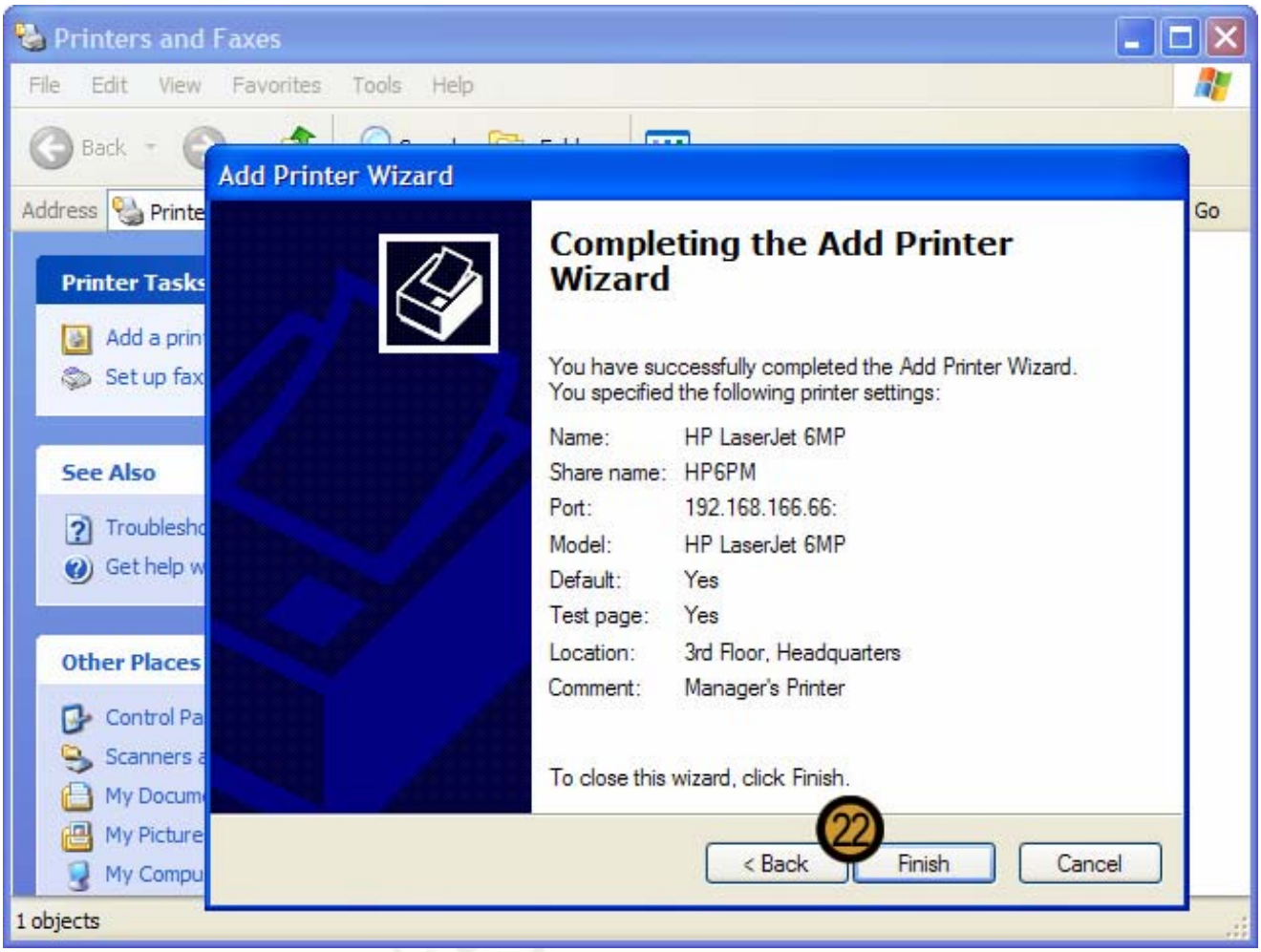


19. Provide required information that will help network users to physically locate the printer so as to know where to locate their printed work. You can also provide a description for the printer.

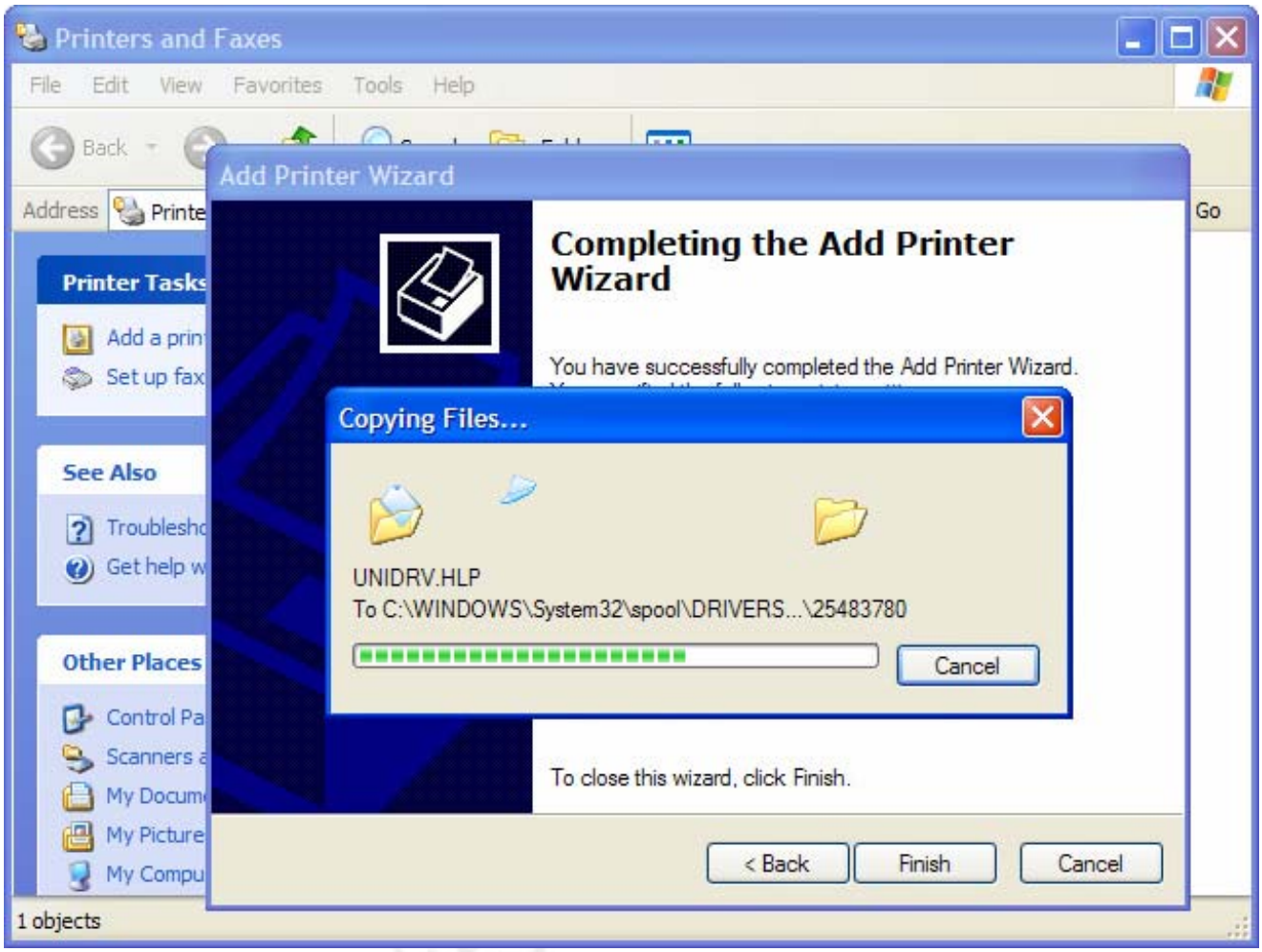
20. Click on **NEXT**



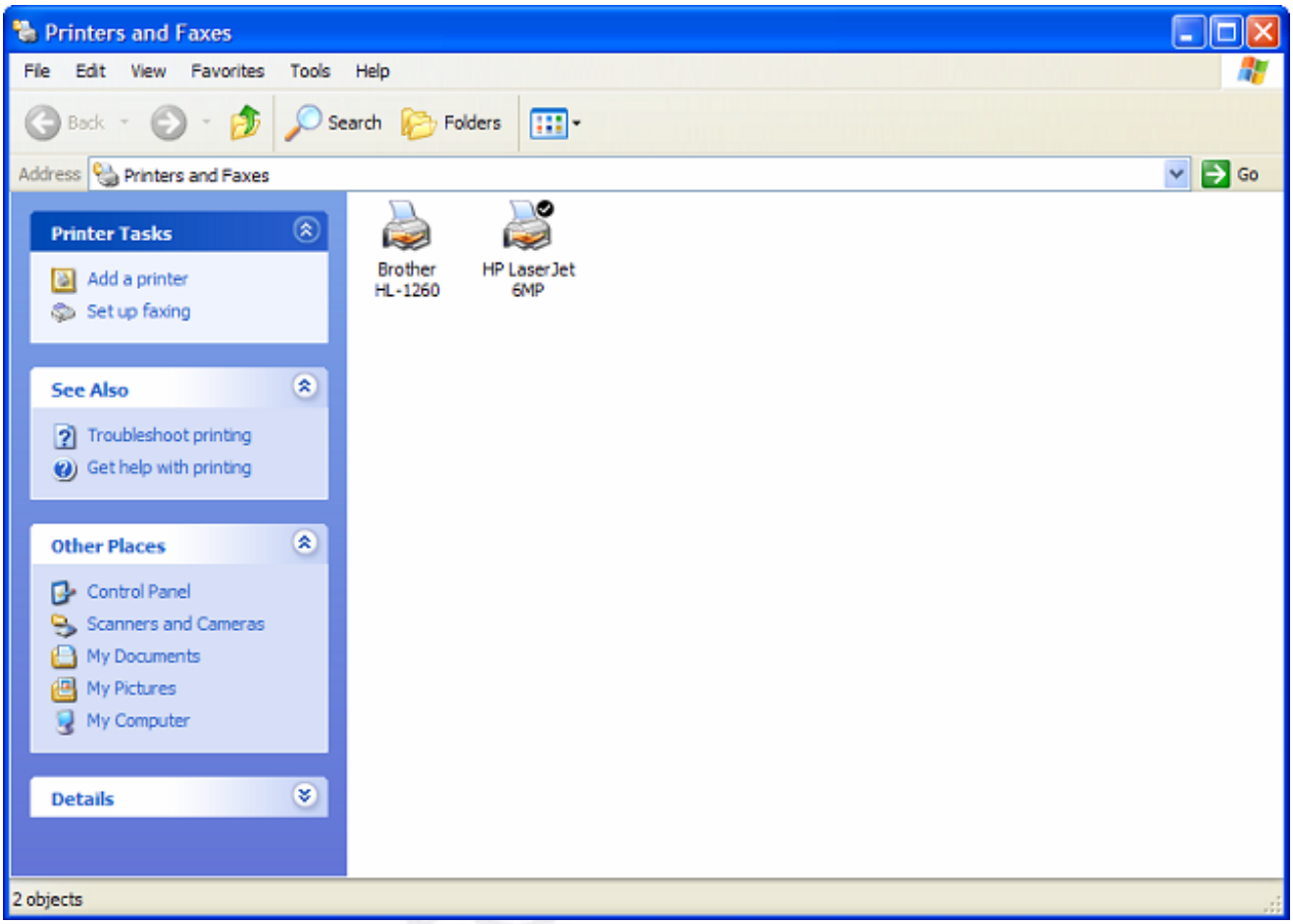
21. Click **NEXT** again



22. Click **FINISH** to complete the installation of the printer



Windows XP Professional installs the required drivers for the print device

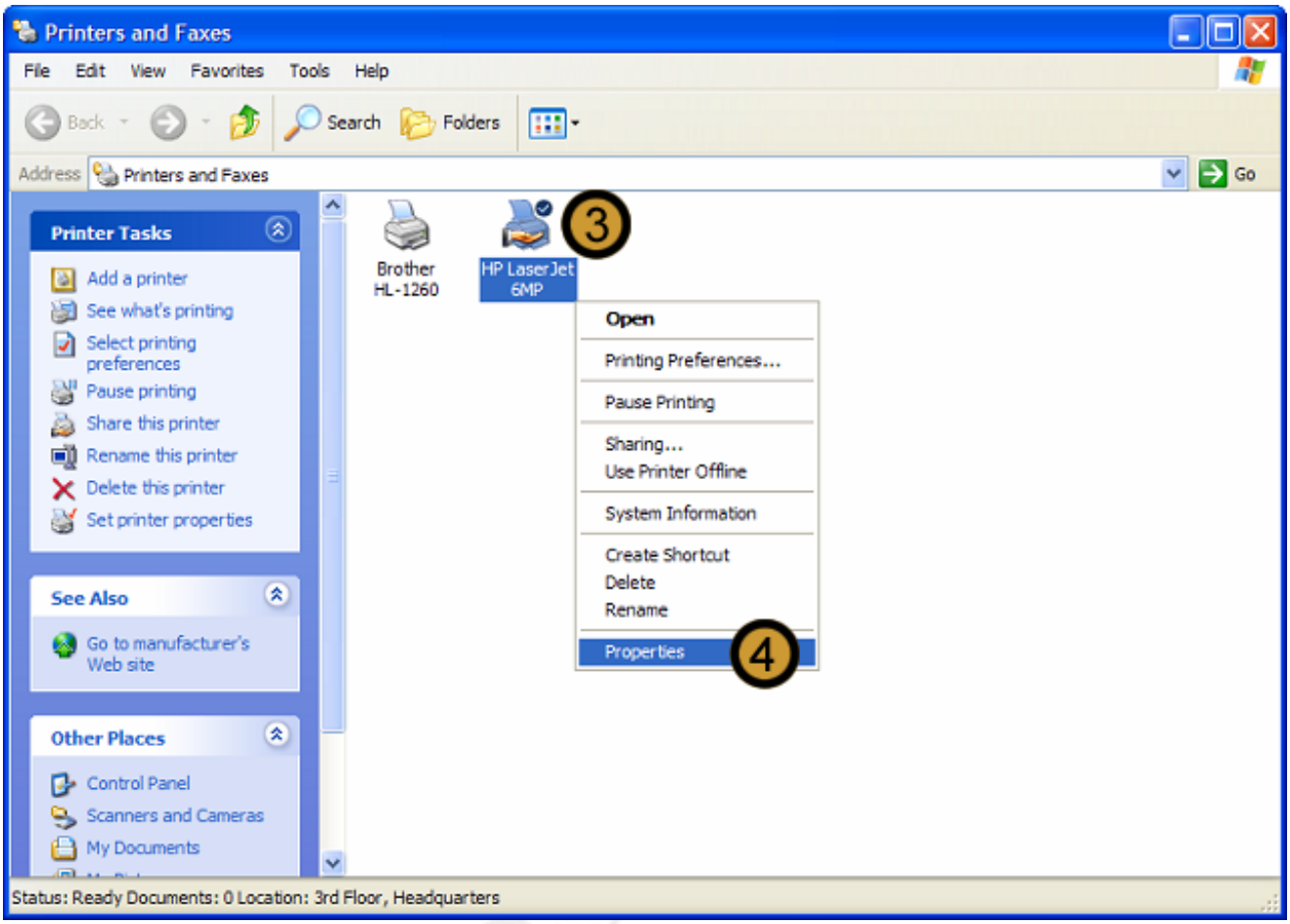


The new printer is now listed in the PRINTERS AND FAXES folder

9.4 Setting Printer Priorities

1. Click on the **START** button

2. Click on **PRINTERS AND FAXES**

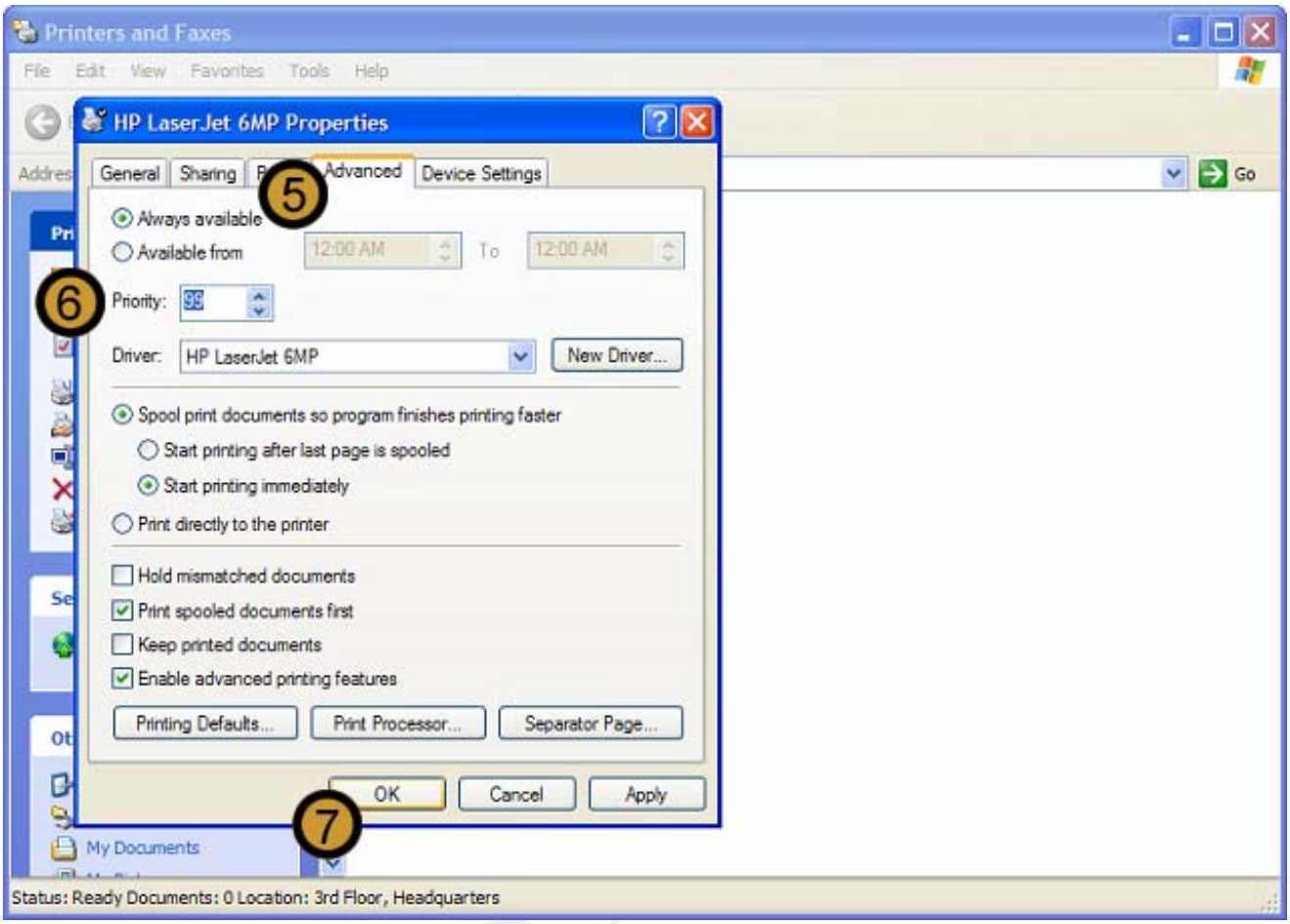


The PRINTERS AND FAXES folder appears

3. In the PRINTERS AND FAXES folder, right-click the printer for which you want to increase the priority

> **Note:** The printer priority range is 1 to 99 with the highest priority being 99 and the lowest being 1. The default setting is 1. Therefore we adjust the printer priority for the printer that we want to specify a higher priority for.

4. On the pop down menu that appears, click **PROPERTIES**



5. On the selected printer's **PROPERTIES** dialog box, click on the **ADVANCED** tab

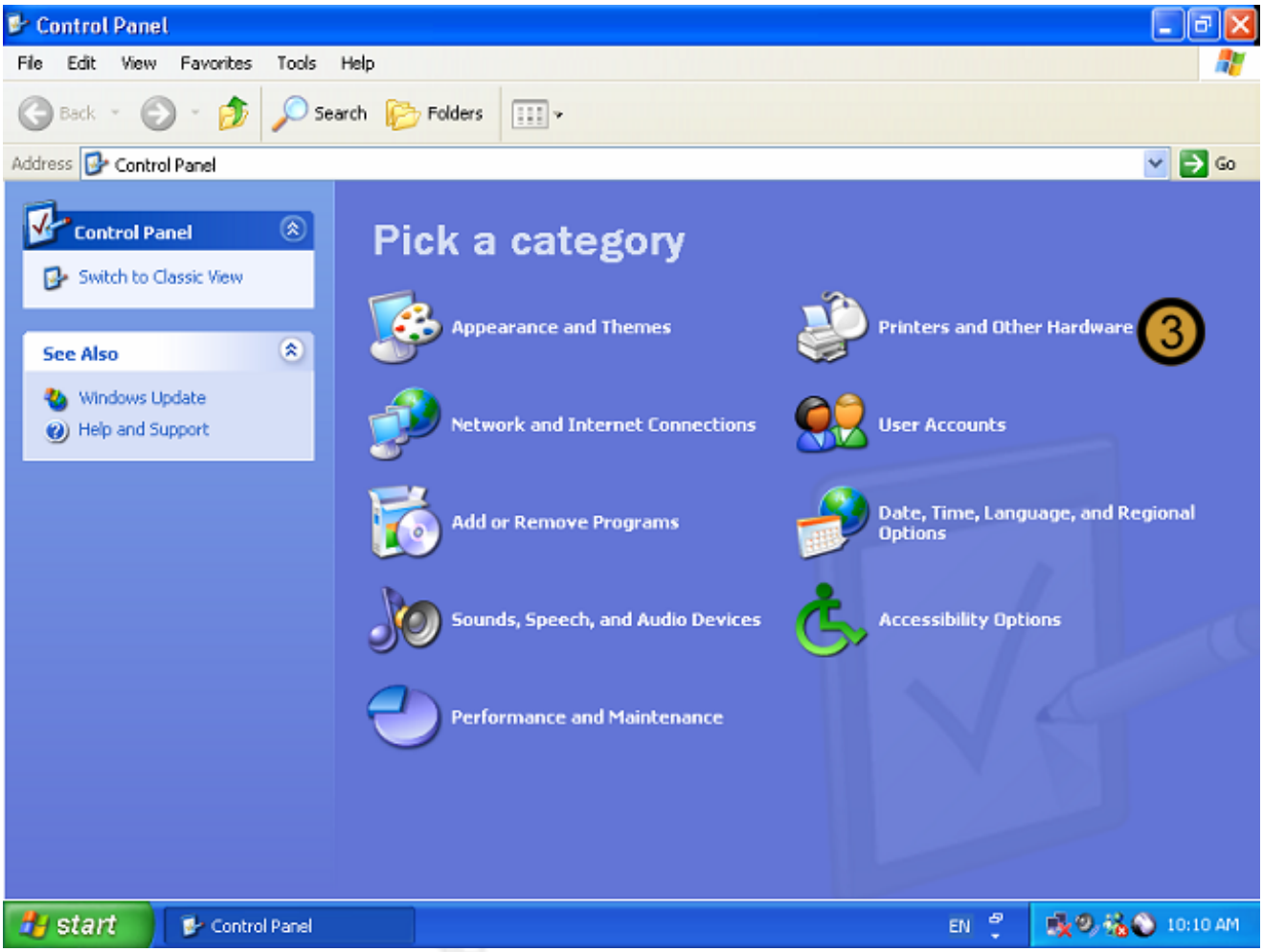
6. Set the priority for the printer

7. And click **OK**

9.5 Installing new hardware devices

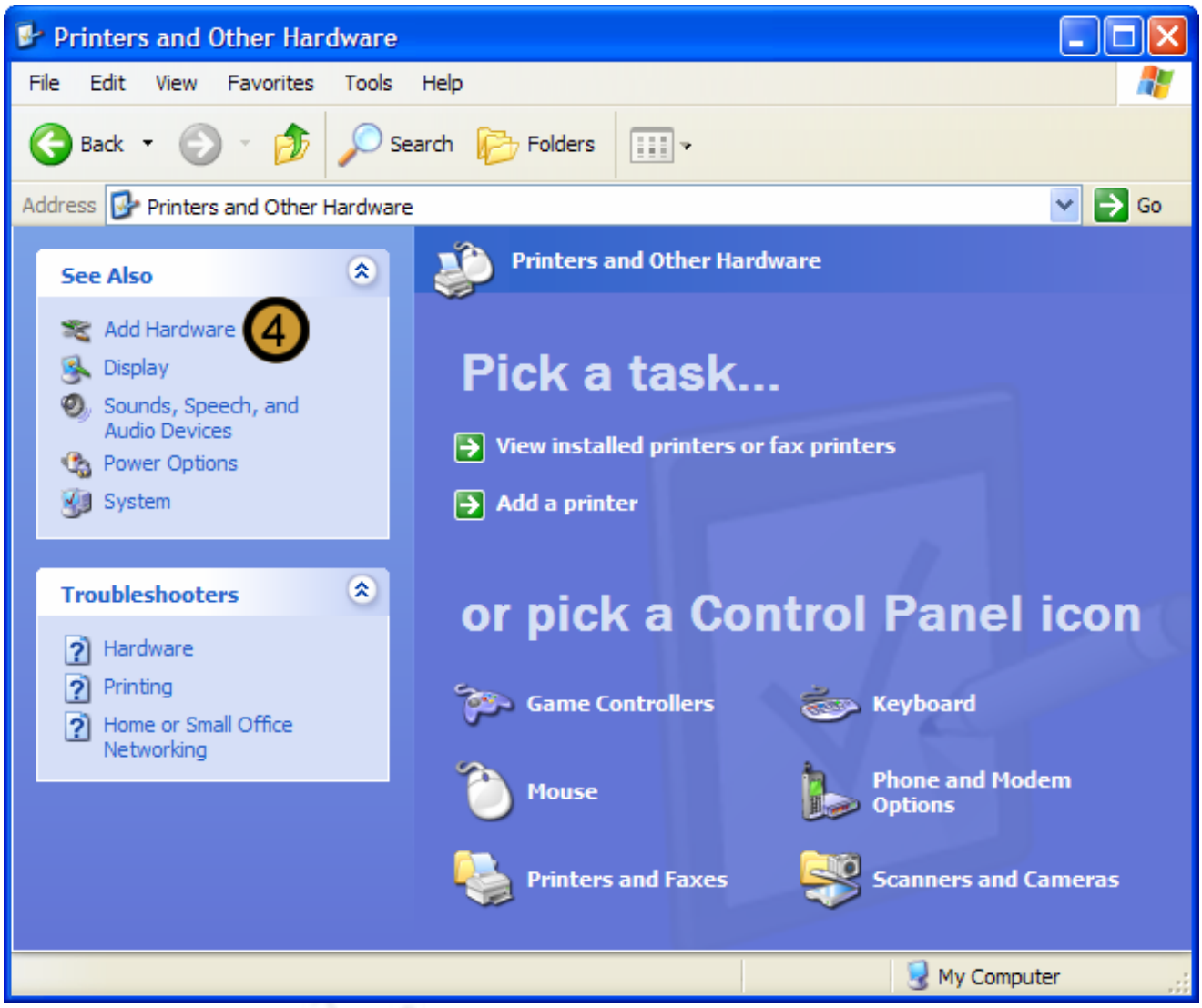
1. Click on the **START** button

2. Click on **CONTROL PANEL**



The Control Panel appears

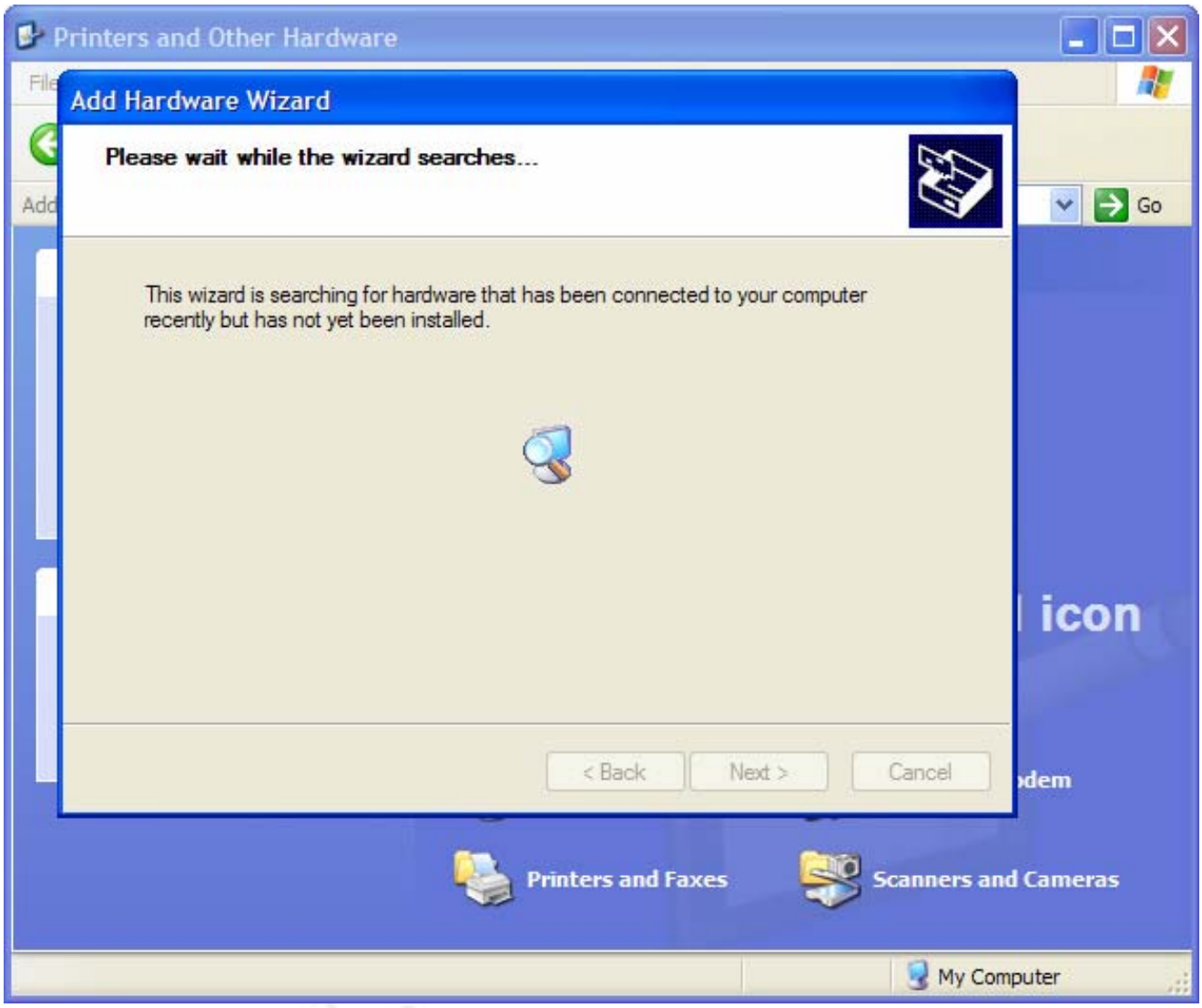
3. In the CONTROL PANEL, click on the **PRINTERS AND OTHER HARDWARE** icon



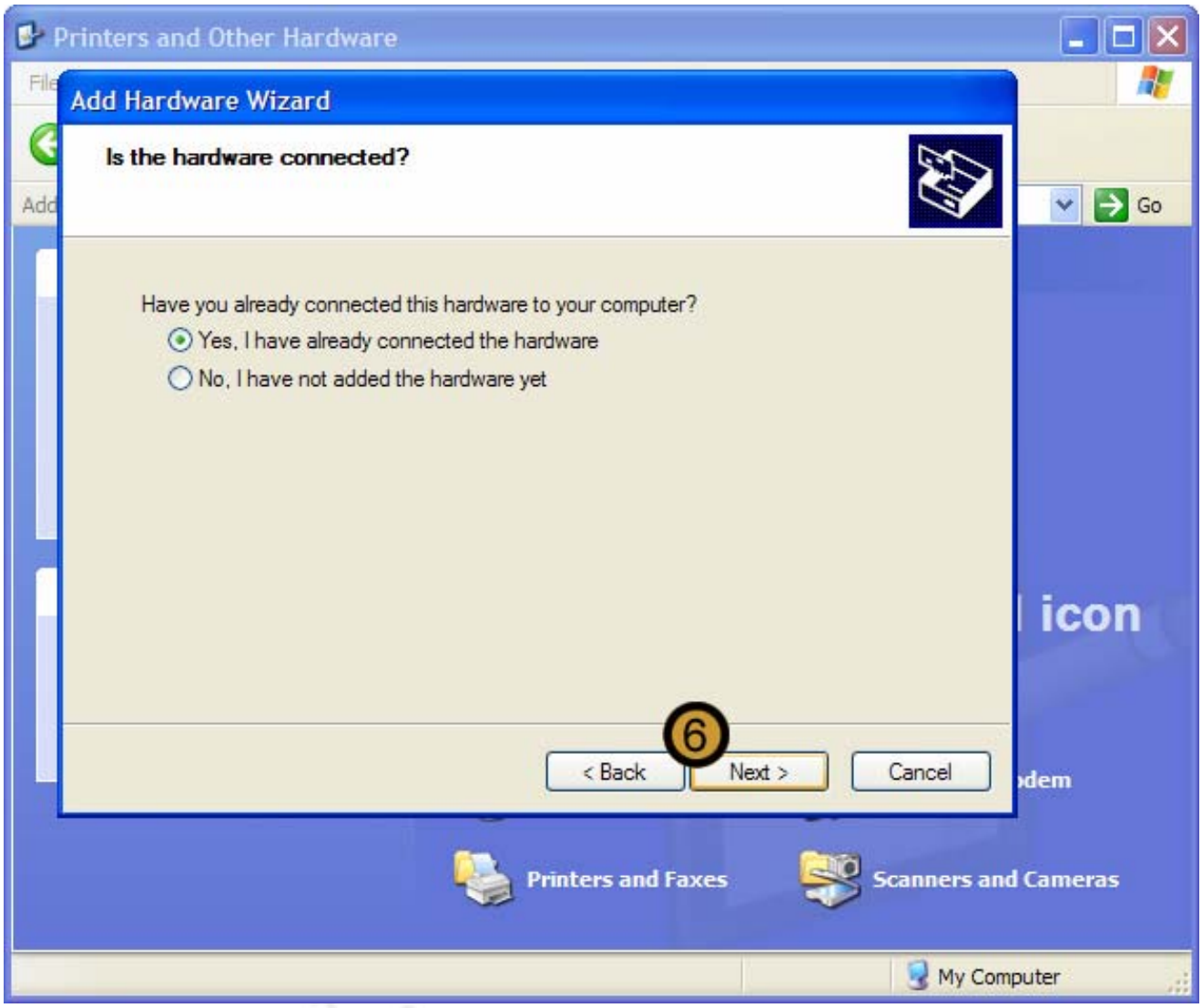
4. Click on **ADD HARDWARE**

The ADD HARDWARE WIZARD appears

5. In the ADD HARDWARE WIZARD, click on the **PRINTERS AND OTHER HARDWARE** icon



The ADD HARDWARE WIZARD searches for new hardware


Printers and Other Hardware
Add Hardware Wizard
Is the hardware connected?
Have you already connected this hardware to your computer?
Yes, I have already connected the hardware
No, I have not added the hardware yet
6
< Back
Next >
Cancel
Go
icon
Printers and Faxes
Scanners and Cameras
My Computer

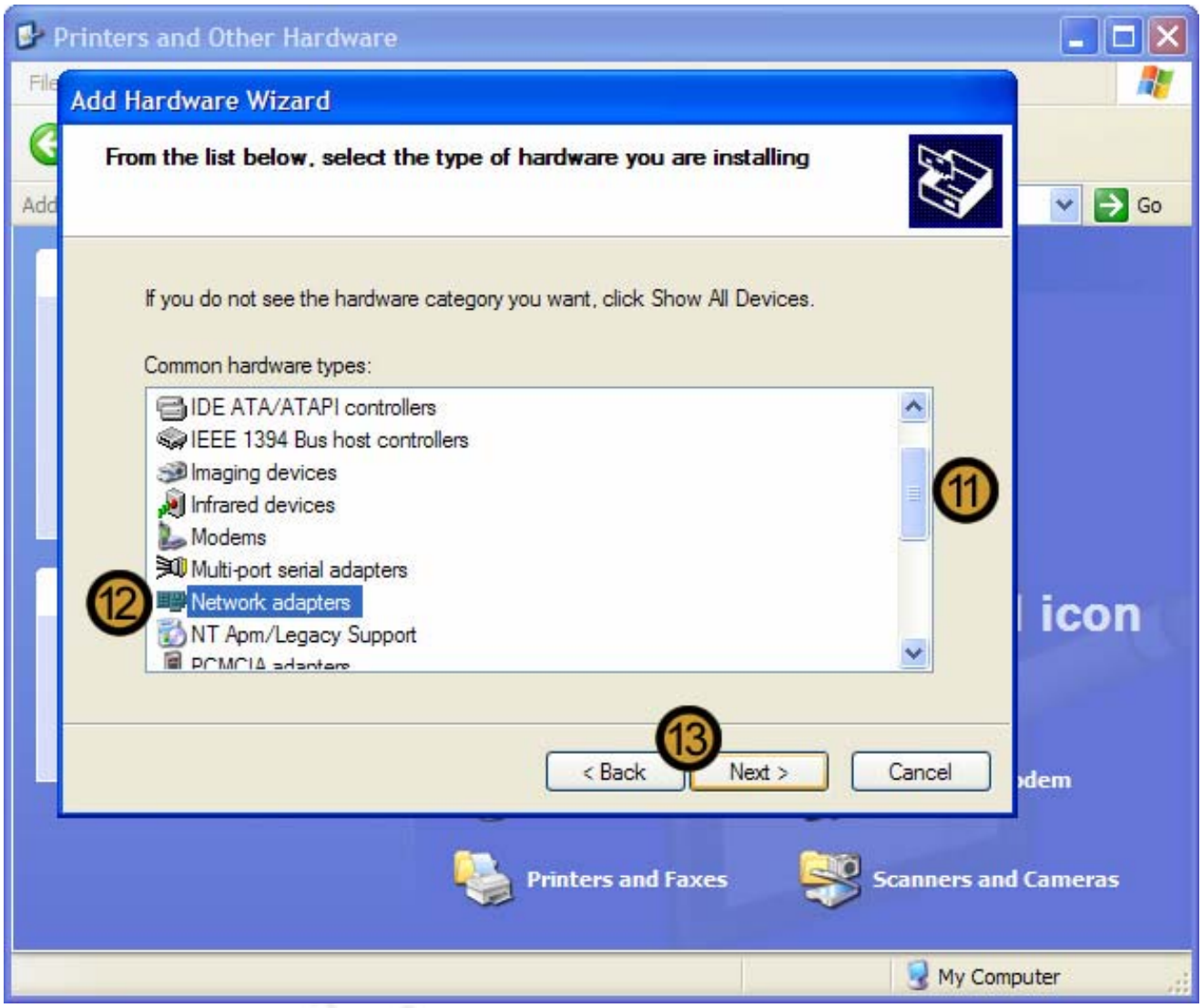
6. Click **NEXT**

7. On the Installed hardware list, scroll down to locate the hardware you wish to install. If it is not on the list click on the **ADD A NEW HARDWARE DEVICE**

8. Click **NEXT**

9. Select the **INSTALL THE HARDWARE THAT I MANUALLY SELECT FROM A LIST** radio button

10. Click **NEXT**

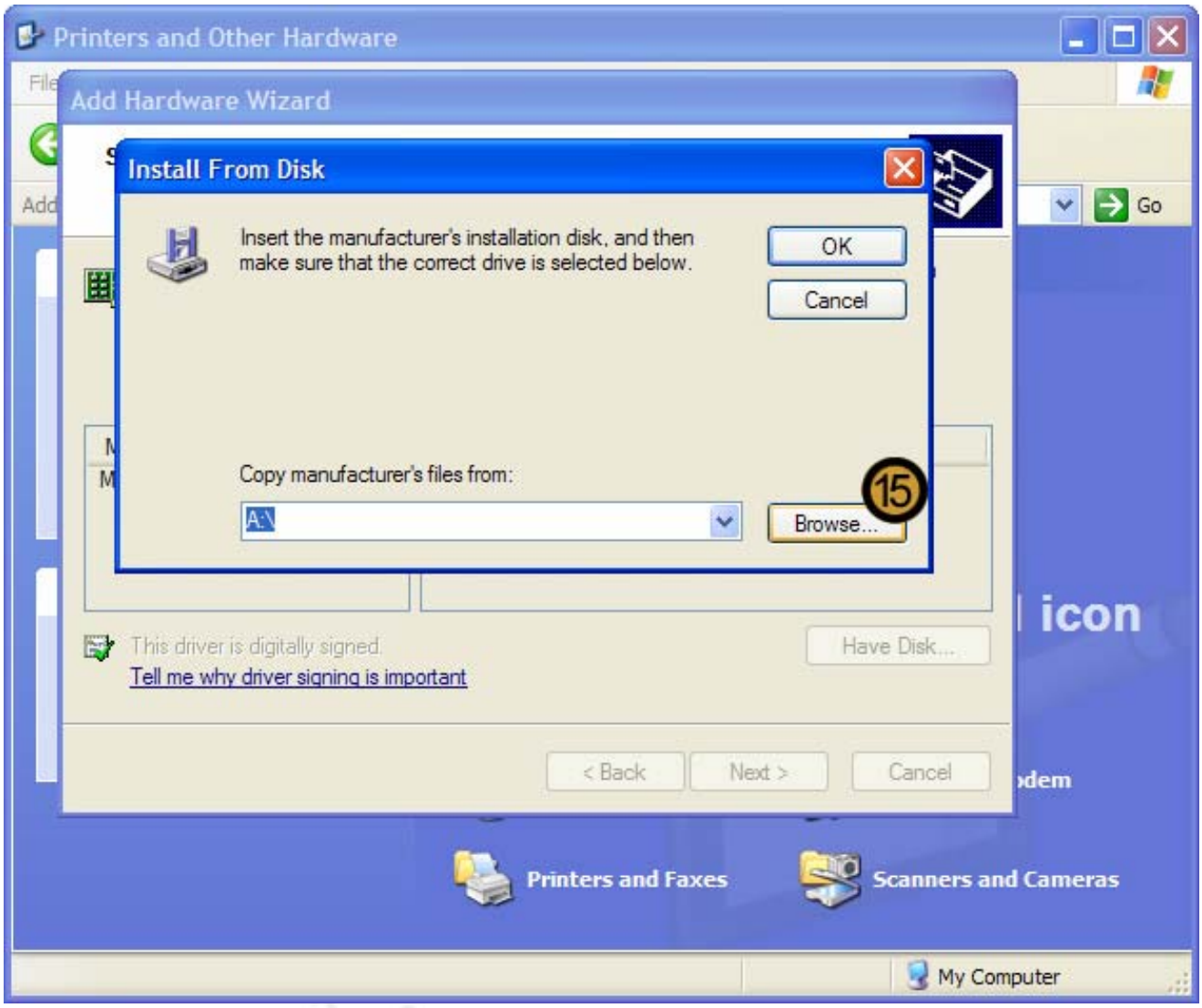


11. On the COMMON HARDWARE TYPES list, use the scroll bar to scroll down t o the hardware type that you want to install

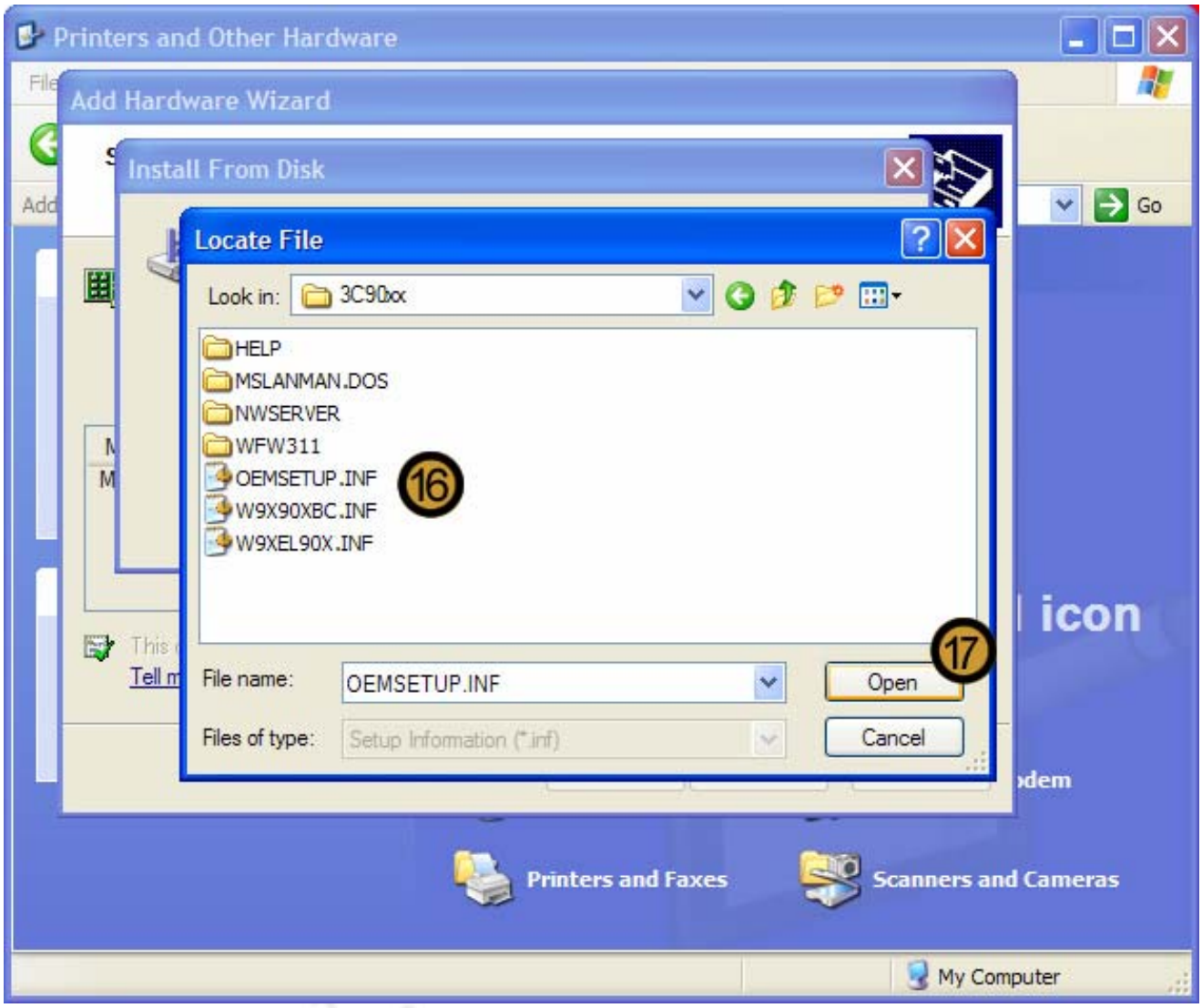
12. Click on the Hardware Type that you want to install

13. Click **NEXT**

14. Click on **HAVE DISK …**

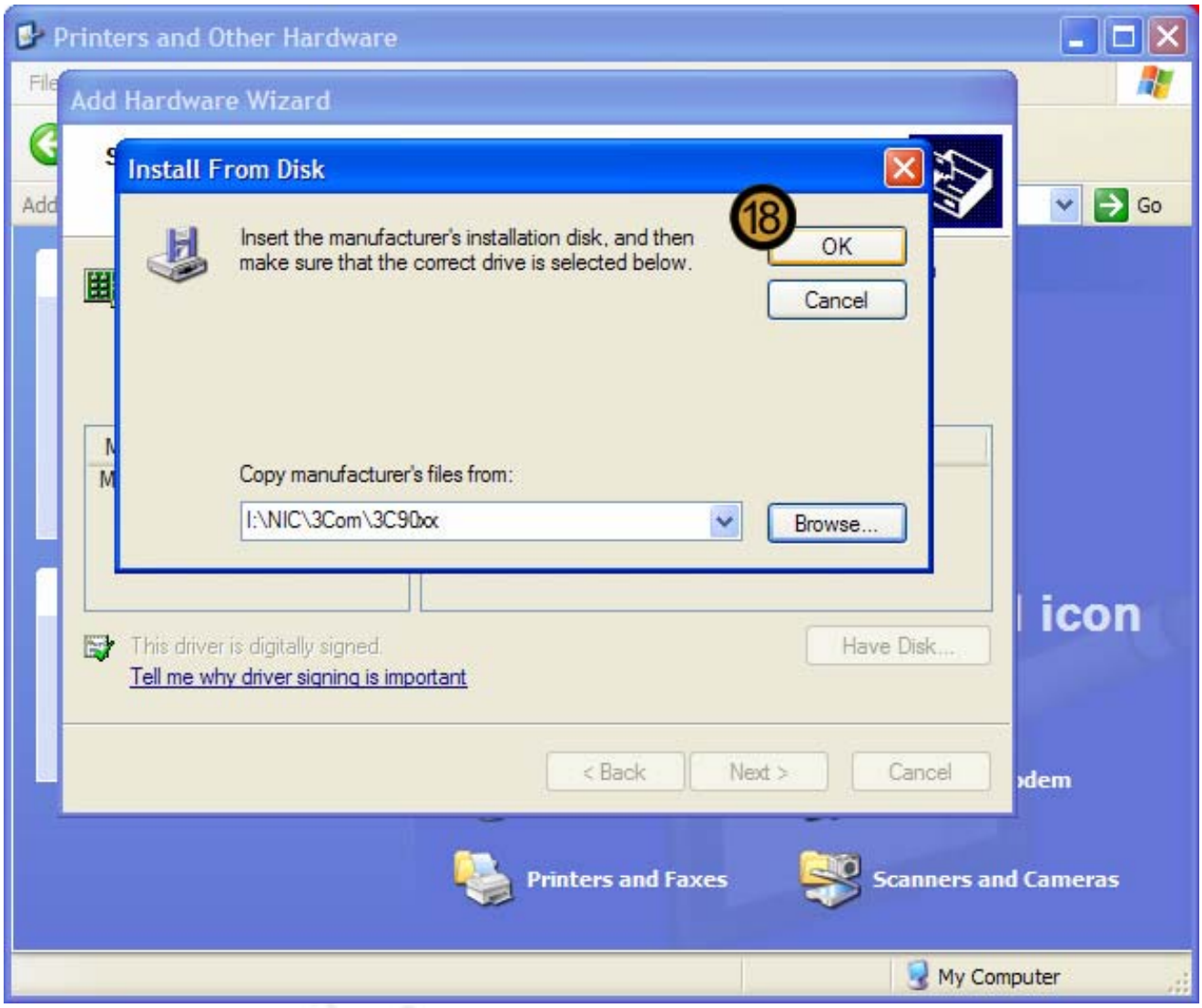


15. Click **BROWSE …**

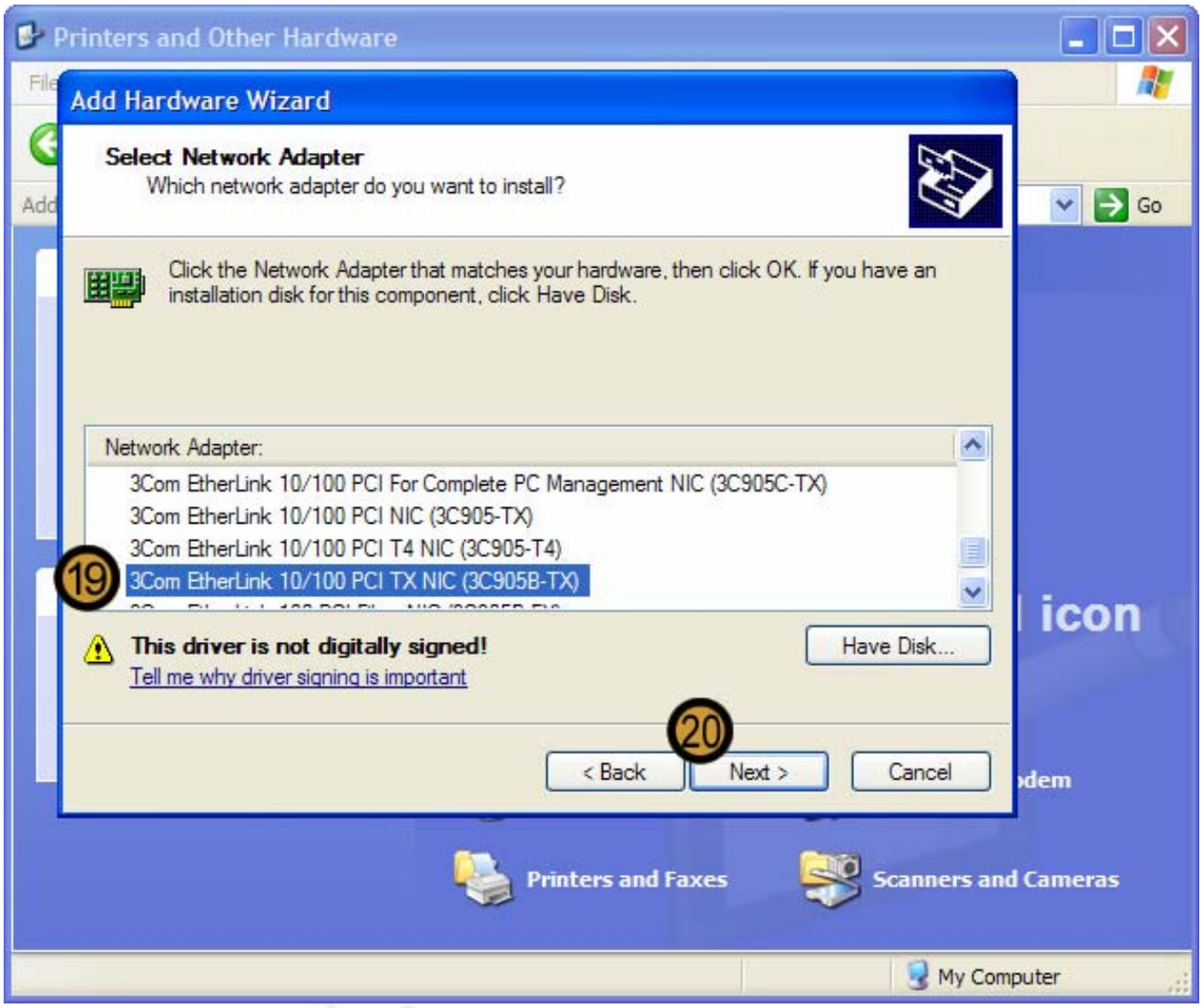


16. Locate the driver for the device that you want to install

17. Click **OPEN**

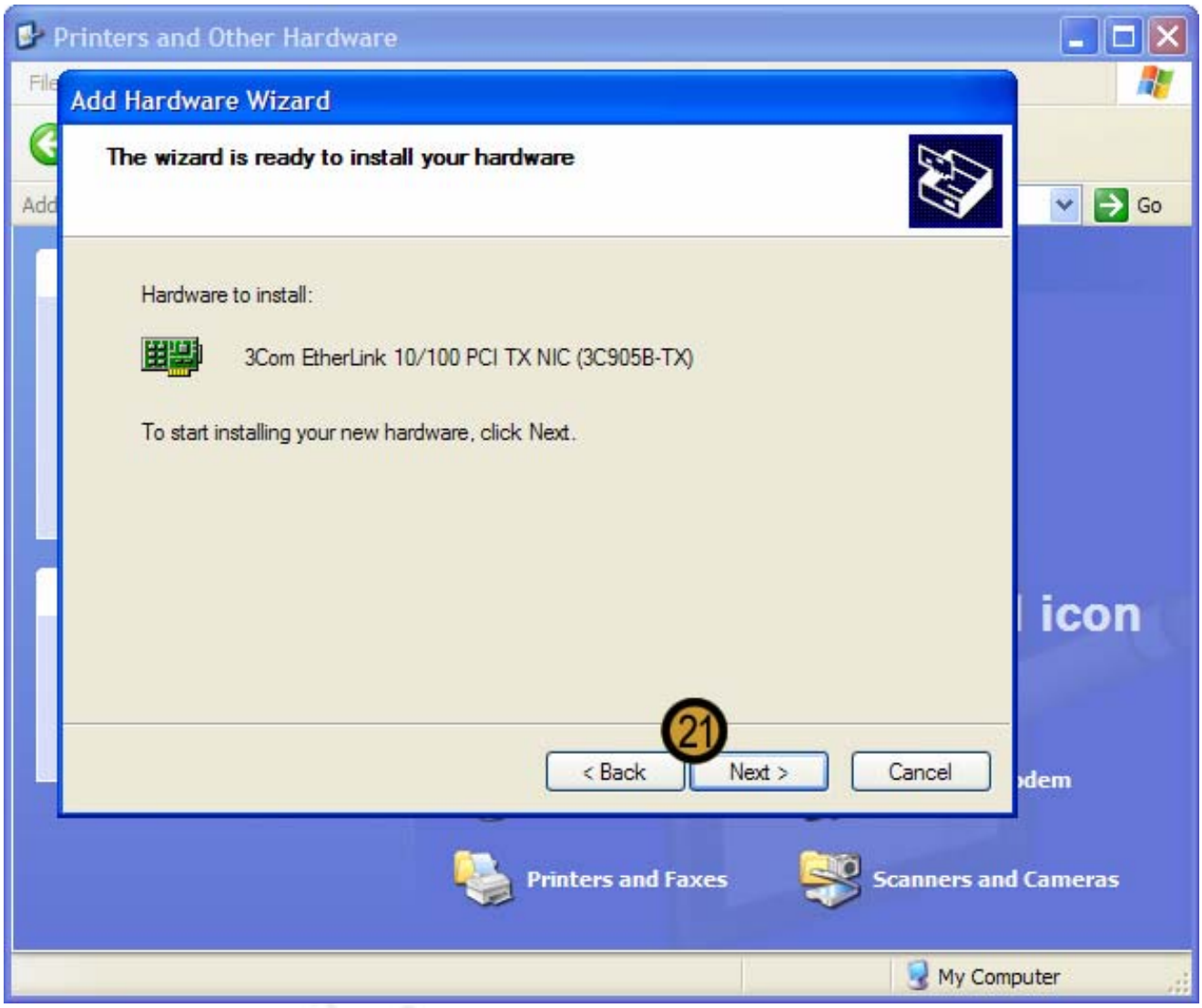


18. Once you have located the device driver, click **OK**



19. Select the correct hardware device if the device driver is associated with a number of hardware devices

20. Click **NEXT**



21. Click **NEXT**

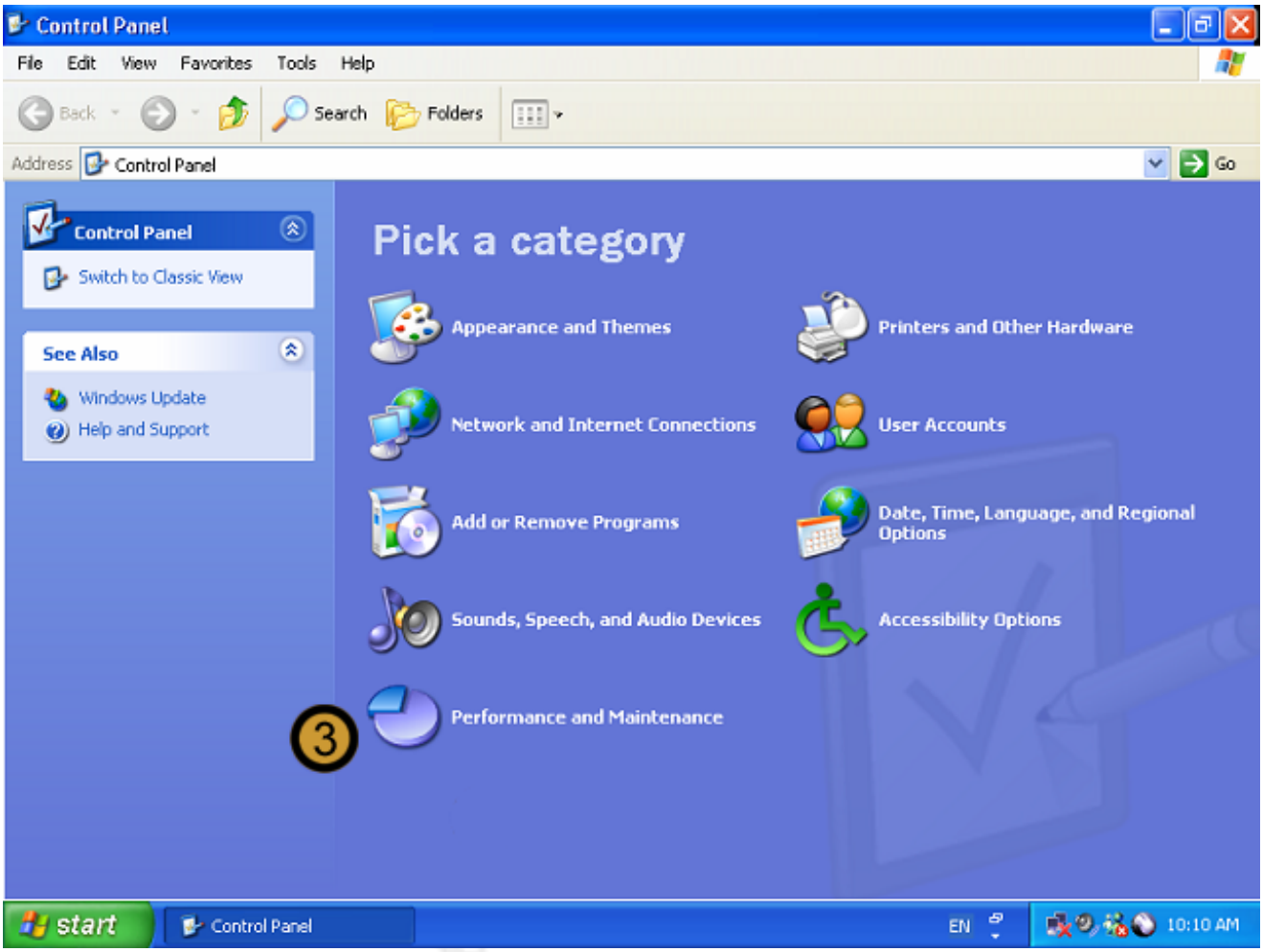
Windows XP Professional completes the installation of the required device driver

9.6. Working with Device Drivers
9.6.1 Updating Device Drivers

In this example we will be updating the Network Adapter driver with a driver that has been downloaded from the internet

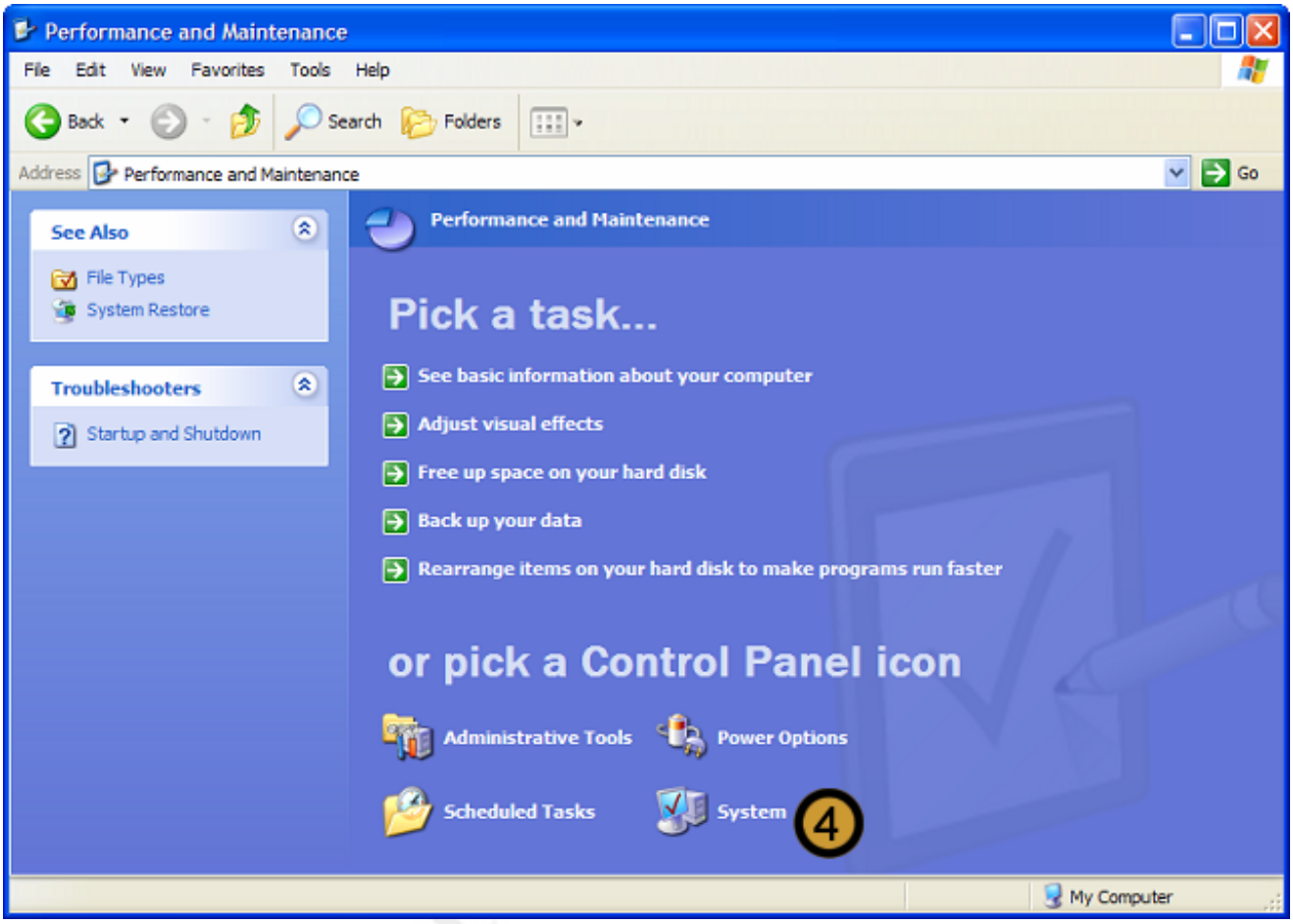
1. Click on the **START** button

2. Click on **CONTROL PANEL**

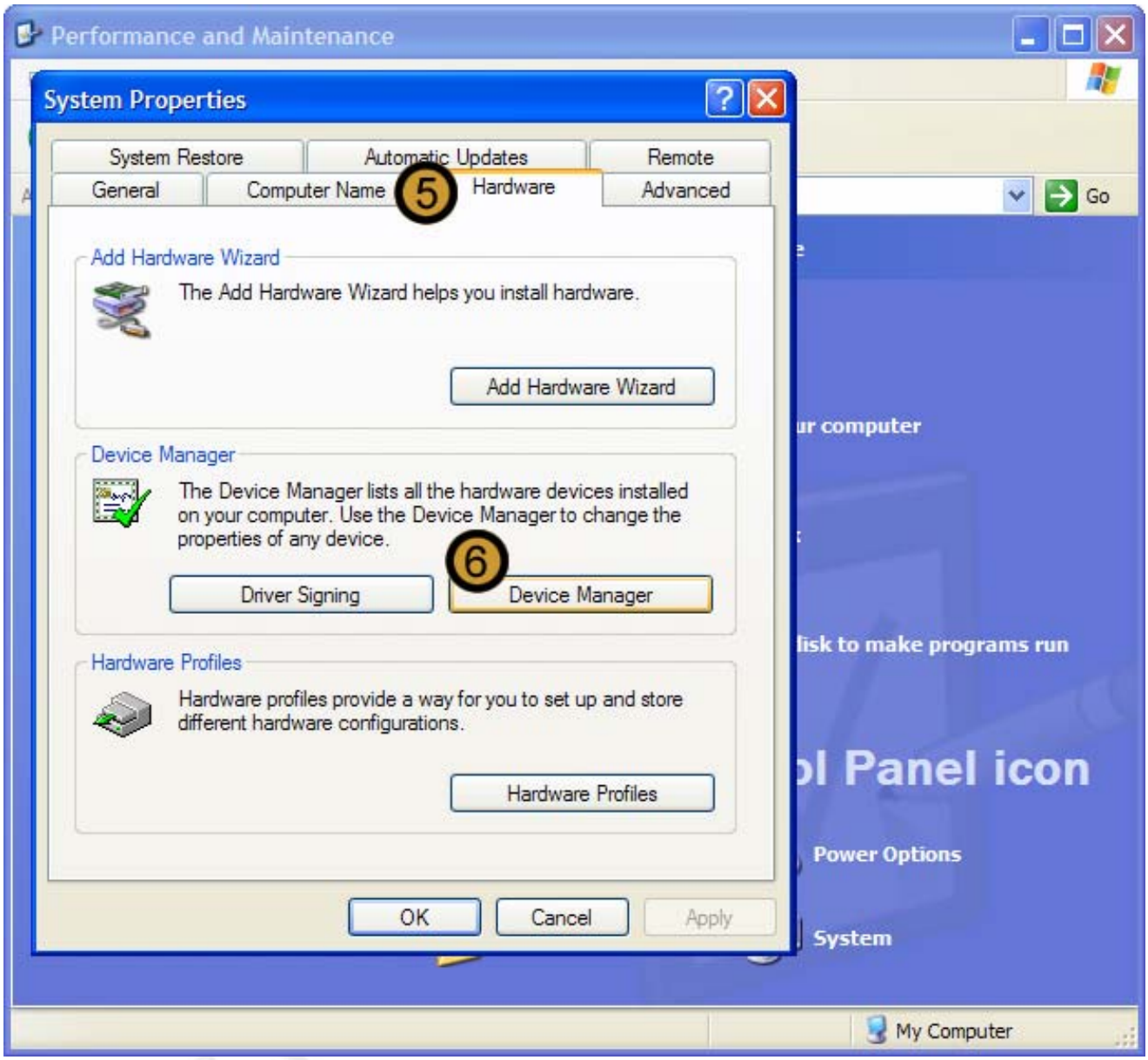


The **Control Panel** appears

3. In the CONTROL PANEL, click on the **PERFORMANCE AND MAINTENANCE** icon



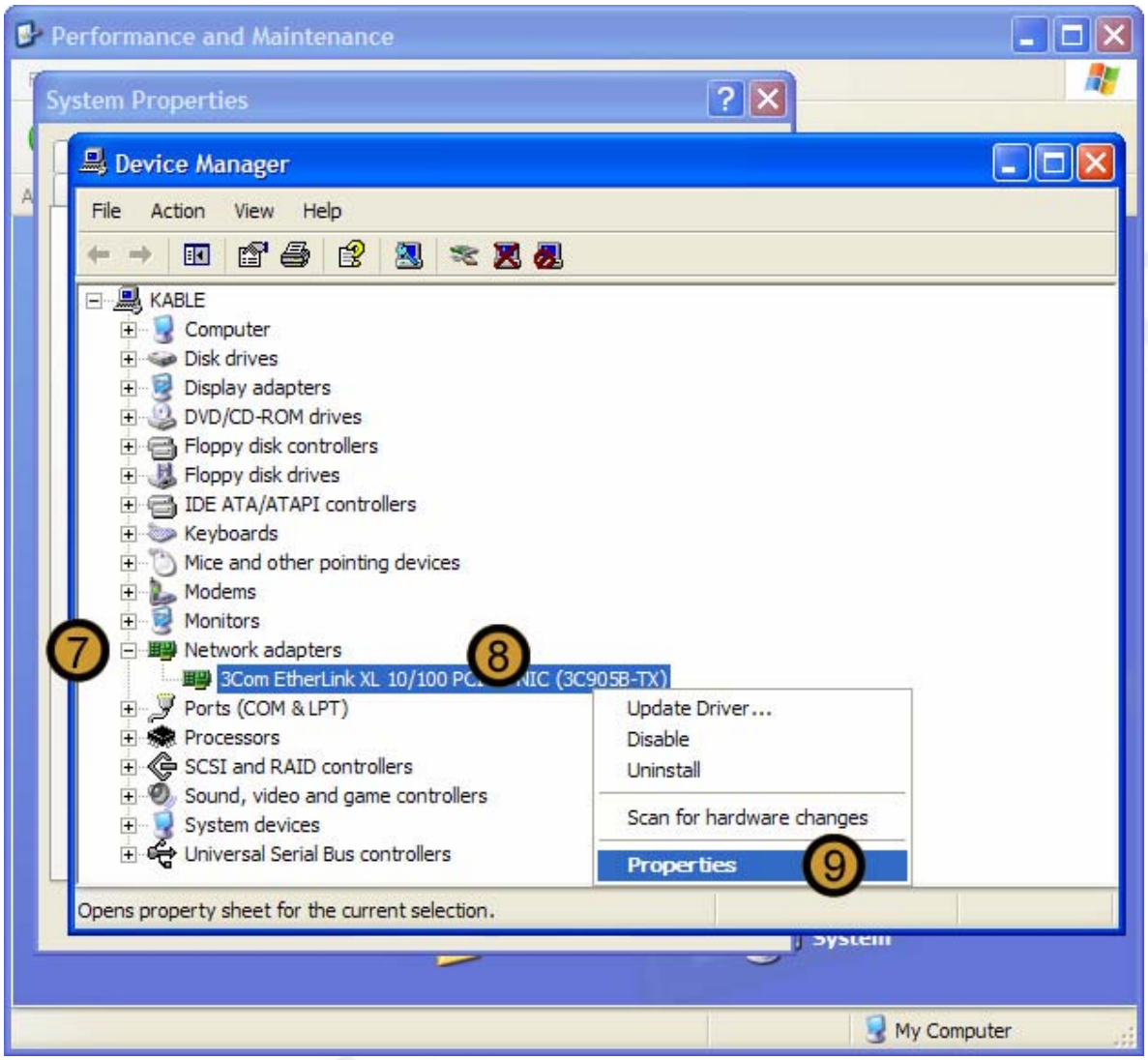
4. In PERFORMANCE AND MAINTENANCE, click **SYSTEM**



The SYSTEM PROPERTIES dialog box appears

5. In SYSTEM PROPERTIES dialog box, click on the **HARDWARE** tab

6. In the DEVICE MANAGER section, click **DEVICE MANAGER**

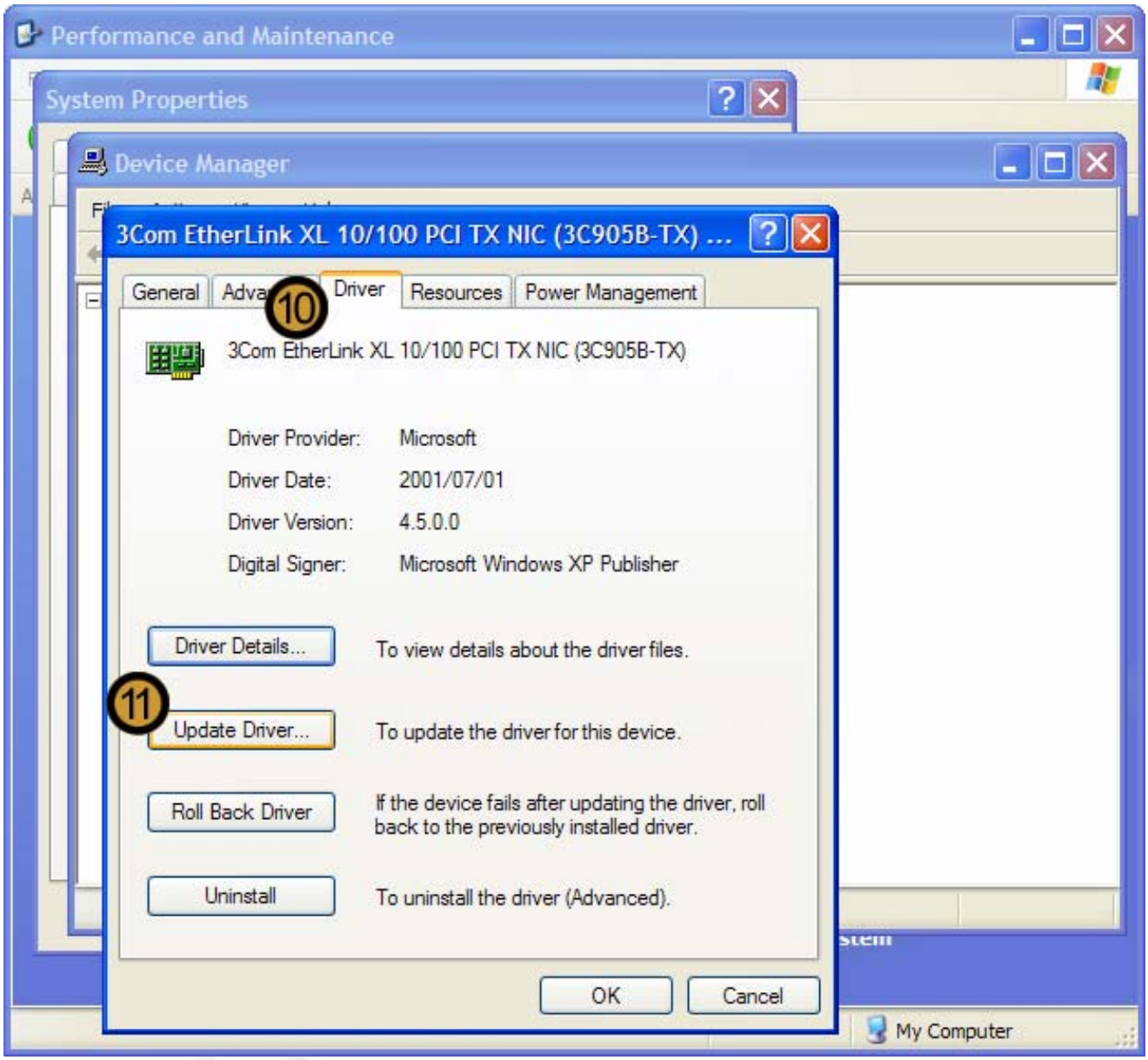


The DEVICE MANANGER appears

7. In DEVICE MANAGER, expand the Hardware Type of the hardware that you want to update

8. Right-click on the Hardware device that you want to upgrade

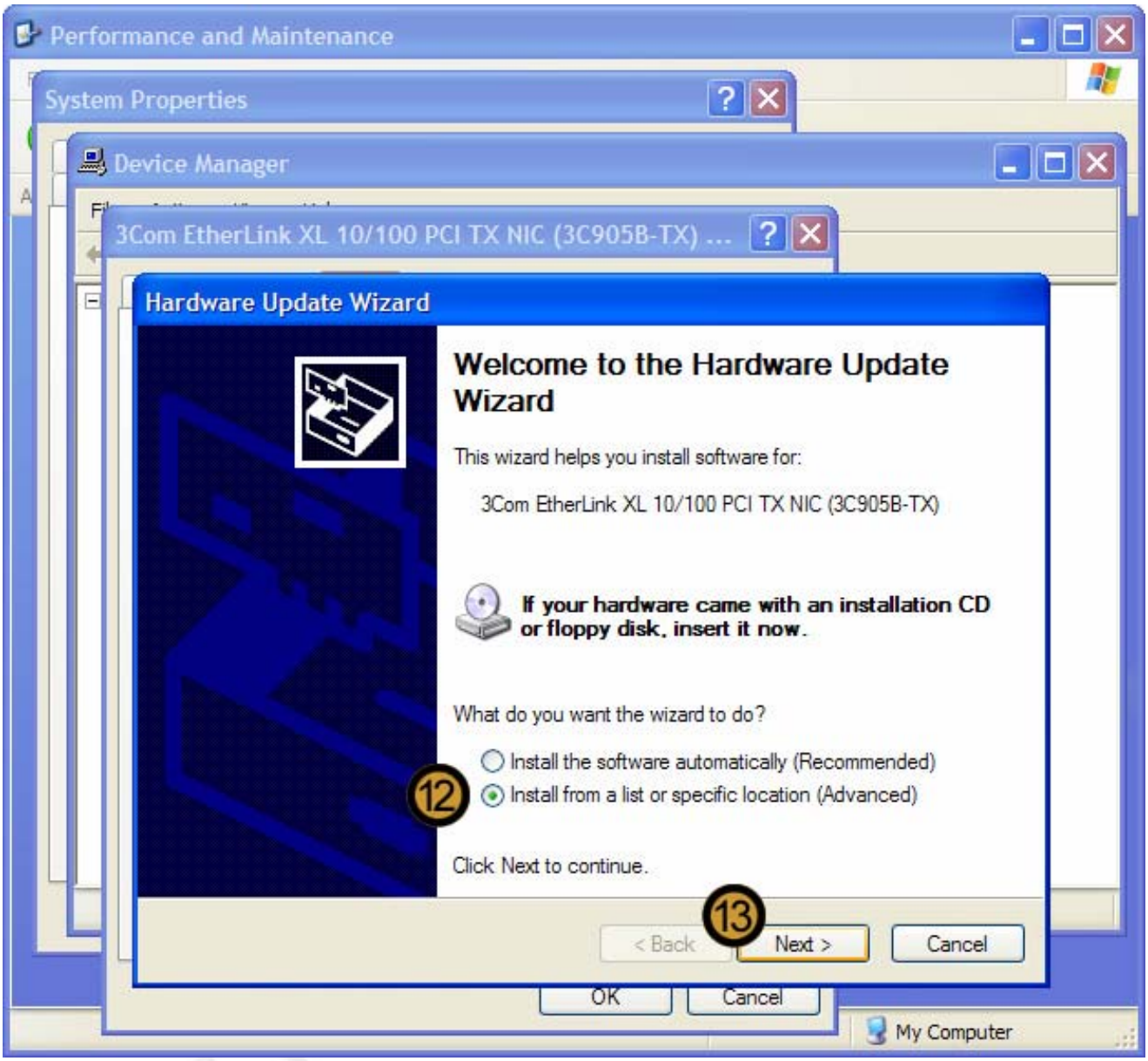
9. On the drop down menu that appears, click **PROPERTIES**



The DEVICE PROPERTIES dialog box appears

10. On the specified DEVICE PROPERTIES dialog box, click on the **DRIVER** tab

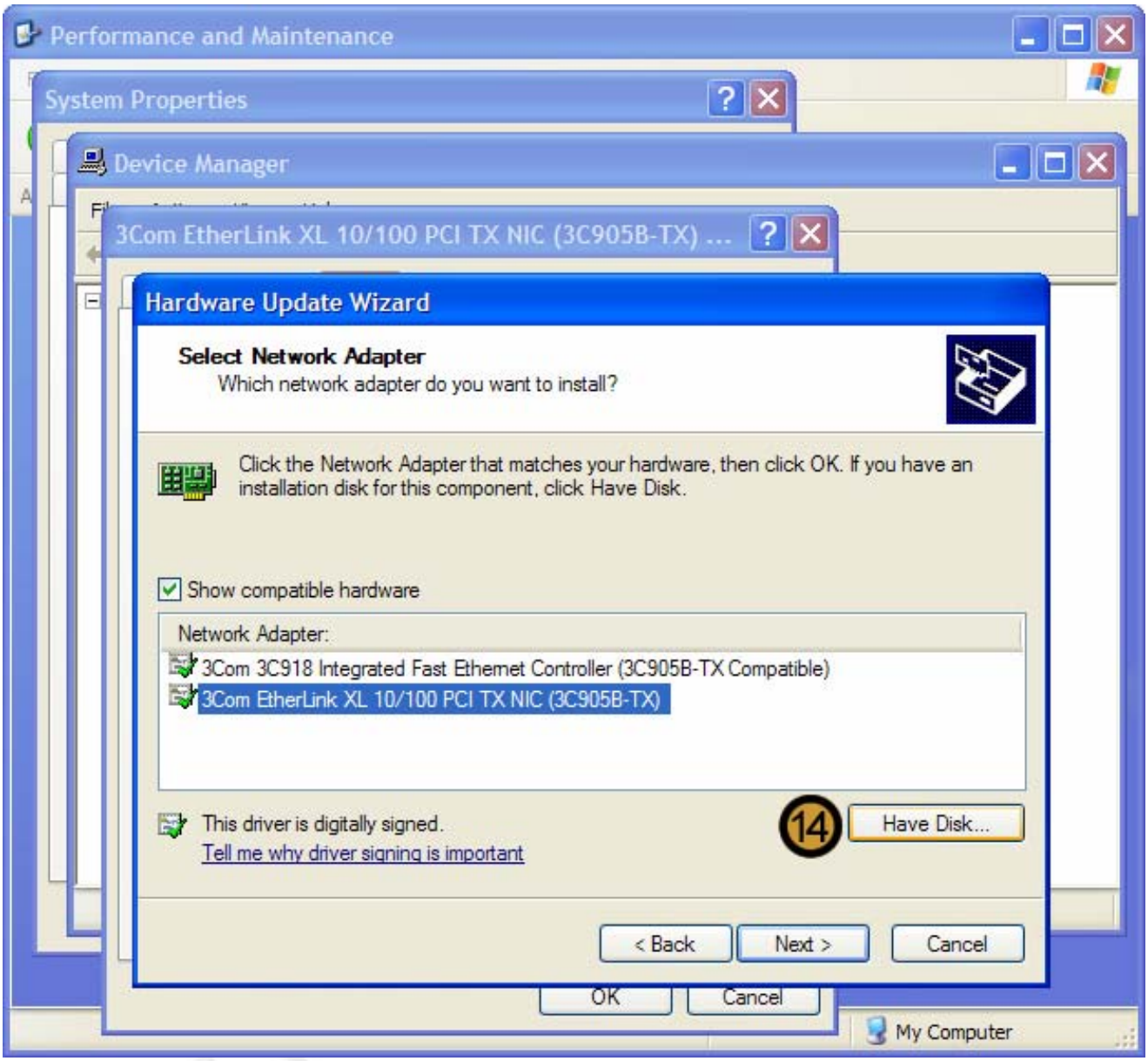
11. Click **UPDATE DRIVER**



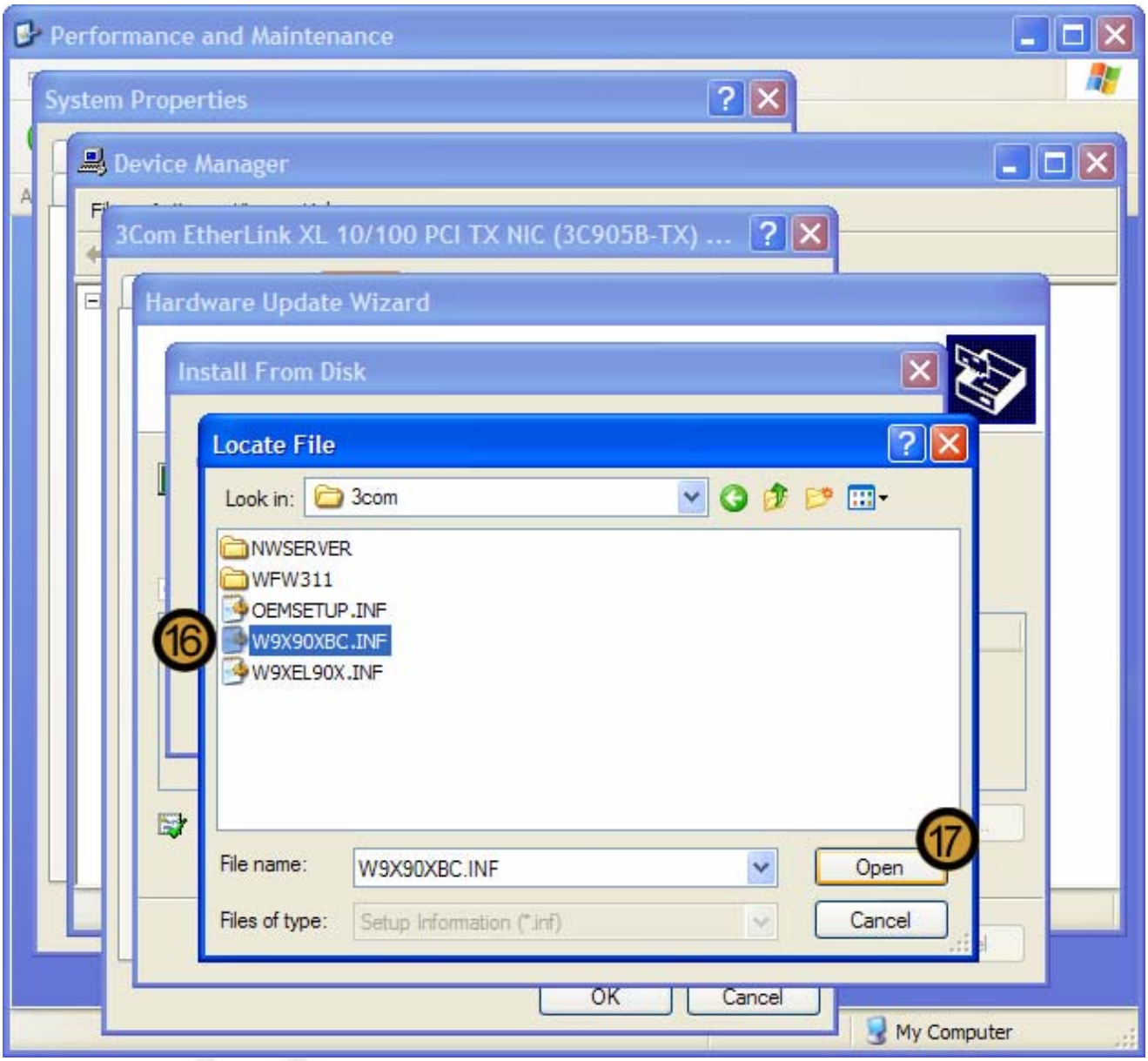
The HARDWARE UPDATE WIZARD appears

12. On HARDWARE UPDATE WIZARD, select the **INSTALL FROM A LIST SPECIFIC LOCATION** radio button

13. Click **NEXT**



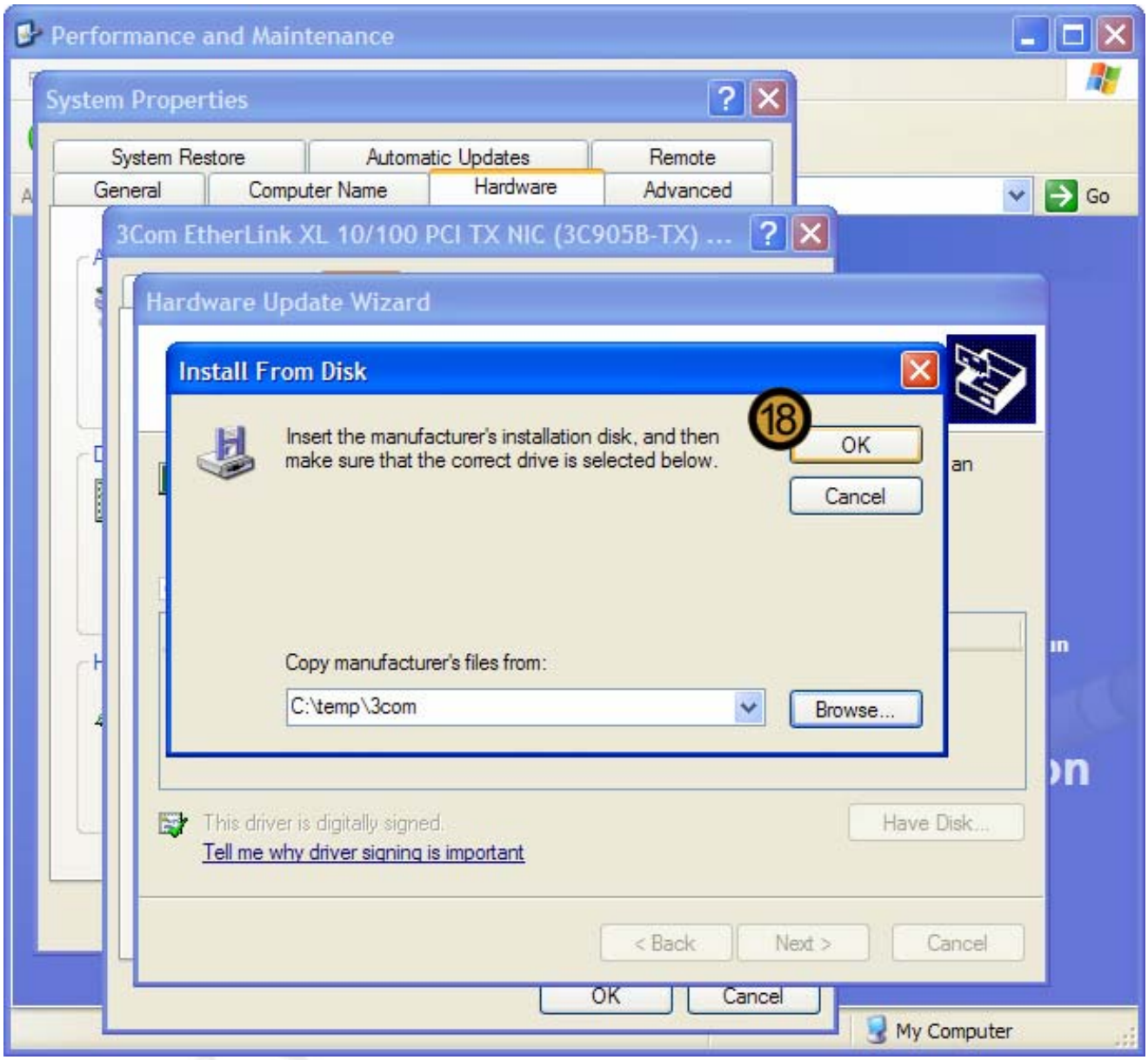
14. Click **HAVE DISK ...**



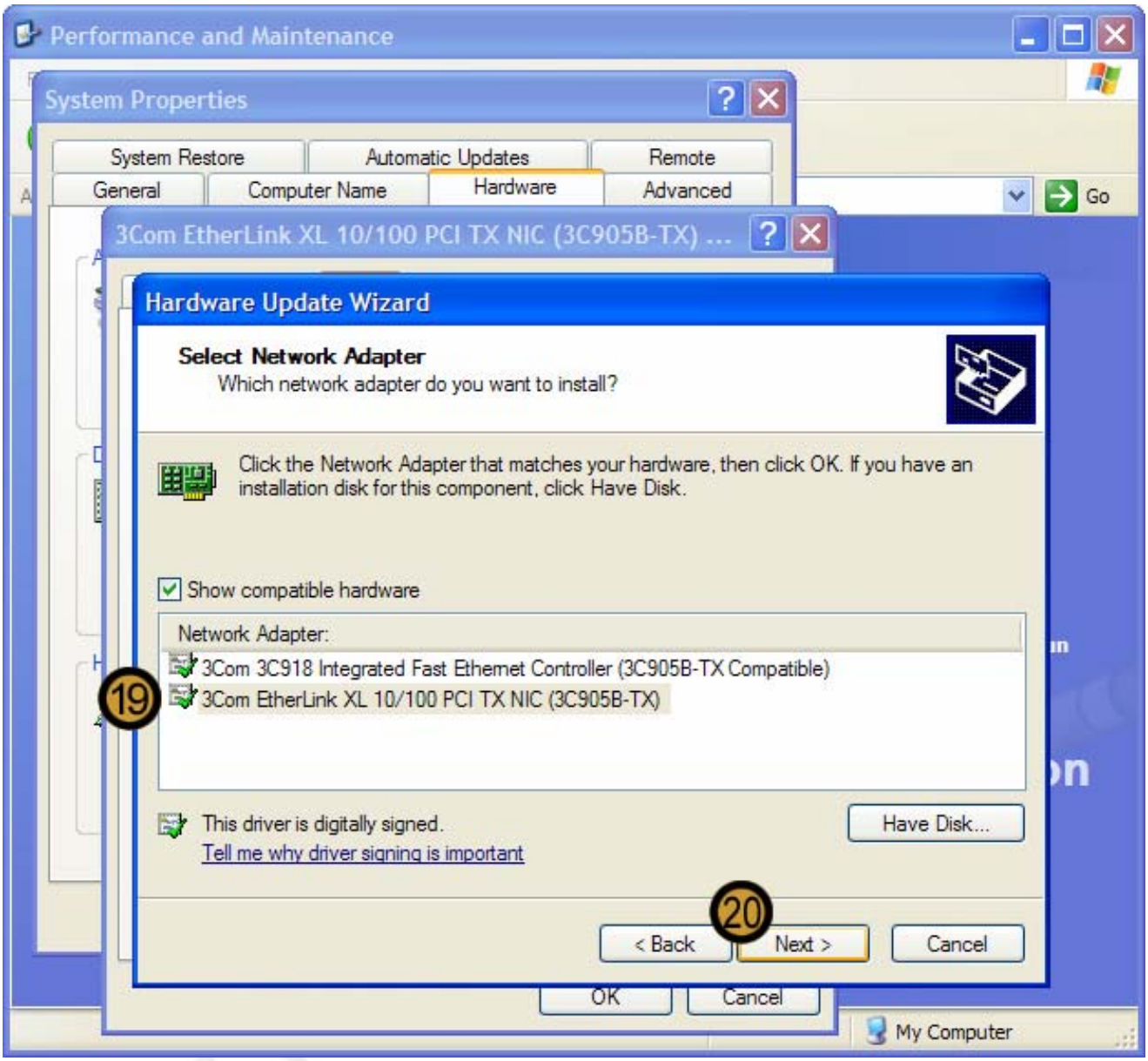
15.

16. Locate the downloaded driver can click on it

17. Click **OPEN**

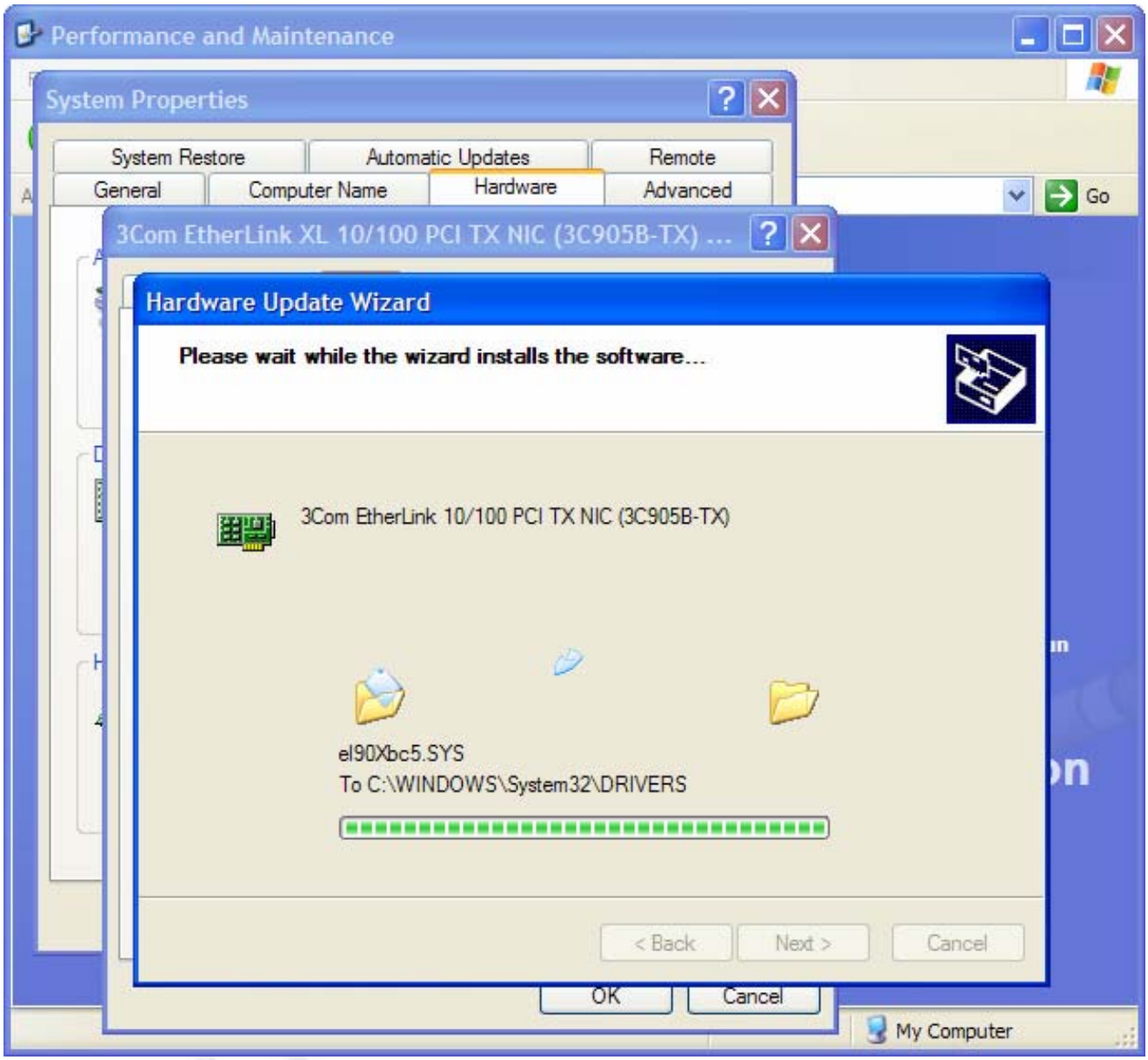

Performance and Maintenance
System Properties
System Restore
Automatic Updates
Remote
General
Computer Name
Hardware
Advanced
Go
3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX) ...
Hardware Update Wizard
Install From Disk
18
Insert the manufacturer's installation disk, and then make sure that the correct drive is selected below.
OK
Cancel
Copy manufacturer's files from:
C:\temp\3com
Browse...
This driver is digitally signed.
Tell me why driver signing is important
Have Disk...
< Back
Next >
Cancel
OK
Cancel
My Computer

18. Click **OK**

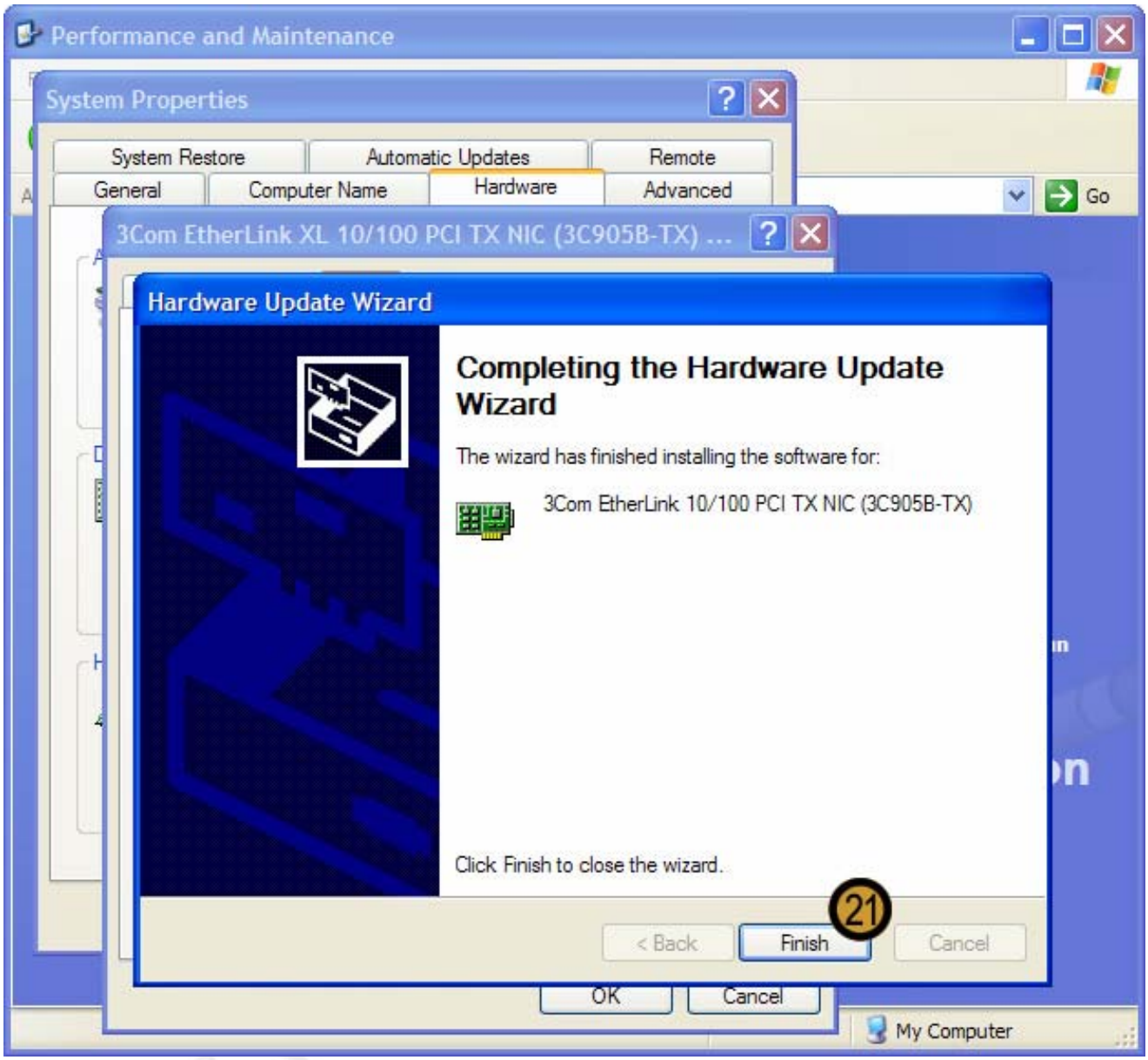


19. Ensure that the correct Device is selected

20. Click **NEXT**



Windows XP Professional installs the new device driver

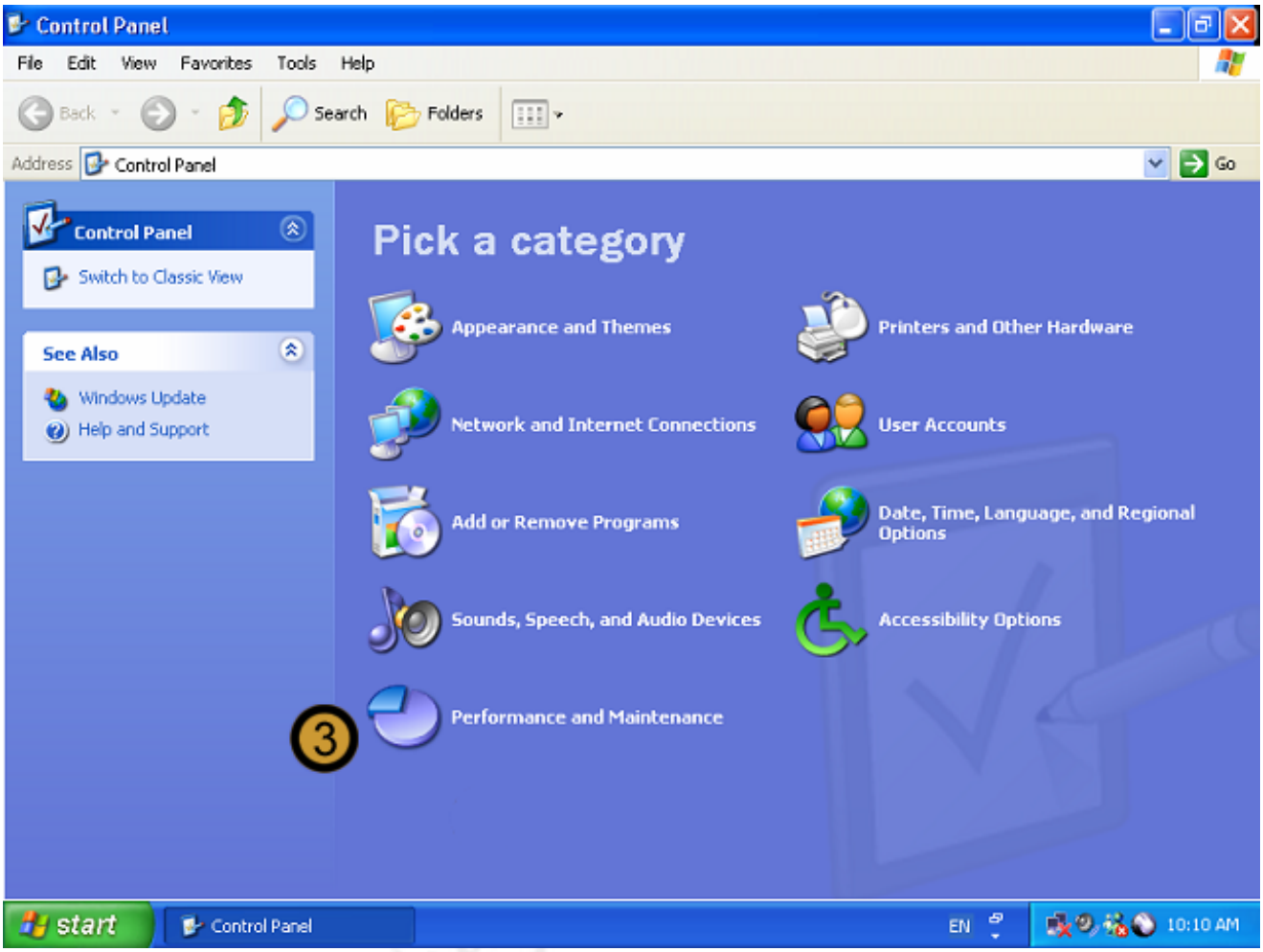


21. to complete the installation of the new device driver, click **FINISH**

9.6.2 Setting Driver Signing options

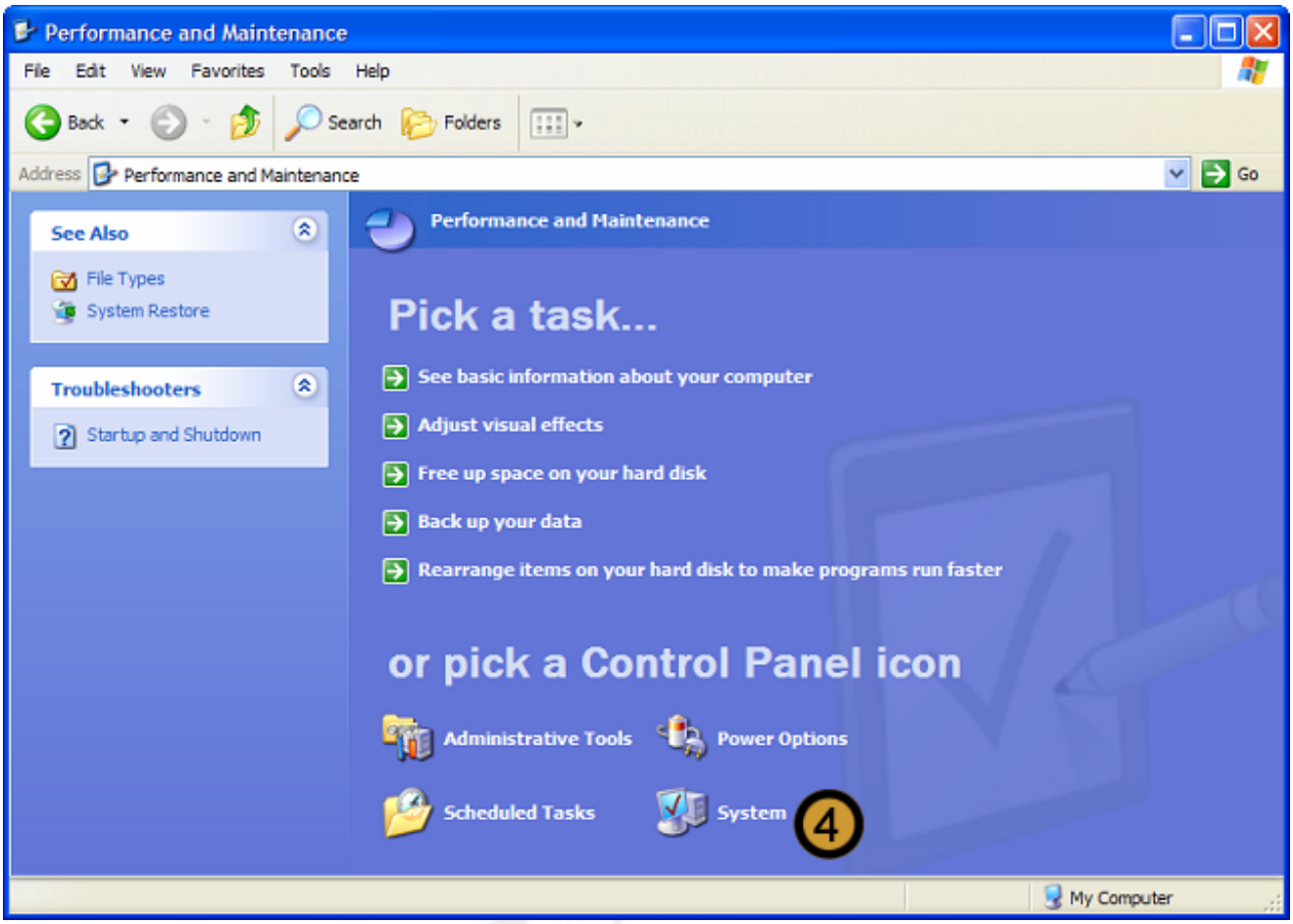
1. Click on the **START** button

2. Click on **CONTROL PANEL**

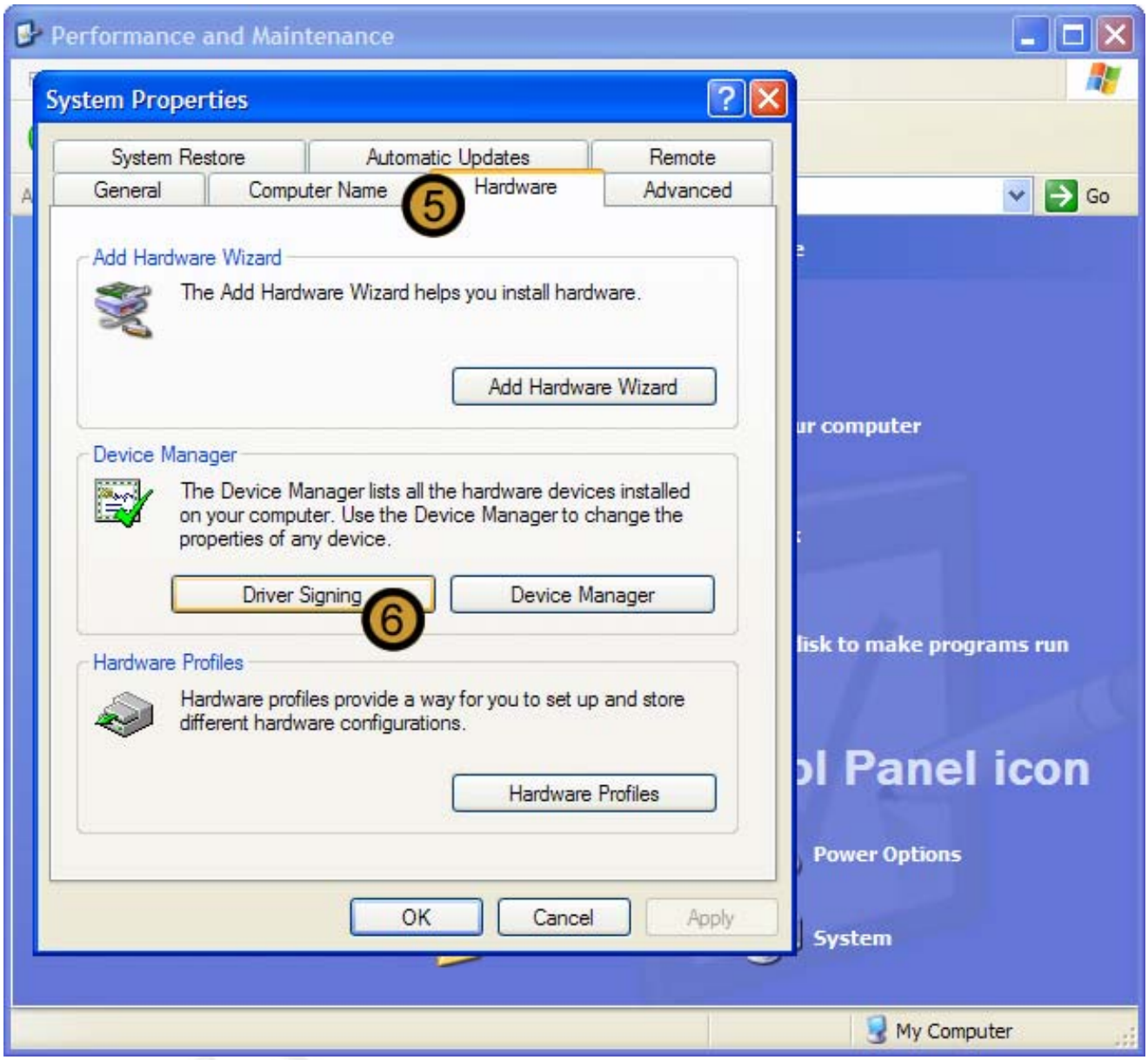


The **Control Panel** appears

3. In the CONTROL PANEL, click on the **PERFORMANCE AND MAINTENANCE** icon



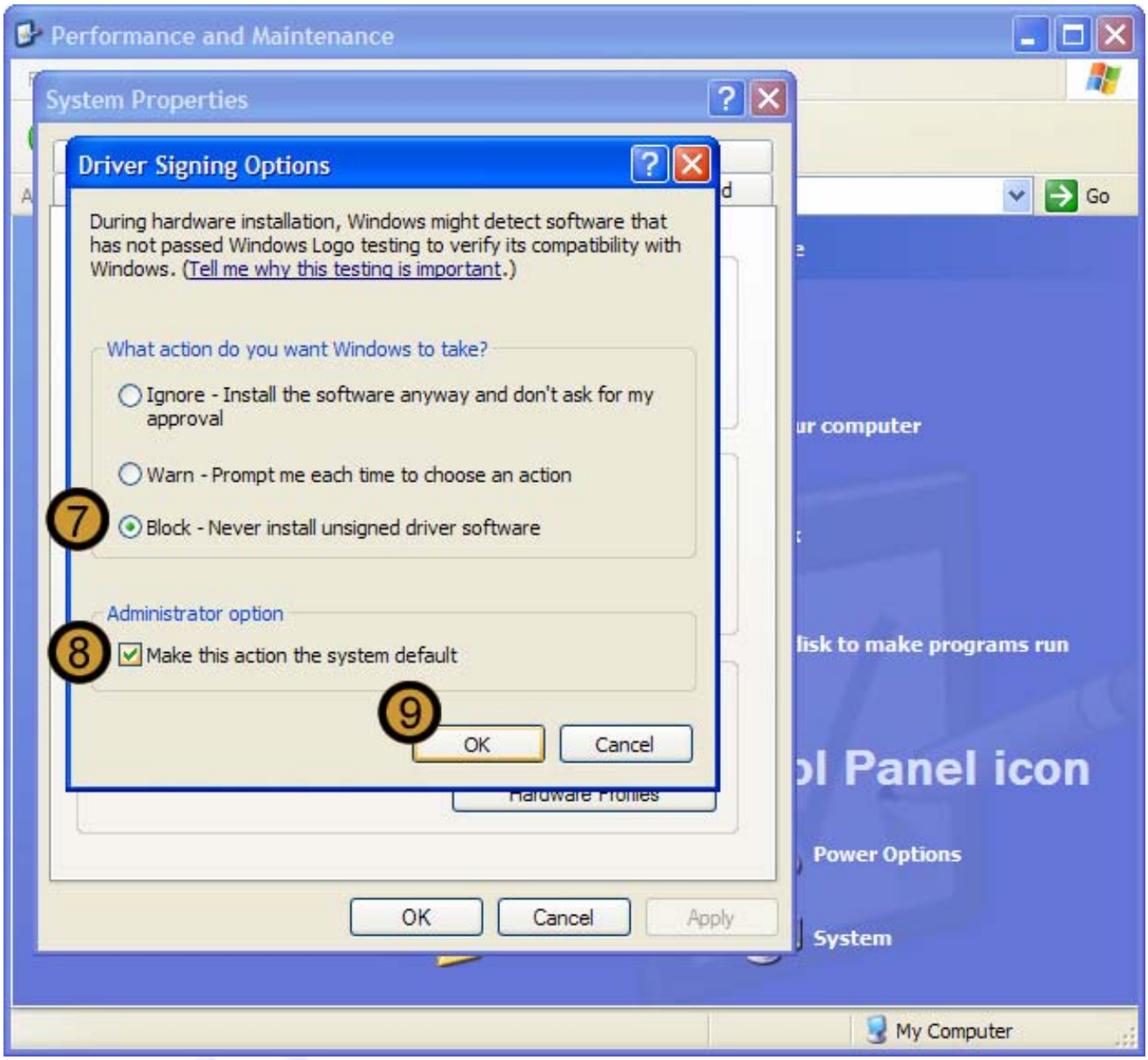
4. In PERFORMANCE AND MAINTENANCE, click **SYSTEM**



The SYSTEM PROPERTIES dialog box appears

5. In SYSTEM PROPERTIES dialog box, click on the **HARDWARE** tab

6. In the DEVICE MANAGER section, click **DRIVER SIGNING**

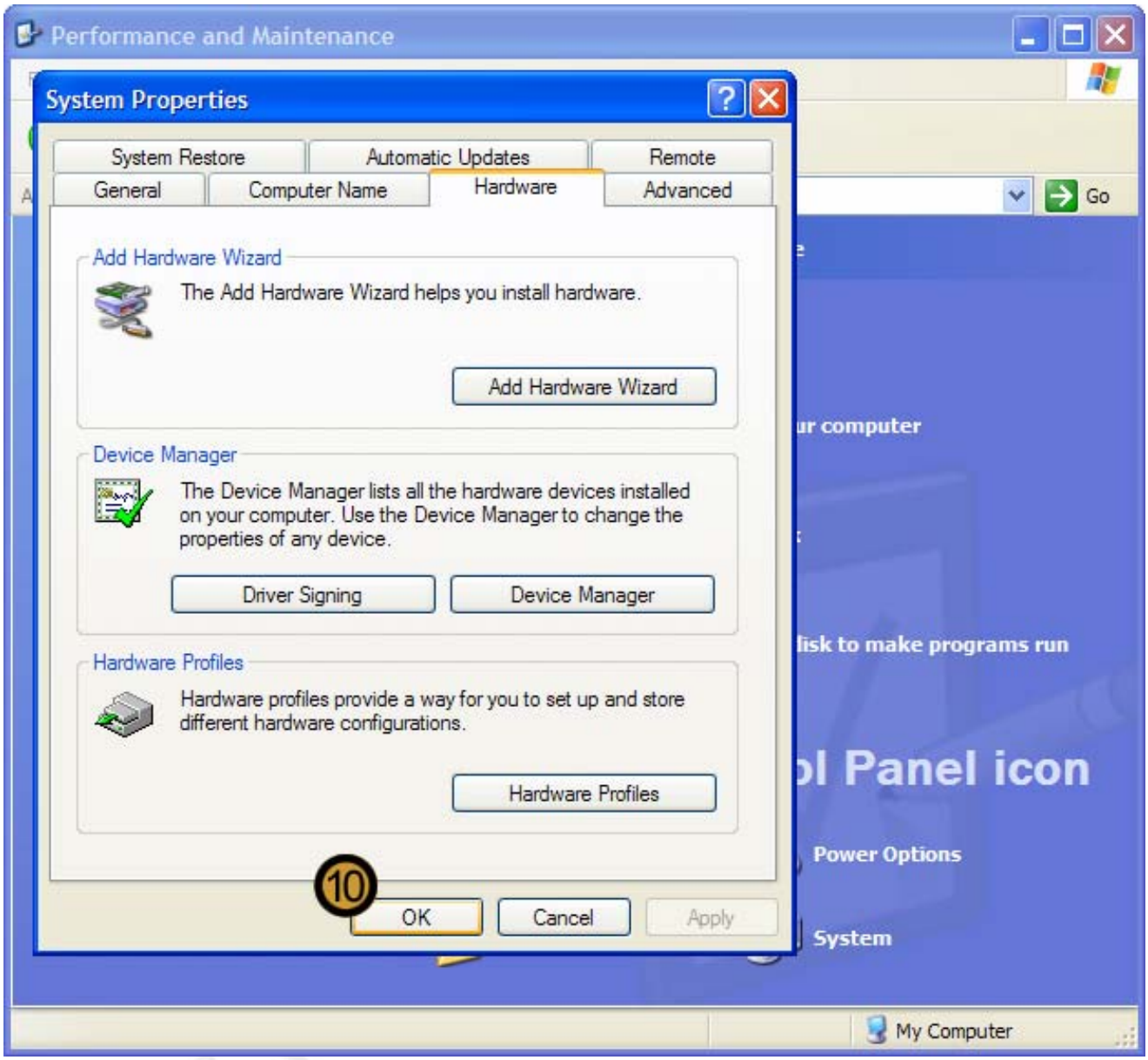


The DRIVER SIGNING OPTIONS dialog box appears

7. In DRIVER SIGNING OPTIONS dialog box, select the DRIVER SIGNING OPTION that you want to implement by clicking on the appropriate radio button

8. Select the **MAKE THIS ACTION THE SYSTEM DEFAULT** check box

9. Click **OK**

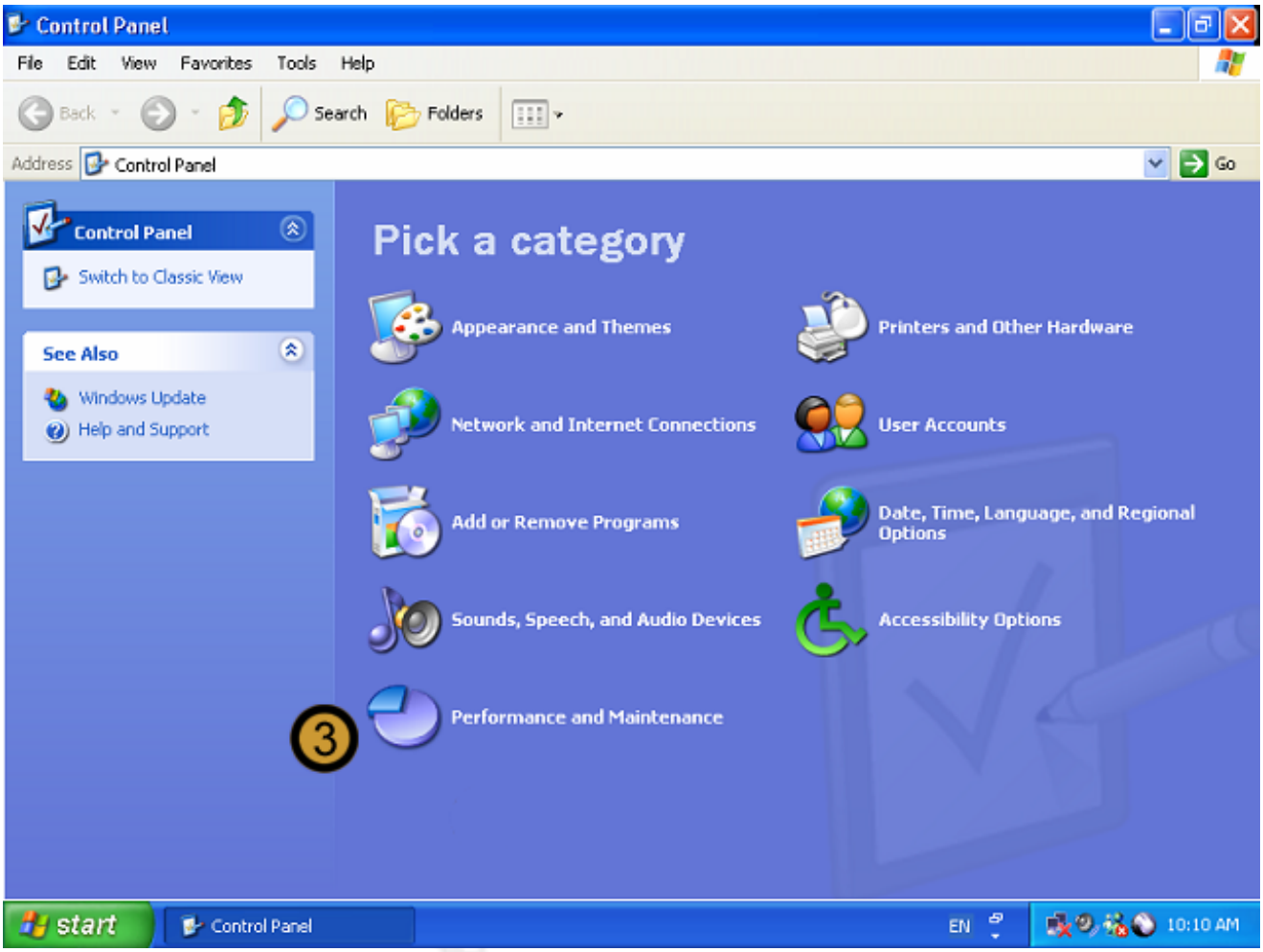


10. Close the SYSTEM PROPERTIES dialog box by clicking **OK**

9.6.3 Using Driver Roll Back

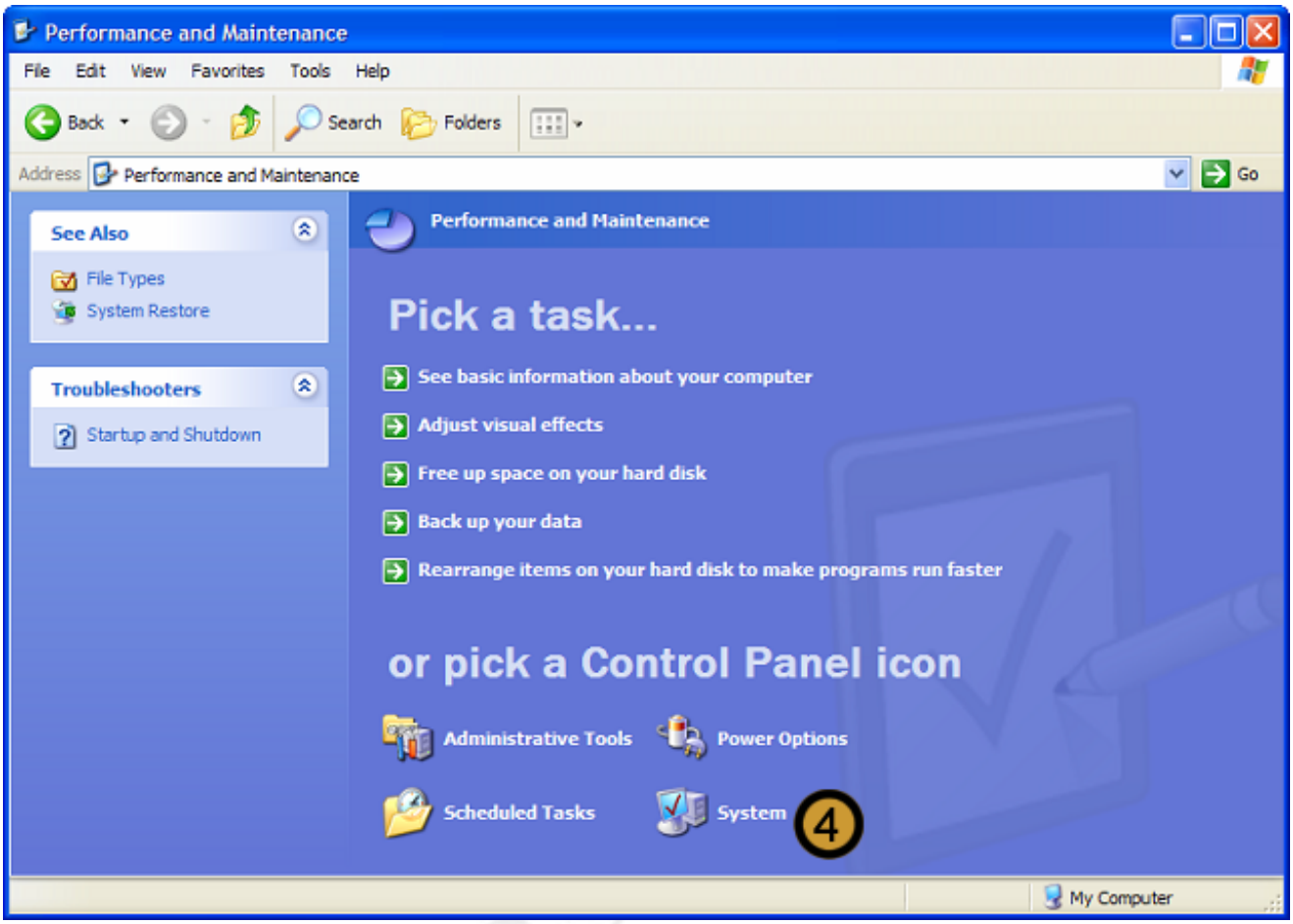
1. Click on the **START** button

2. Click on **CONTROL PANEL**

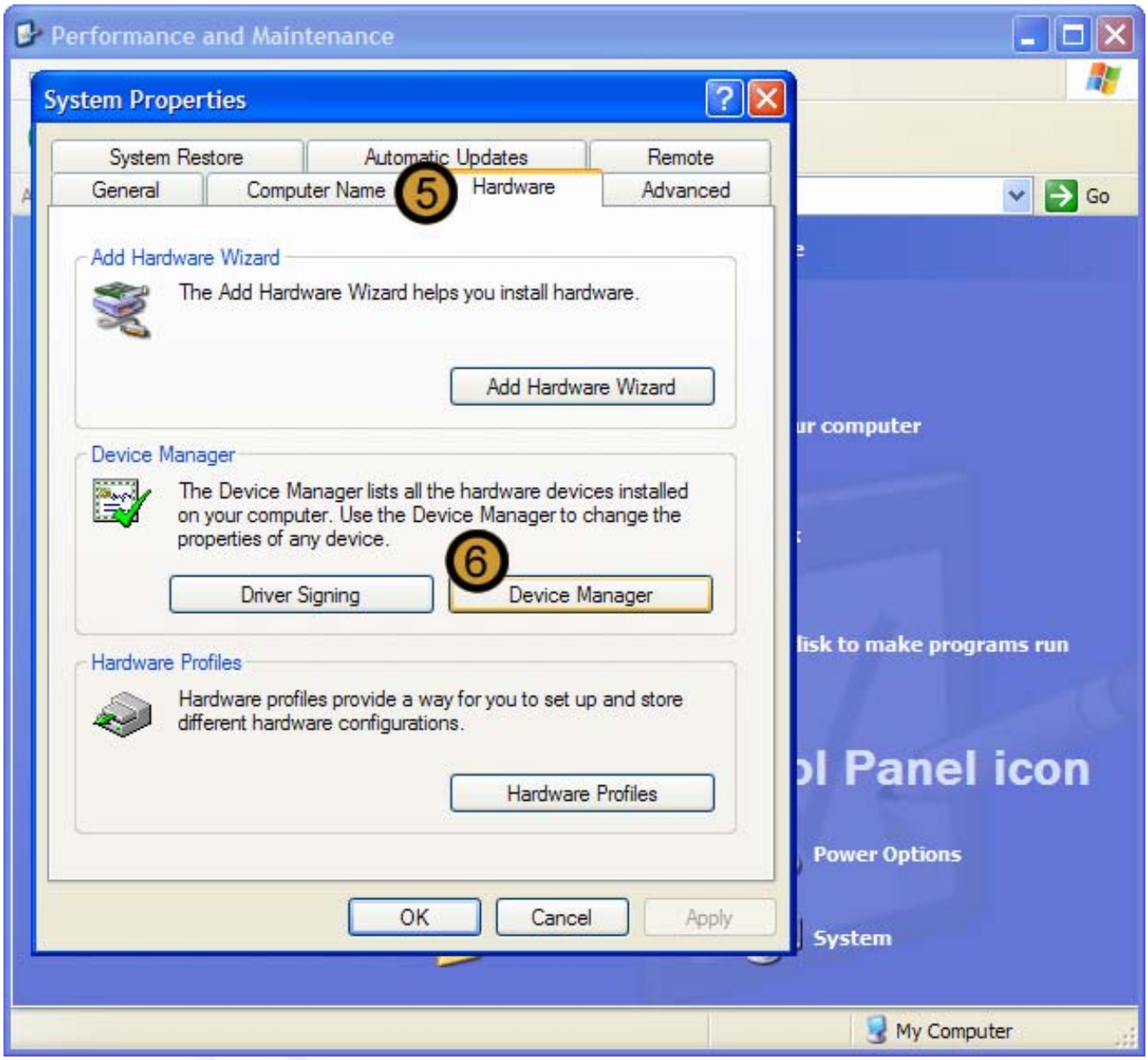


The **Control Panel** appears

3. In the CONTROL PANEL, click on the **PERFORMANCE AND MAINTENANCE** icon



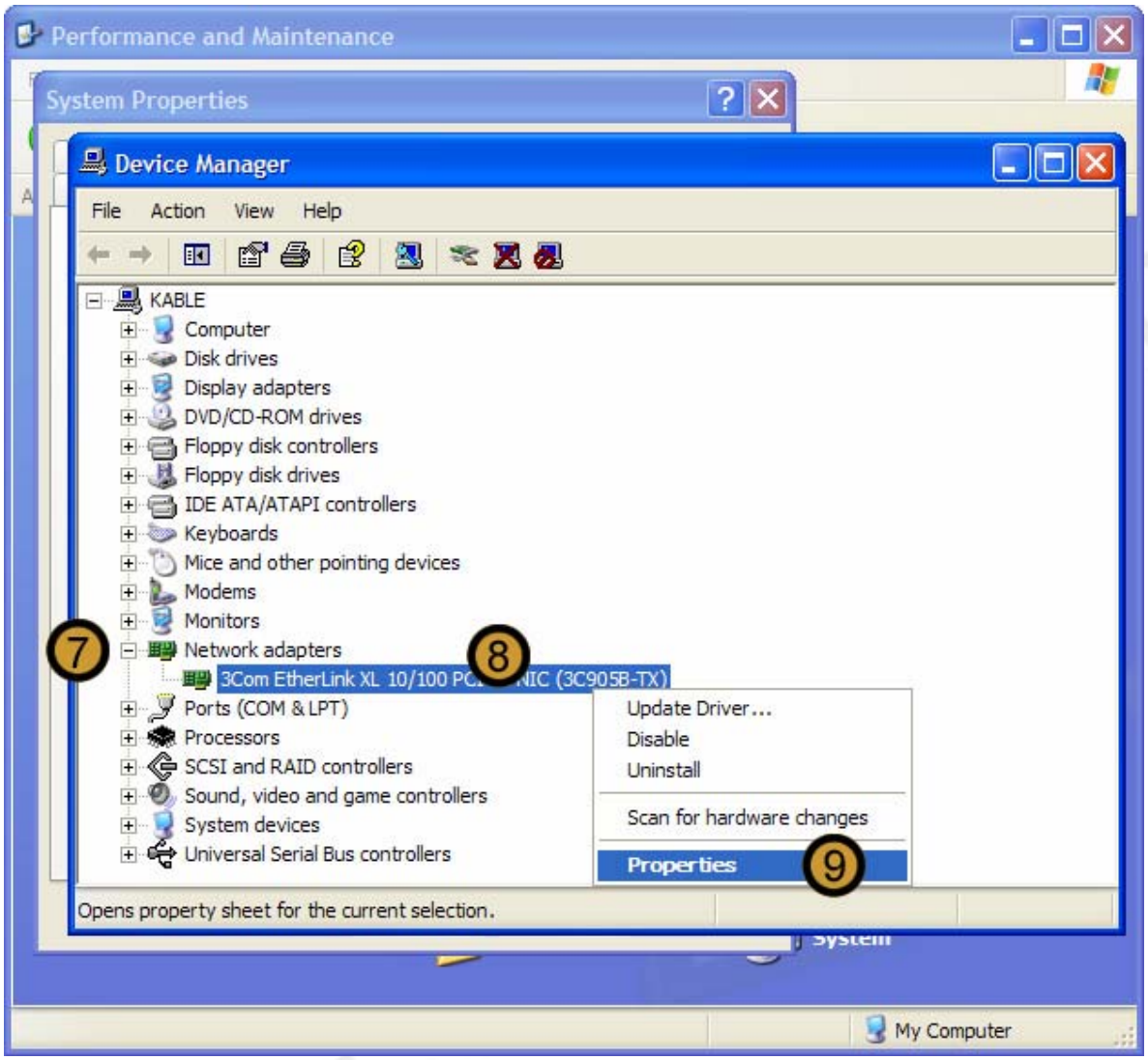
4. In PERFORMANCE AND MAINTENANCE, click **SYSTEM**



The SYSTEM PROPERTIES dialog box appears

5. In SYSTEM PROPERTIES dialog box, click on the **HARDWARE** tab

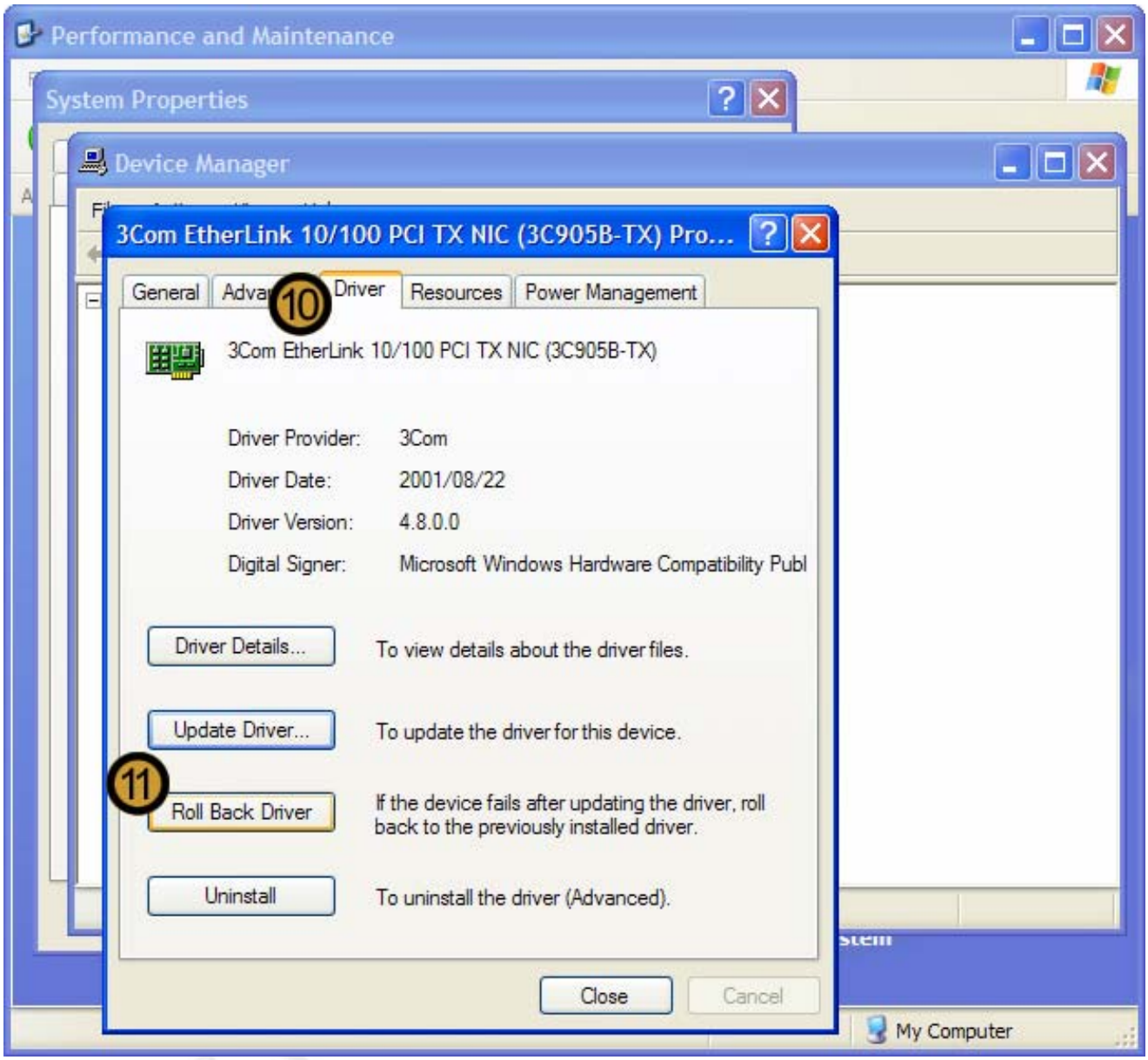
6. In the DEVICE MANAGER section, click **DEVICE MANAGER**



7. In the DEVICE MANAGER, expand the Hardware for which you want to Rollback the driver

8. Right-click device for which you want to Rollback the driver

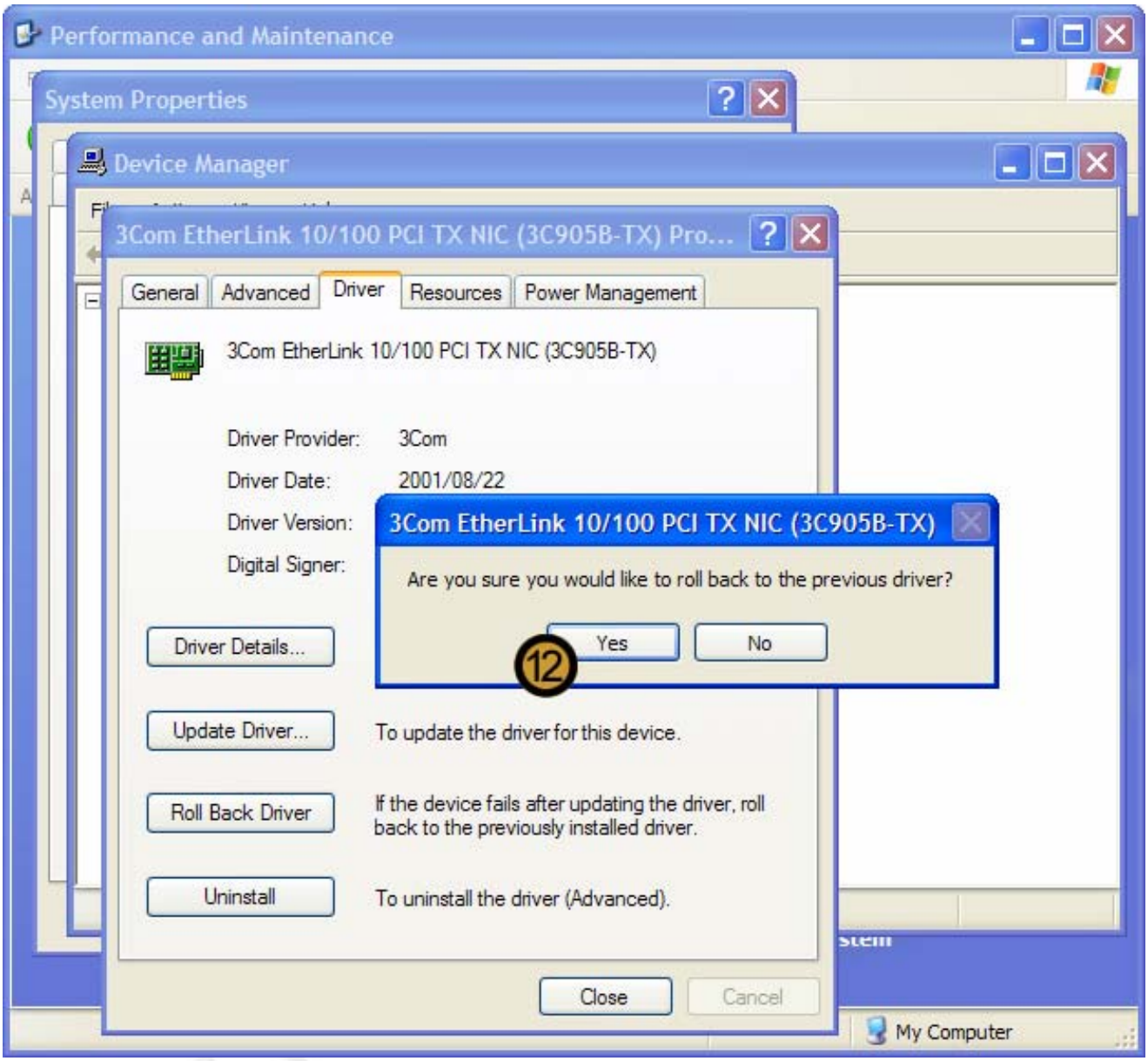
9. On the menu that drops down, click **PROPERTIES**



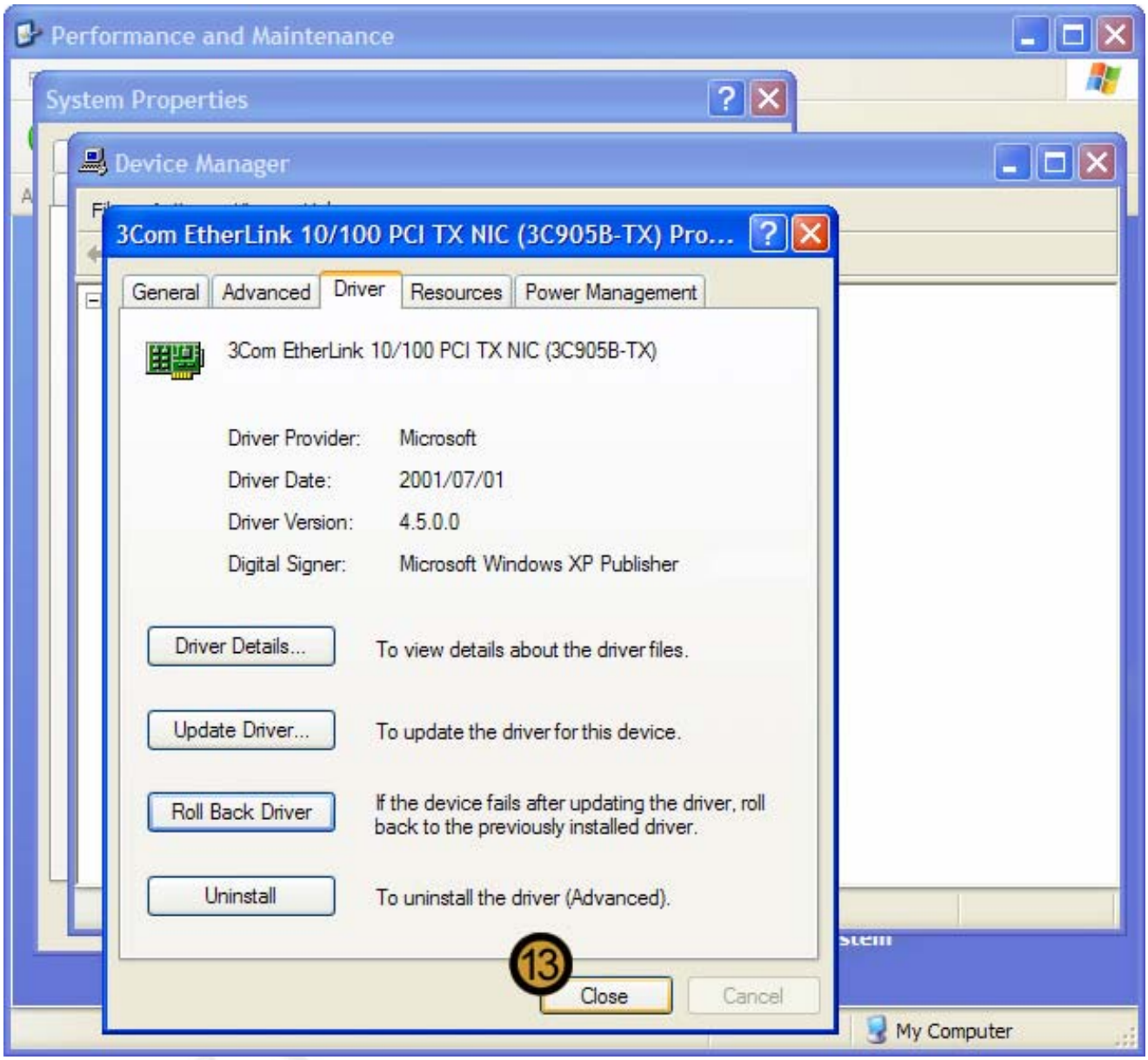
The selected DEVICE PROPERTIES dialog box appears

10. On the selected DEVICE PROPERTIES dialog box, click the **DRIVER** tab

11. Click **ROLL BACK DRIVER**



12. Confirm that you want to Roll back the device driver for the specified device by clicking **YES**

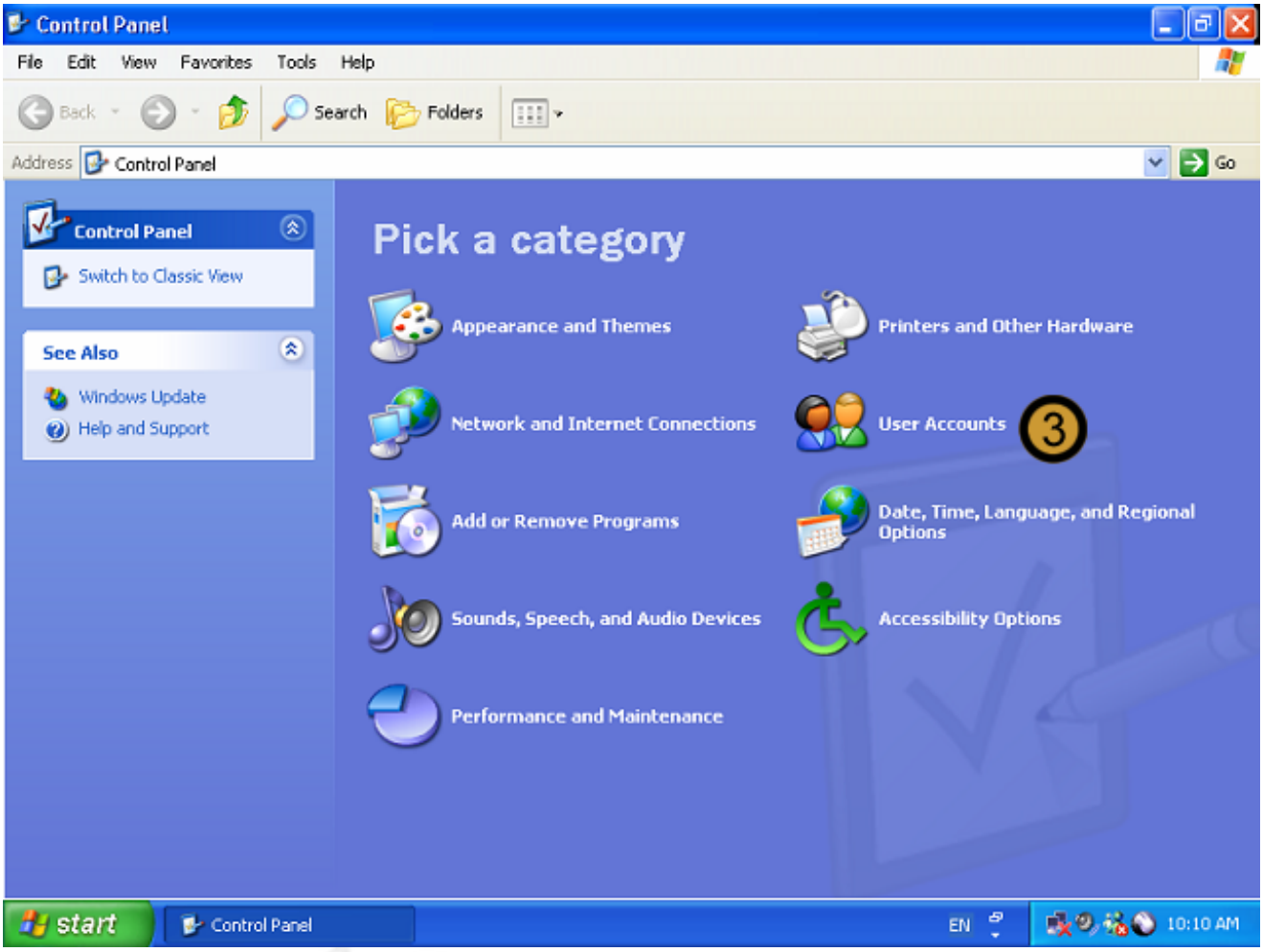


13. Close the selected DEVICE PRPERTIES dialog box by clicking **CLOSE**

9.7 Creating New User Accounts
9.7.1 Using User Accounts

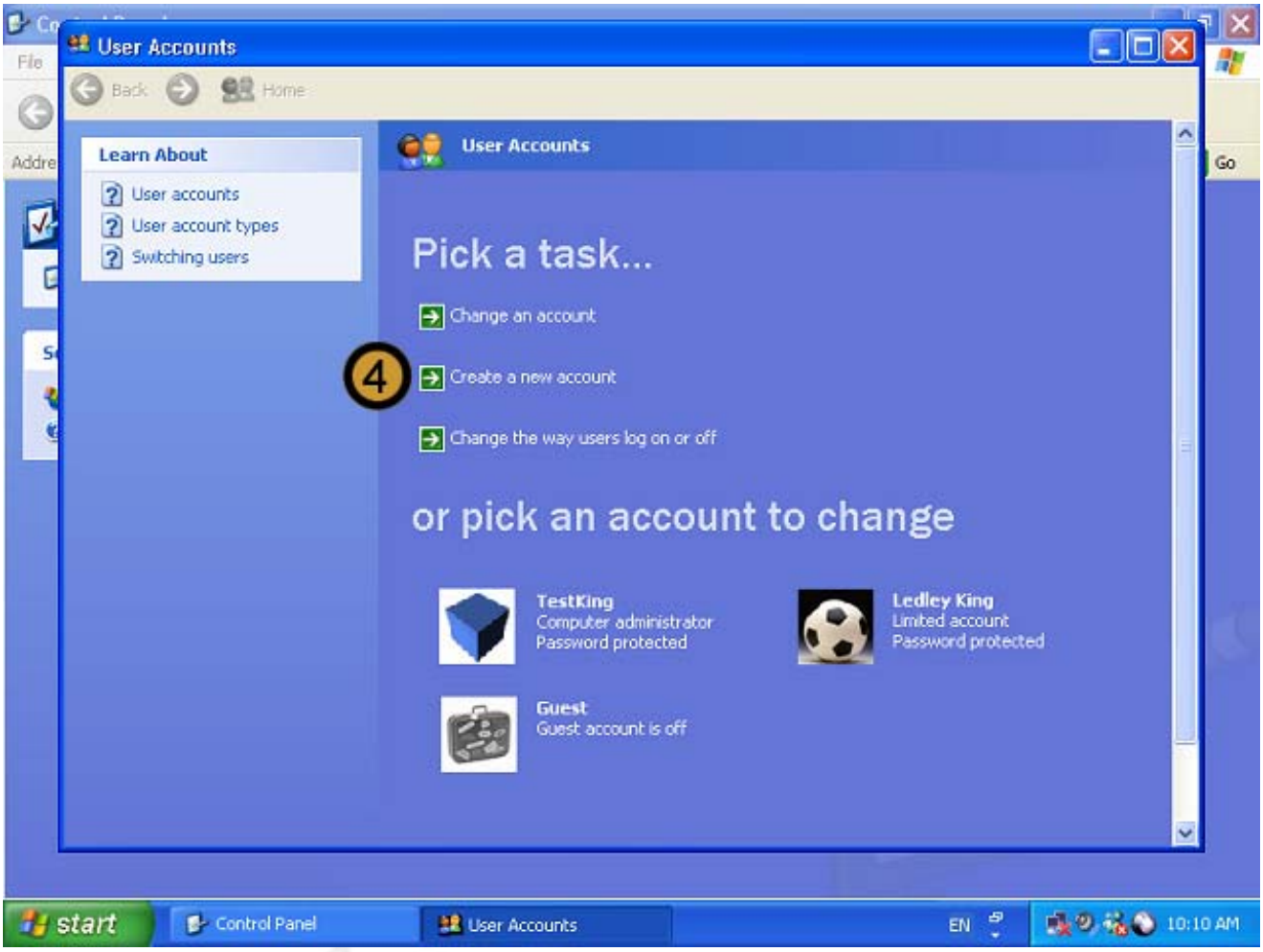
1. Click on the **START** button

2. Click on **CONTROL PANEL**

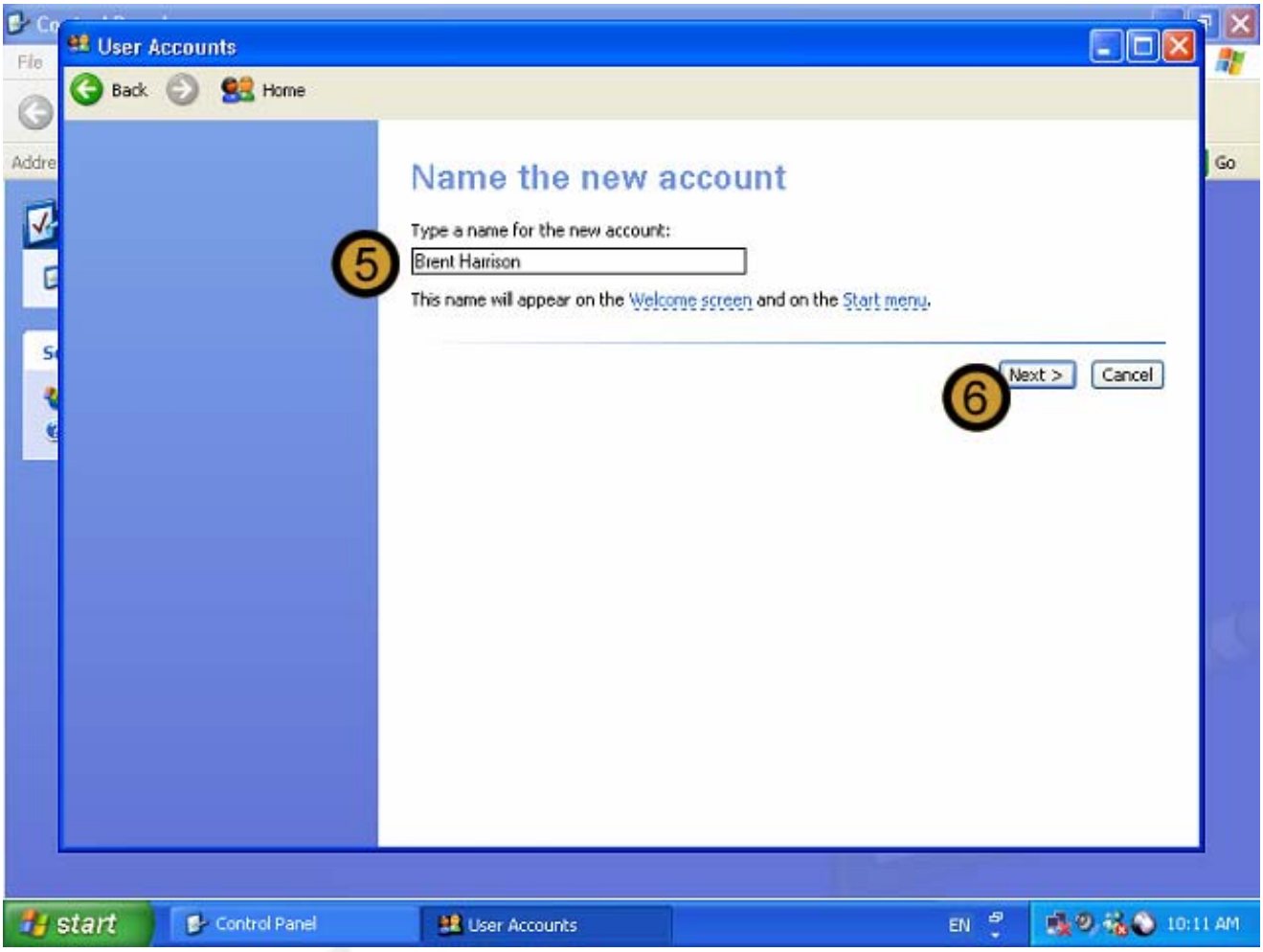


The Control Panel appears

3. In the CONTROL PANEL, click on the **USER ACCOUNTS** icon

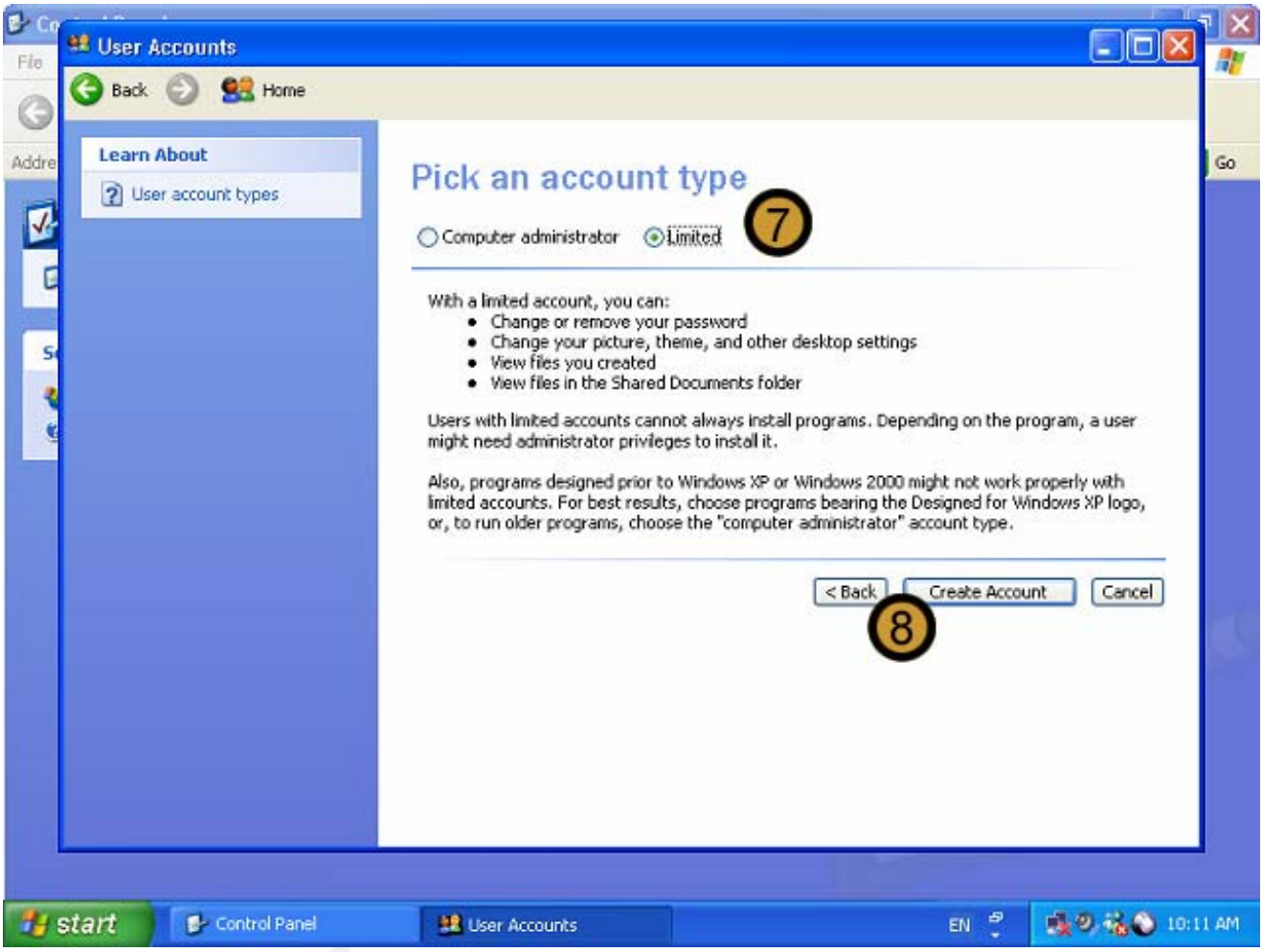


4. In USER ACCOUNTS, click **CREATE A NEW USER ACCOUNT**



5. Provide the new account **name**

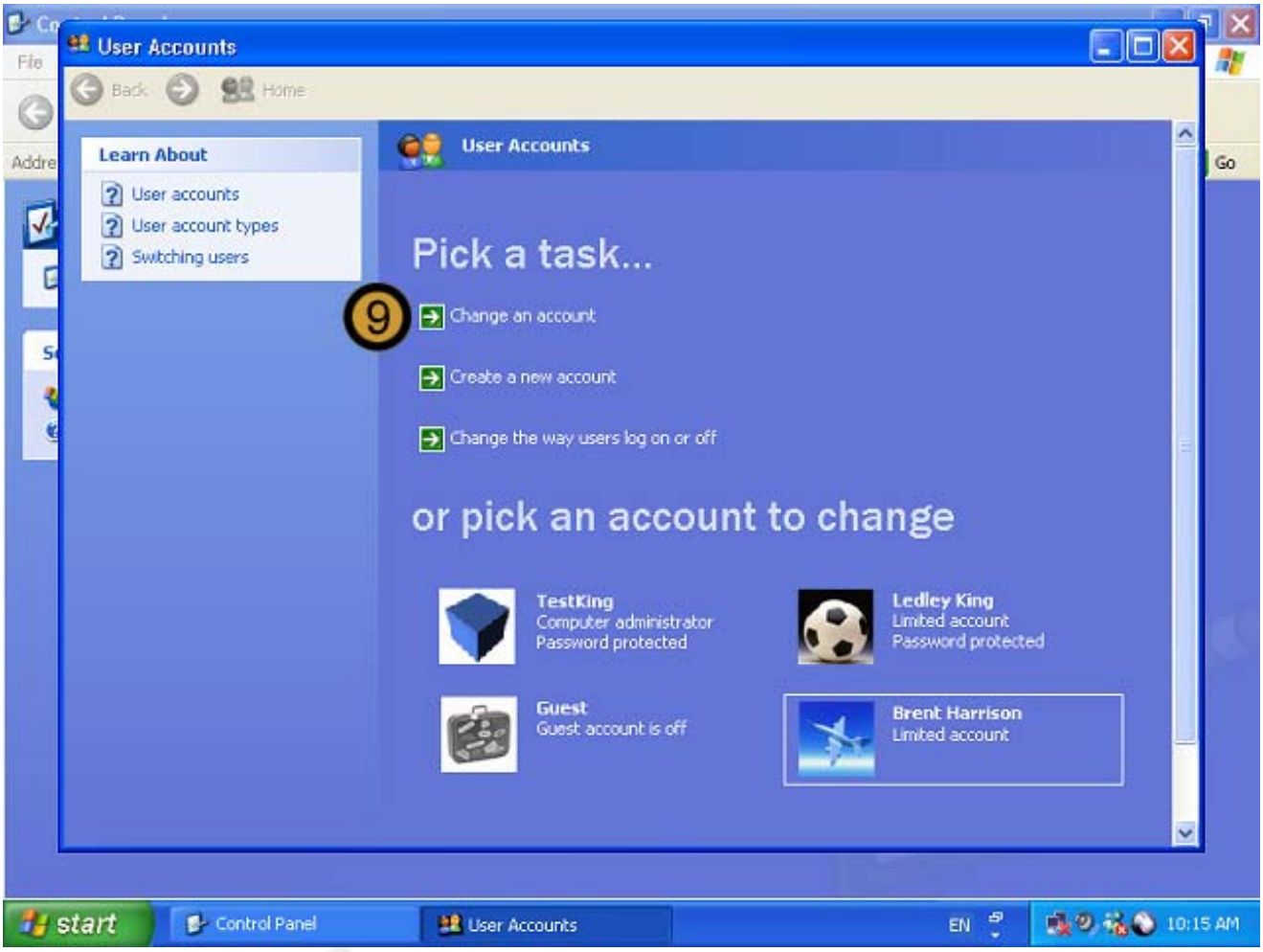
6. Click **NEXT**



7. Choose the **Account Type** that you want to create. In this example we are not creating a Administrator Account

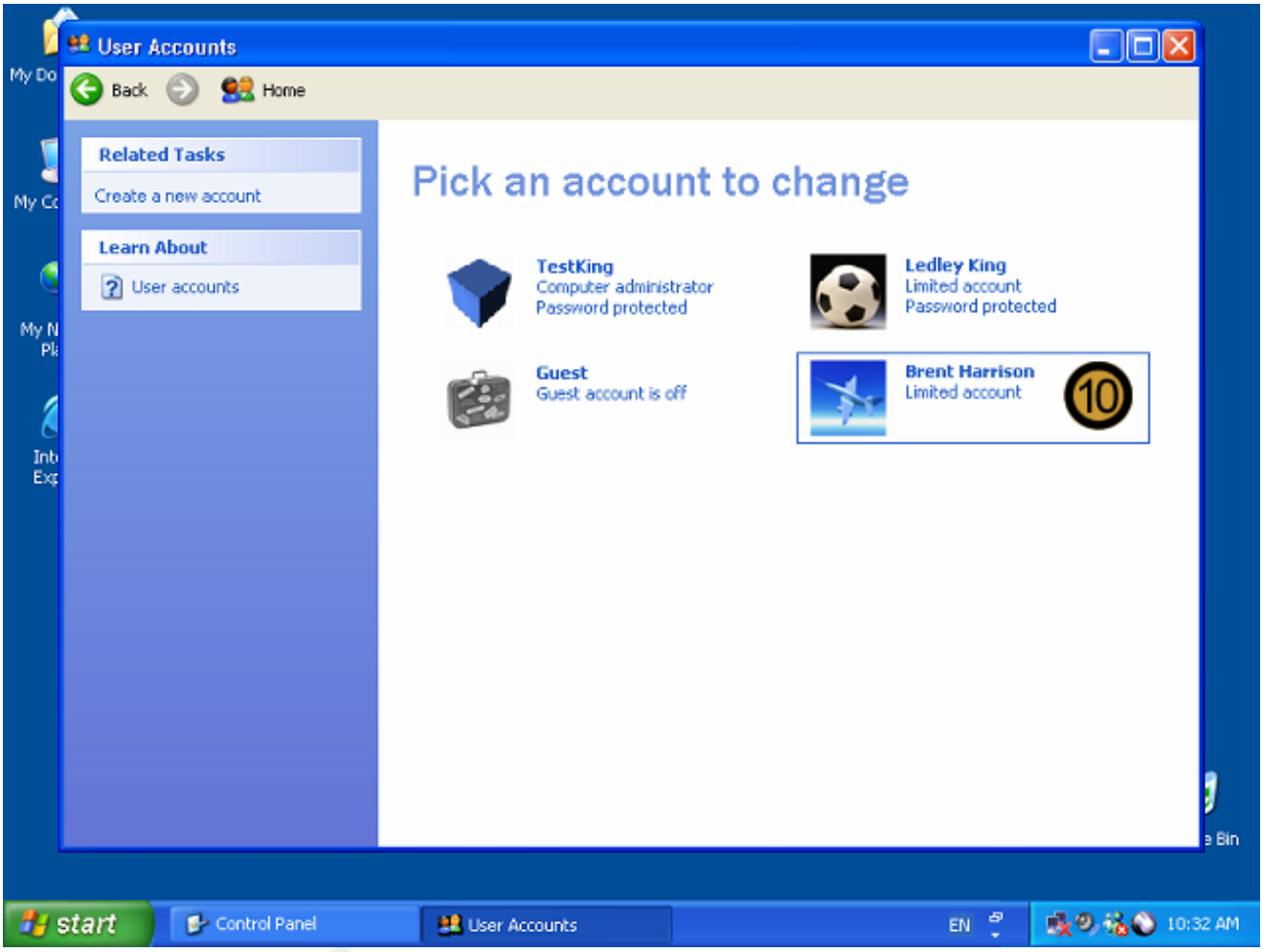
8. Click on the **CREATE ACCOUNT** button

At this point the account is created without a password

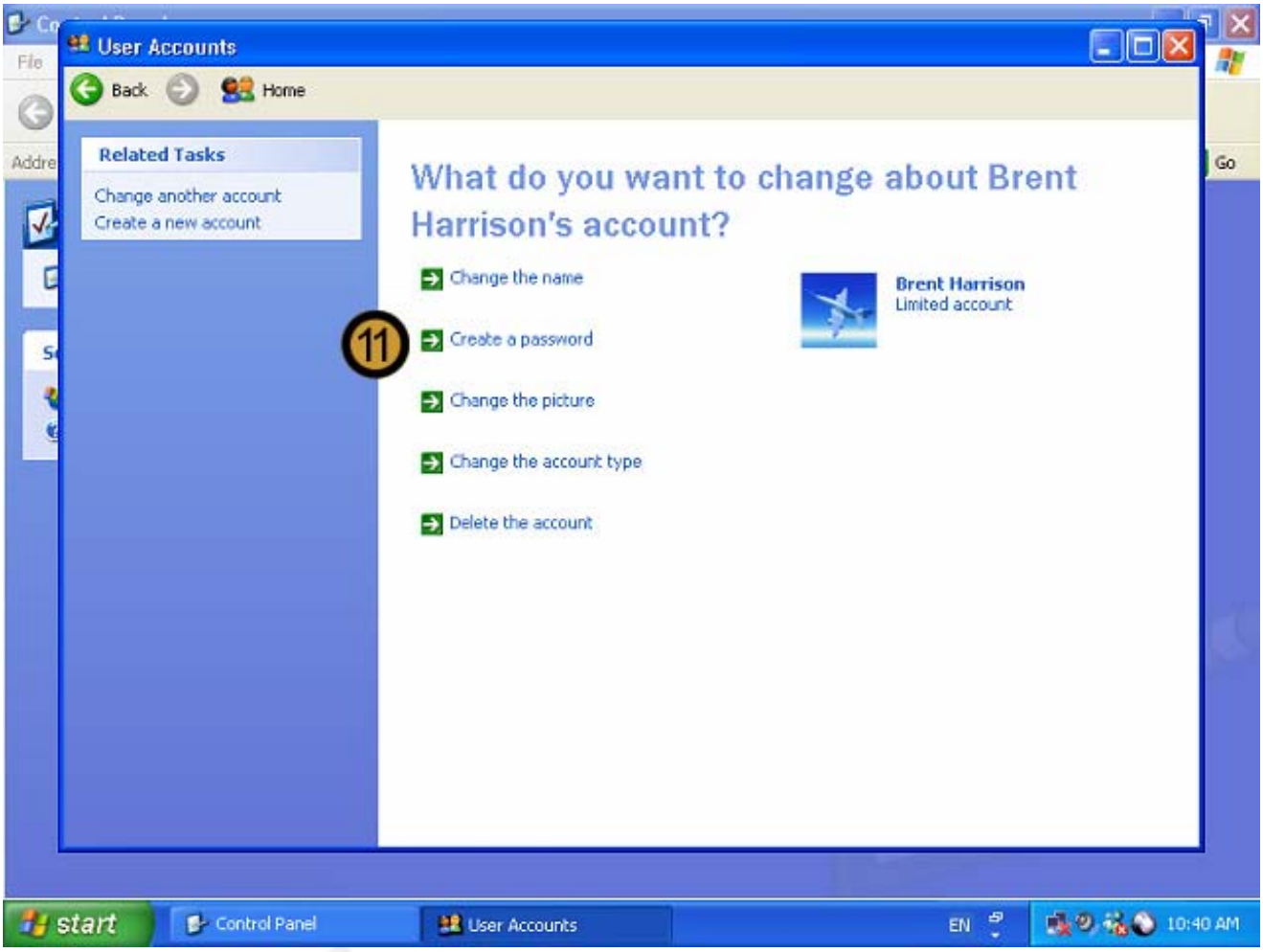


To set a temporary password for the account

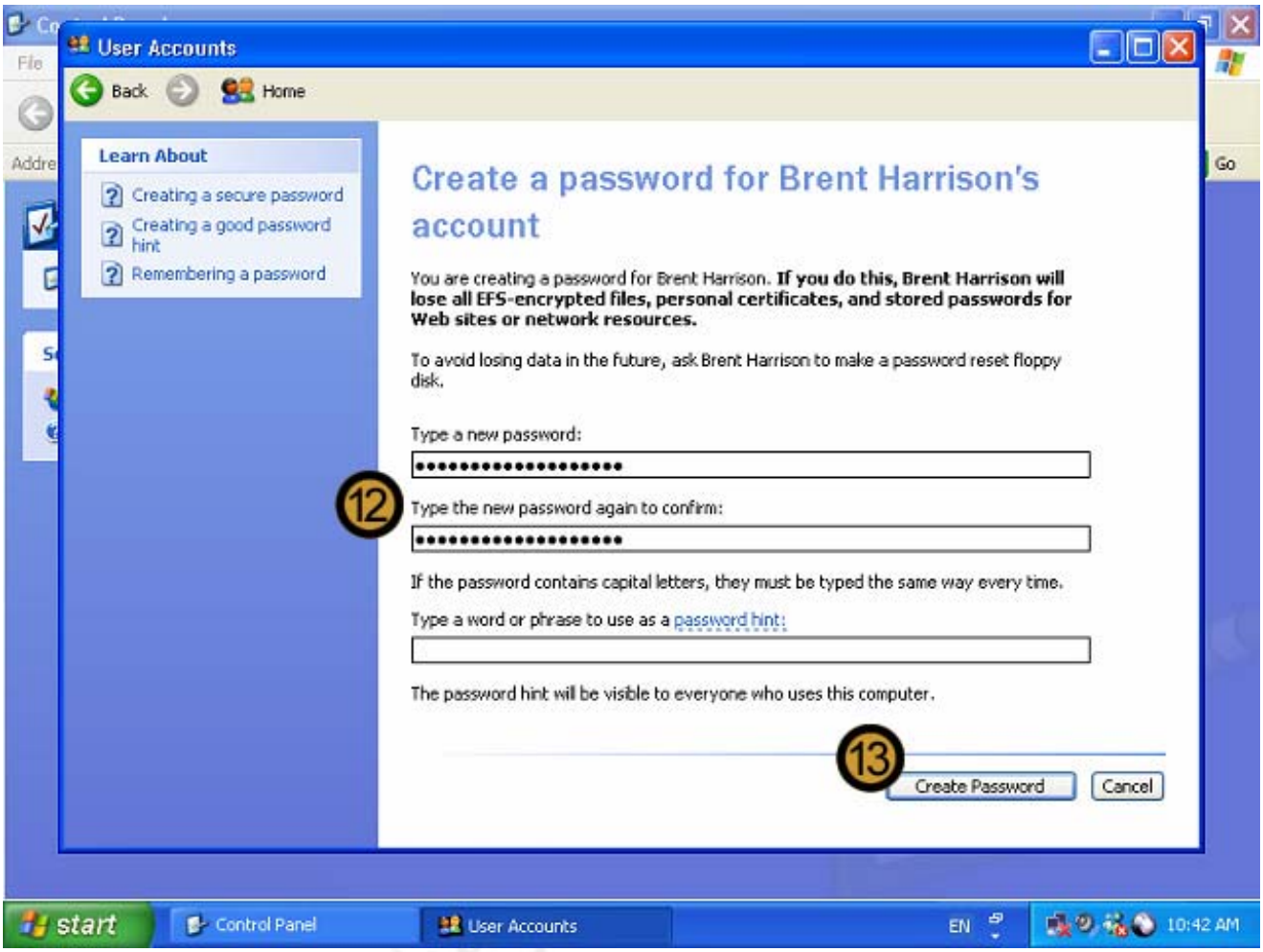
9. On the USER ACCOUNTS dialog box, click **CHANGE AN ACCOUNT**



10. Double-click on the USER ACCOUNT that you want to set a password for.

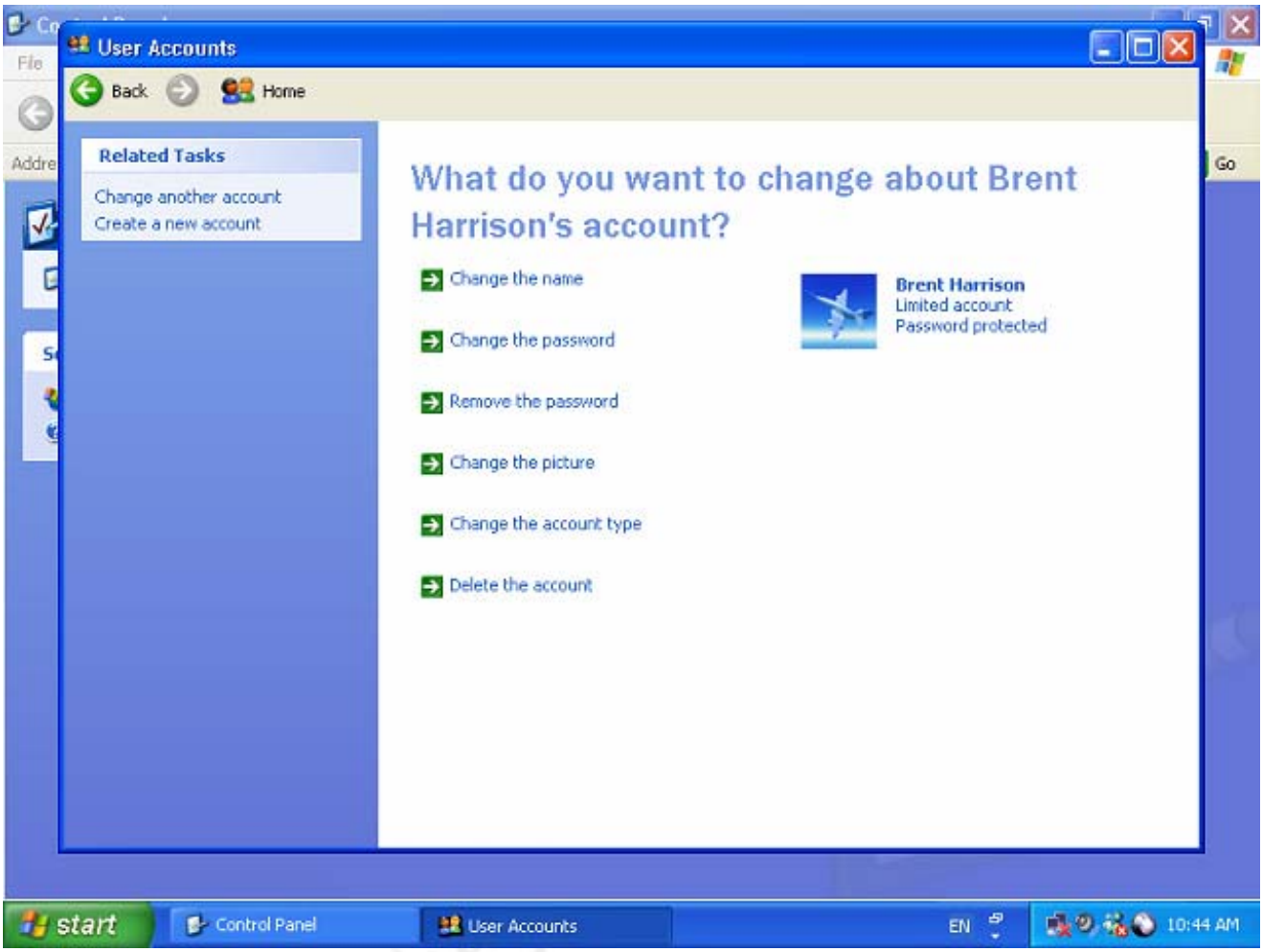


11. Click on **CREATE A PASSWORD**



12. Provide and confirm the **Password**

13. Click **CREATE PASSWORD**

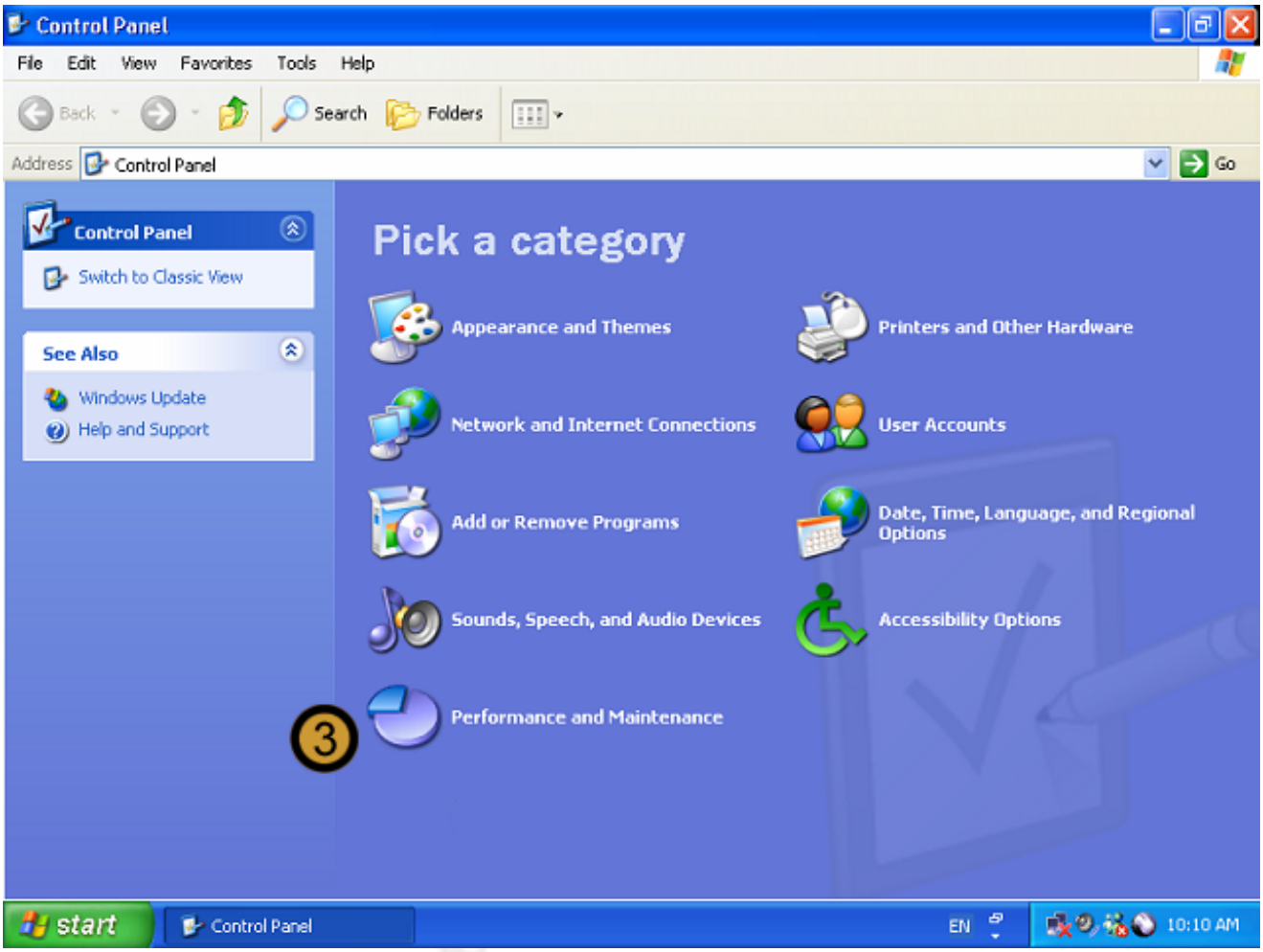


The new user account is now password protected

9.7.2 Using Computer Management

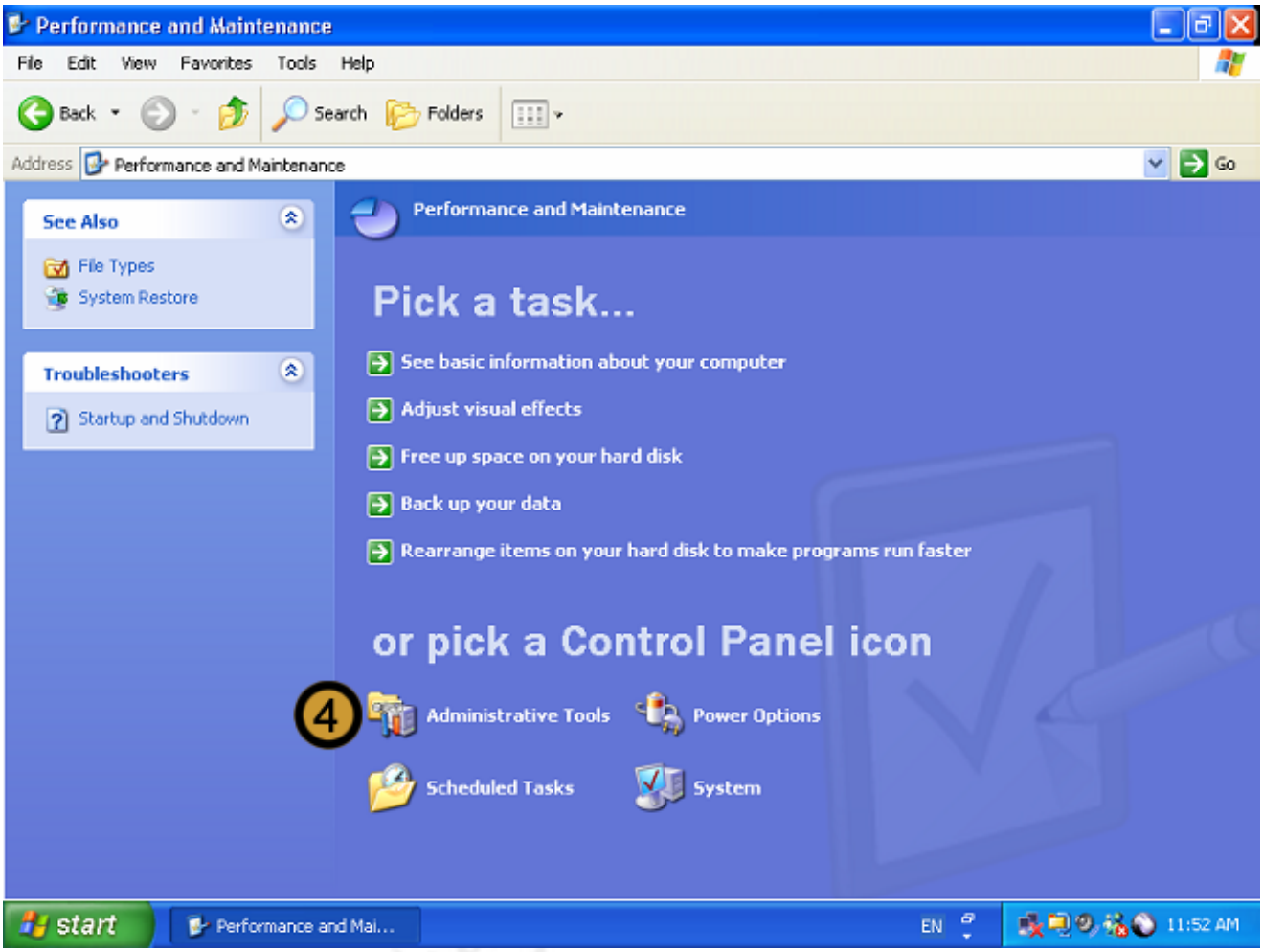
1. Click on the **START** button

2. Click on **CONTROL PANEL**



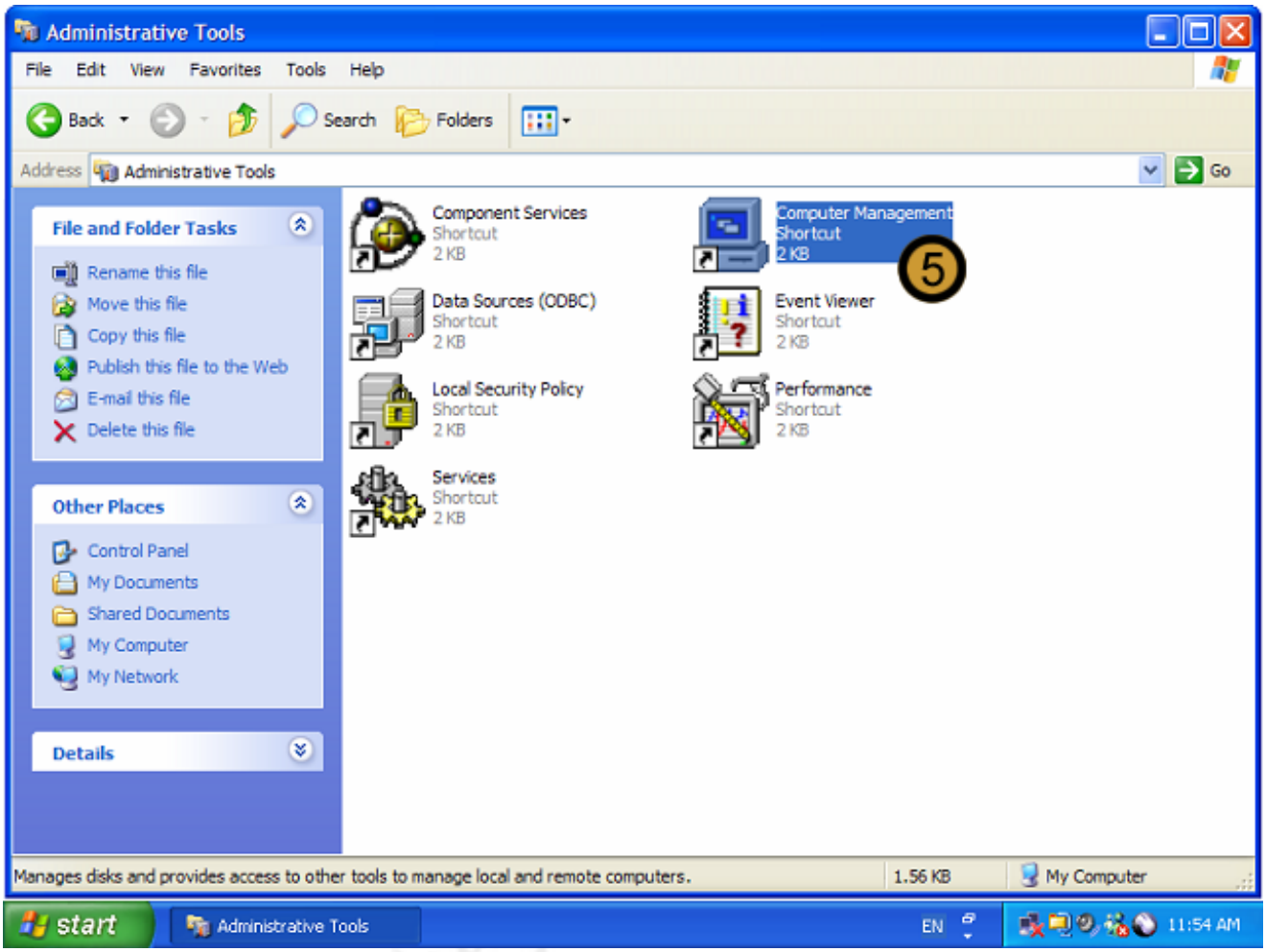
The **Control Panel** appears

3. In the CONTROL PANEL, click on the **PERFORMANCE AND MAINTENANCE** icon



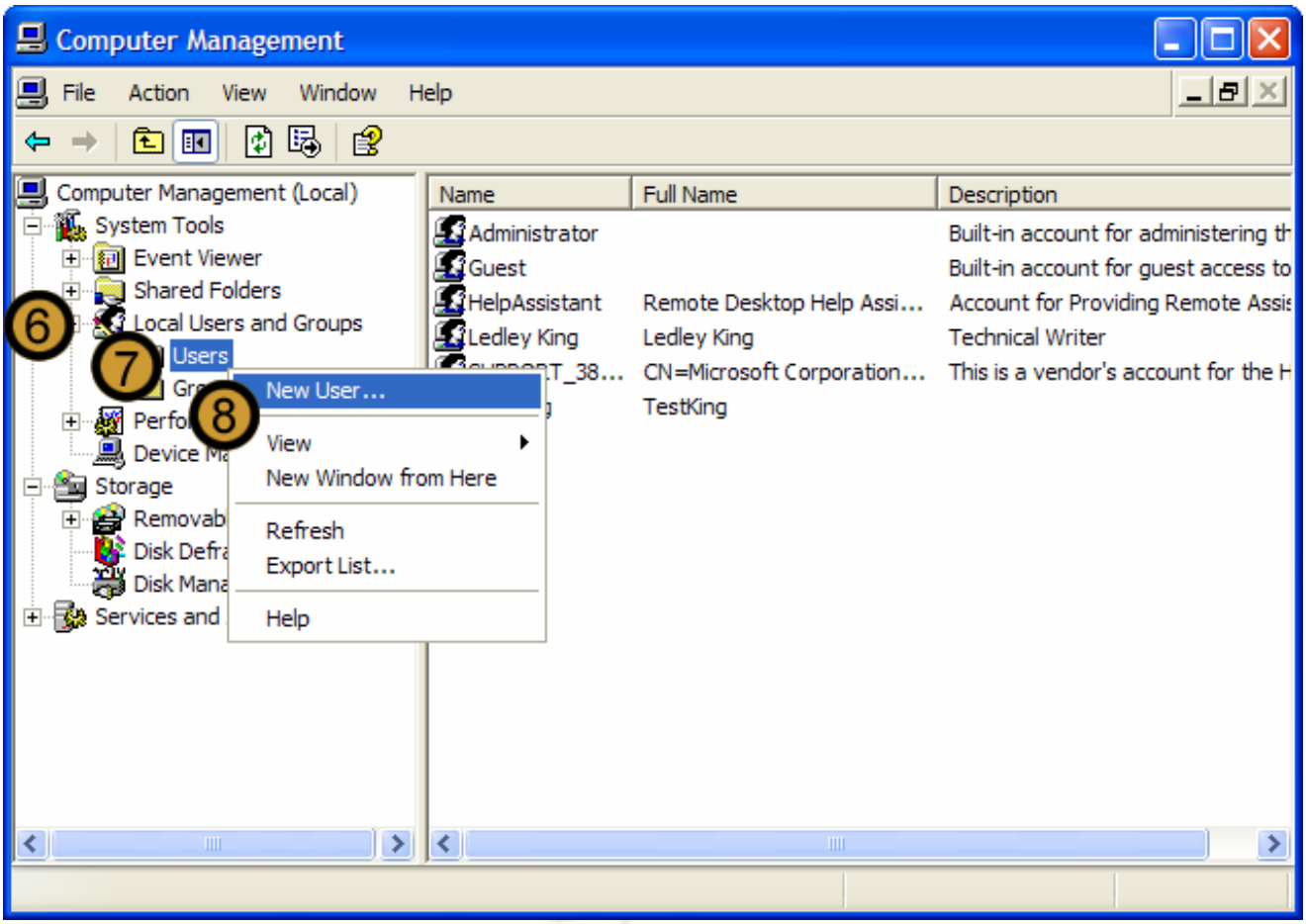
The **Performance and Maintenance** dialog box appears

4. In the PERFORMANCE AND MAINTENANCE dialog box, click **ADMINISTRATIVE TOOLS**



The Windows XP Professional **Administrative Tools** appears

5. In ADMINISTRATIVE TOOLS, double-click on the **COMPUTER MANAGEMENT** icon

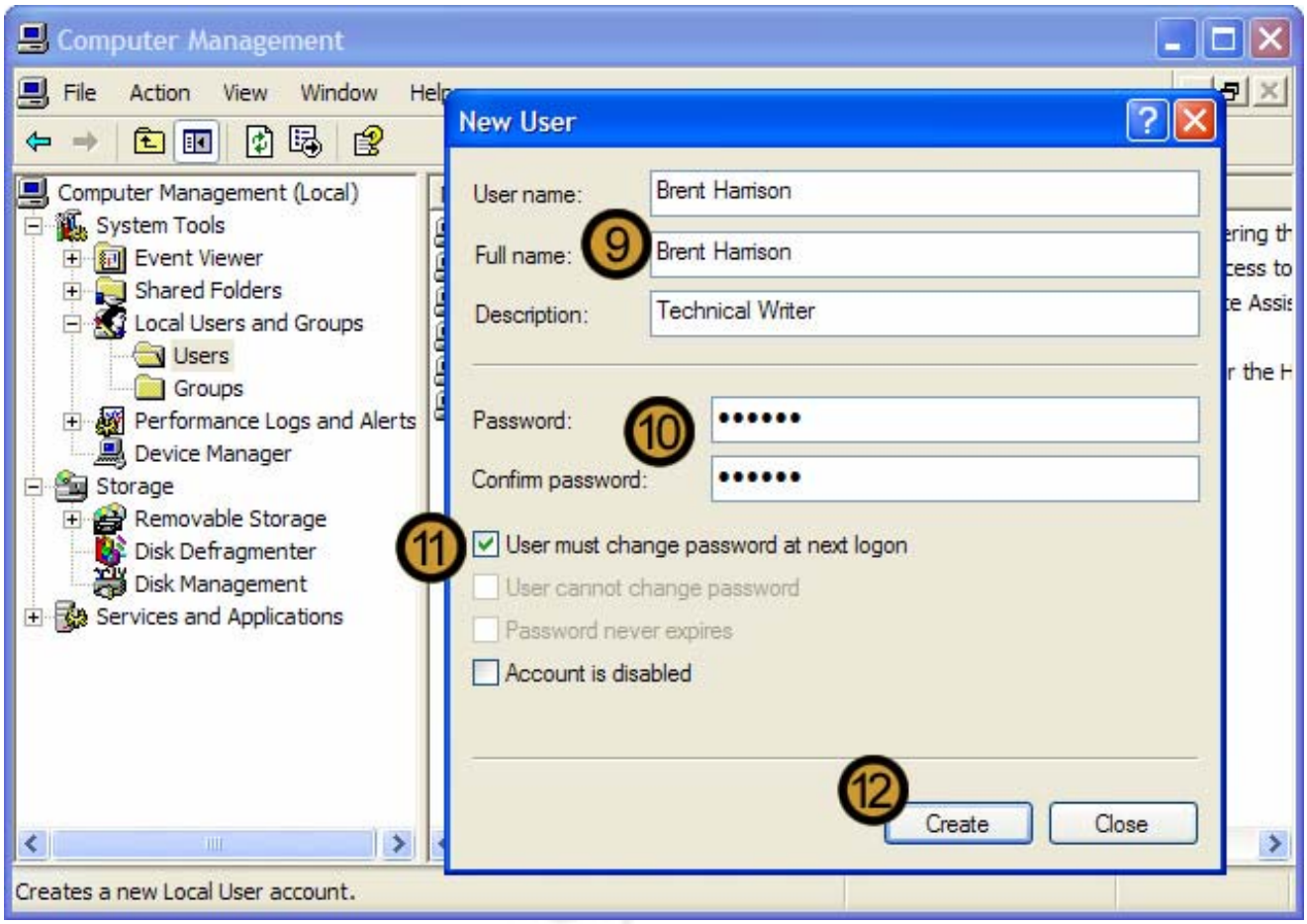


The **Computer Management Console** appears

6. In the COMPUTER MANAGEMENT CONSOLE, expand Local **Users and Groups**

7. Right click **USERS**

8. On the drop down menu that appears, click **NEW USER …**

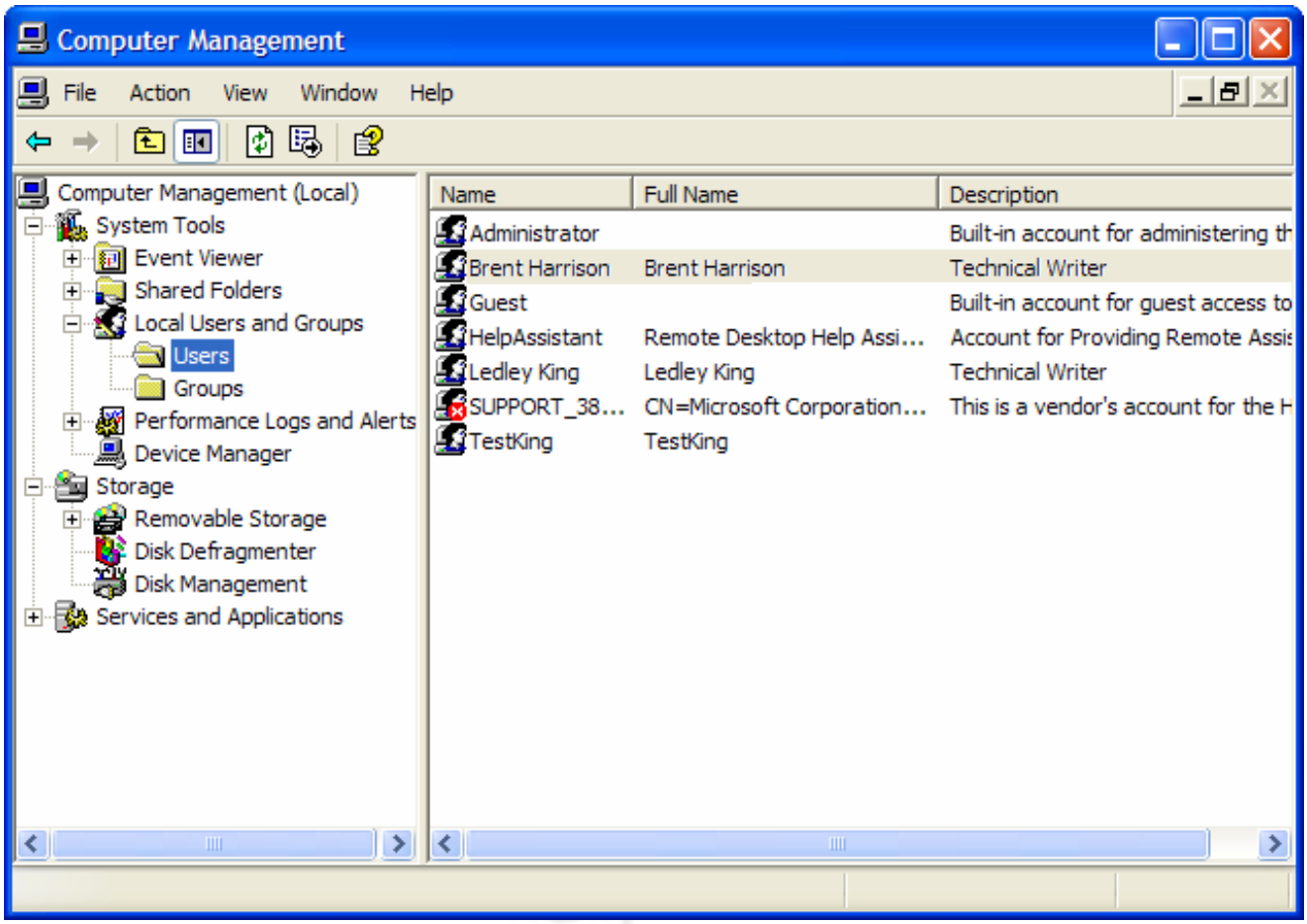


9. In the CONTROL PANEL, click on the **PERFORMANCE AND MAINTENANCE** icon

10. Provide and confirm a **temporary password** and, if you want, provide a description for the account

11. Select the **USER MUST CHANGE PASSWORD AT NEXT LOGON** check box

12. Click **CREATE**

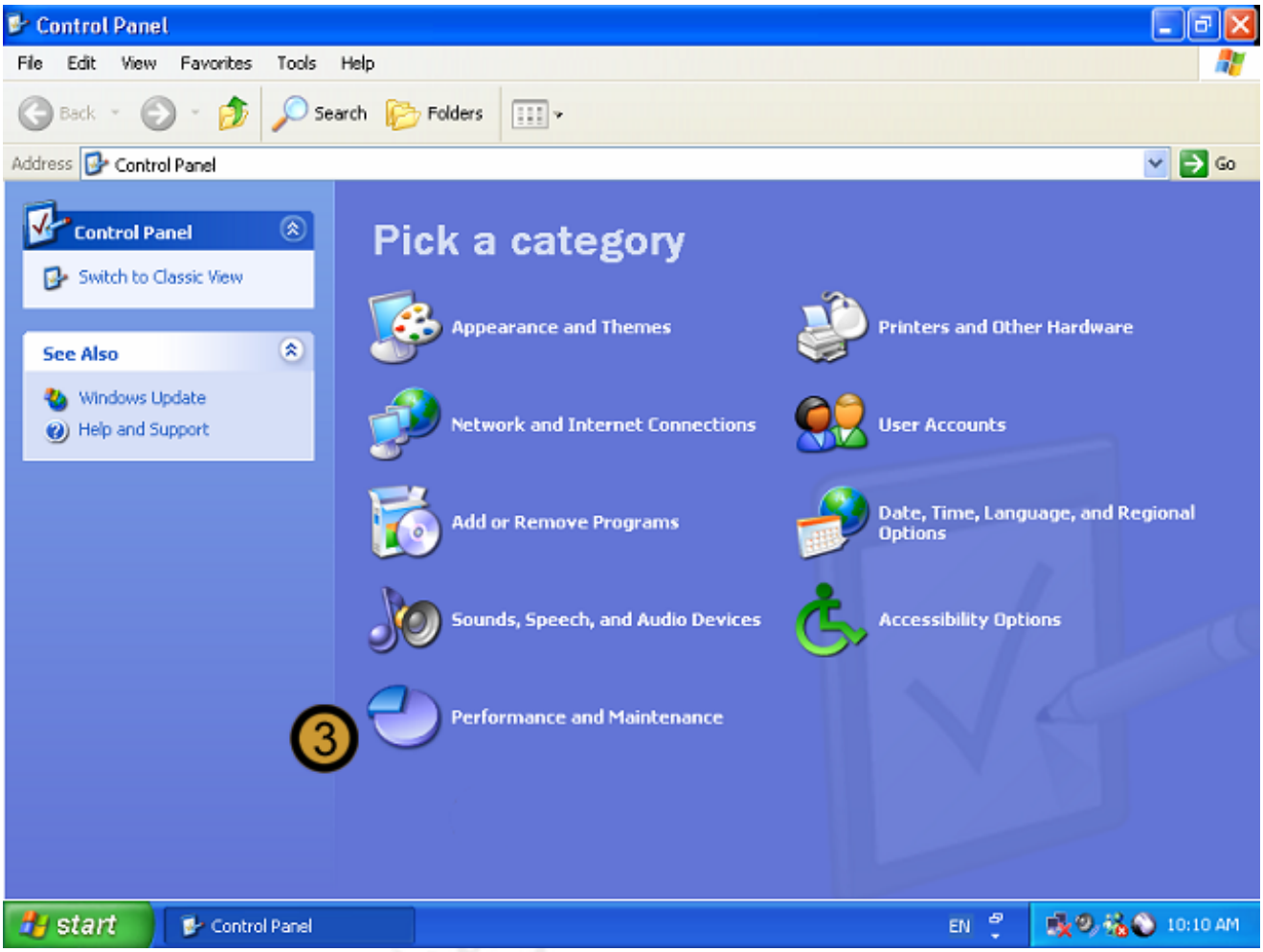


The new user account is created

9.8 Creating User Groups

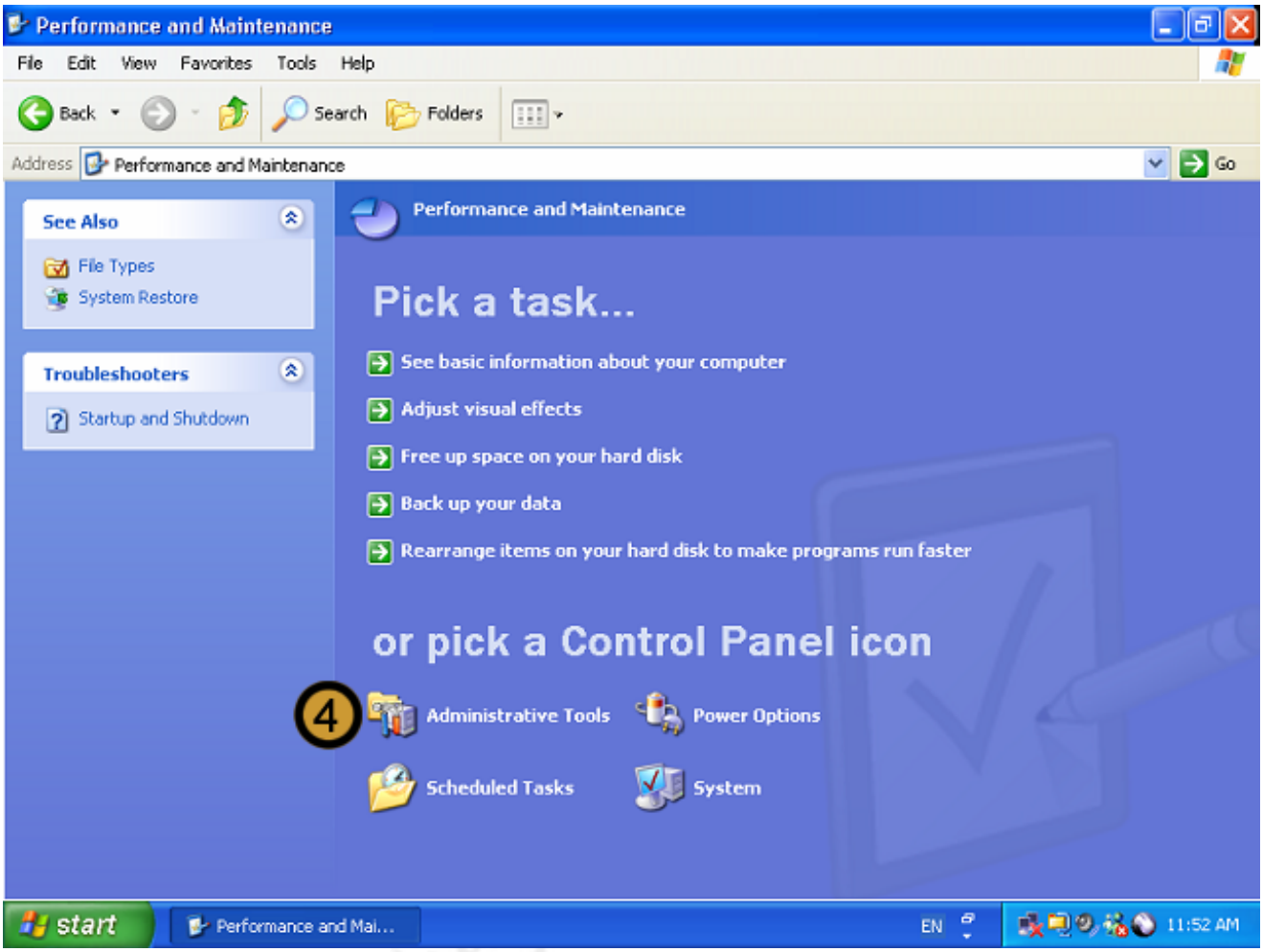
1. Click on the **START** button

2. Click on **CONTROL PANEL**



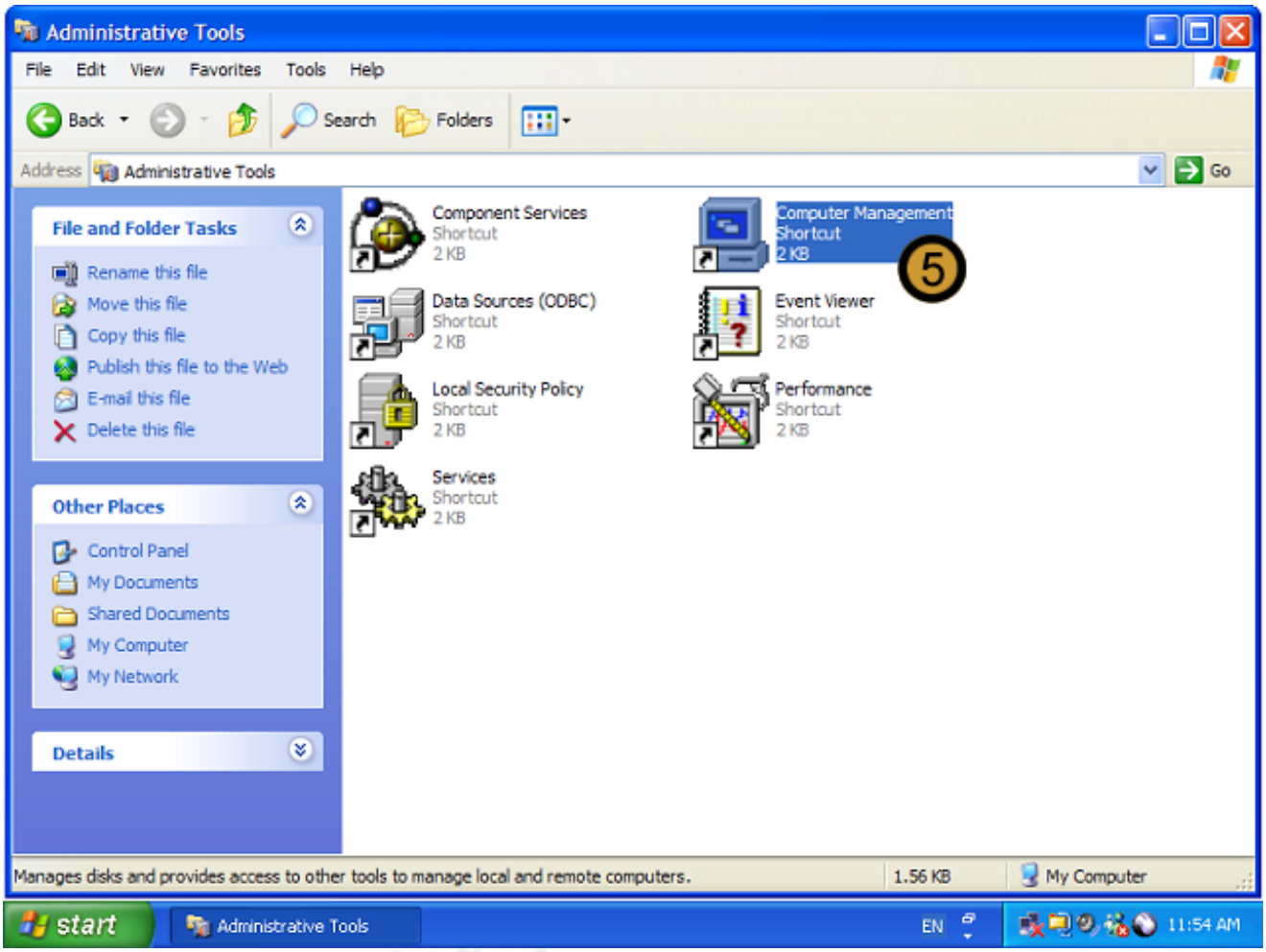
The **Control Panel** appears

3. In the CONTROL PANEL, click on the **PERFORMANCE AND MAINTENANCE** icon



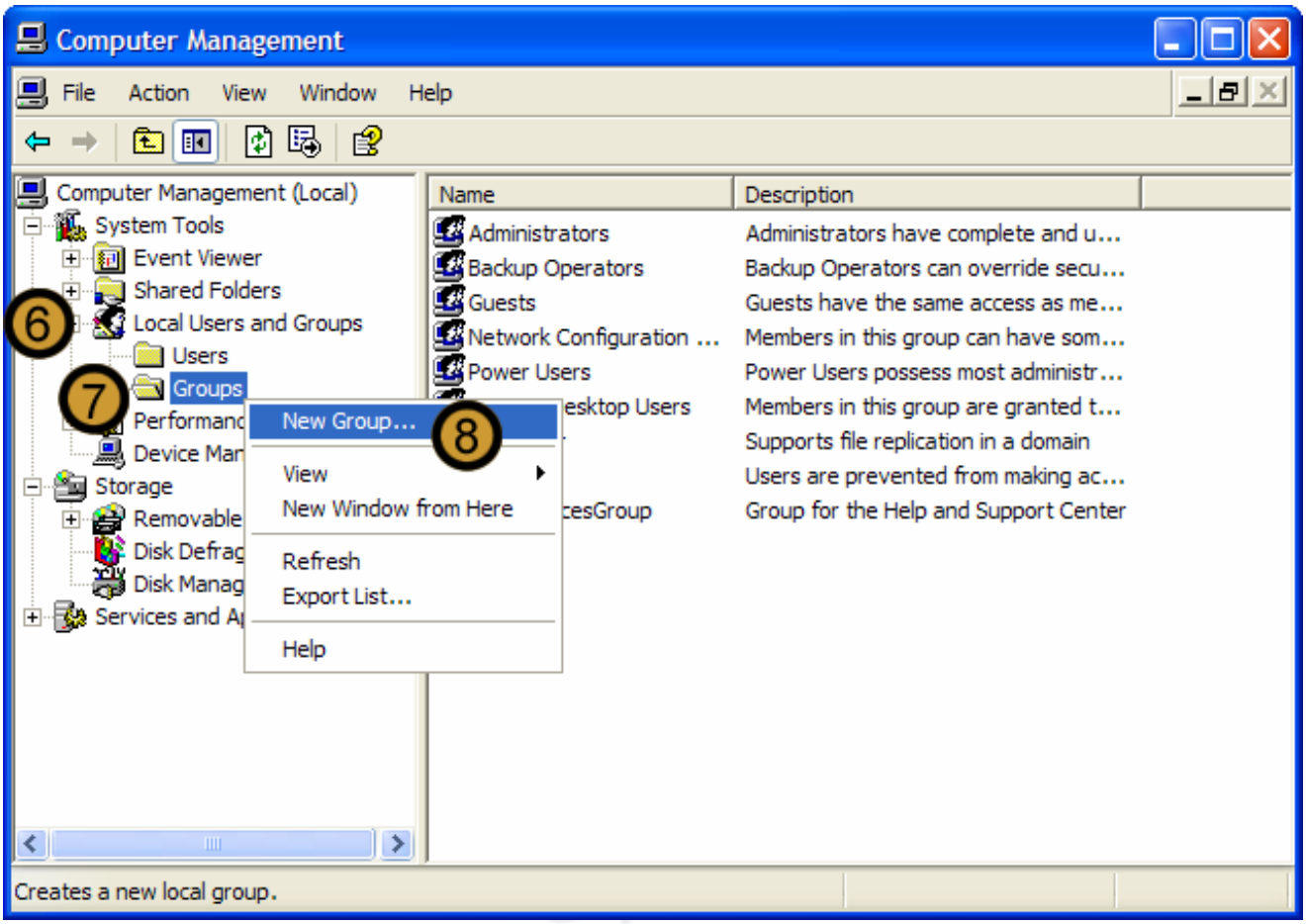
The **Performance and Maintenance** dialog box appears

4. In the PERFORMANCE AND MAINTENANCE dialog box, click **ADMINISTRATIVE TOOLS**



The Windows XP Professional **Administrative Tools** appears

5. In ADMINISTRATIVE TOOLS, double-click on the **COMPUTER MANAGEMENT** icon

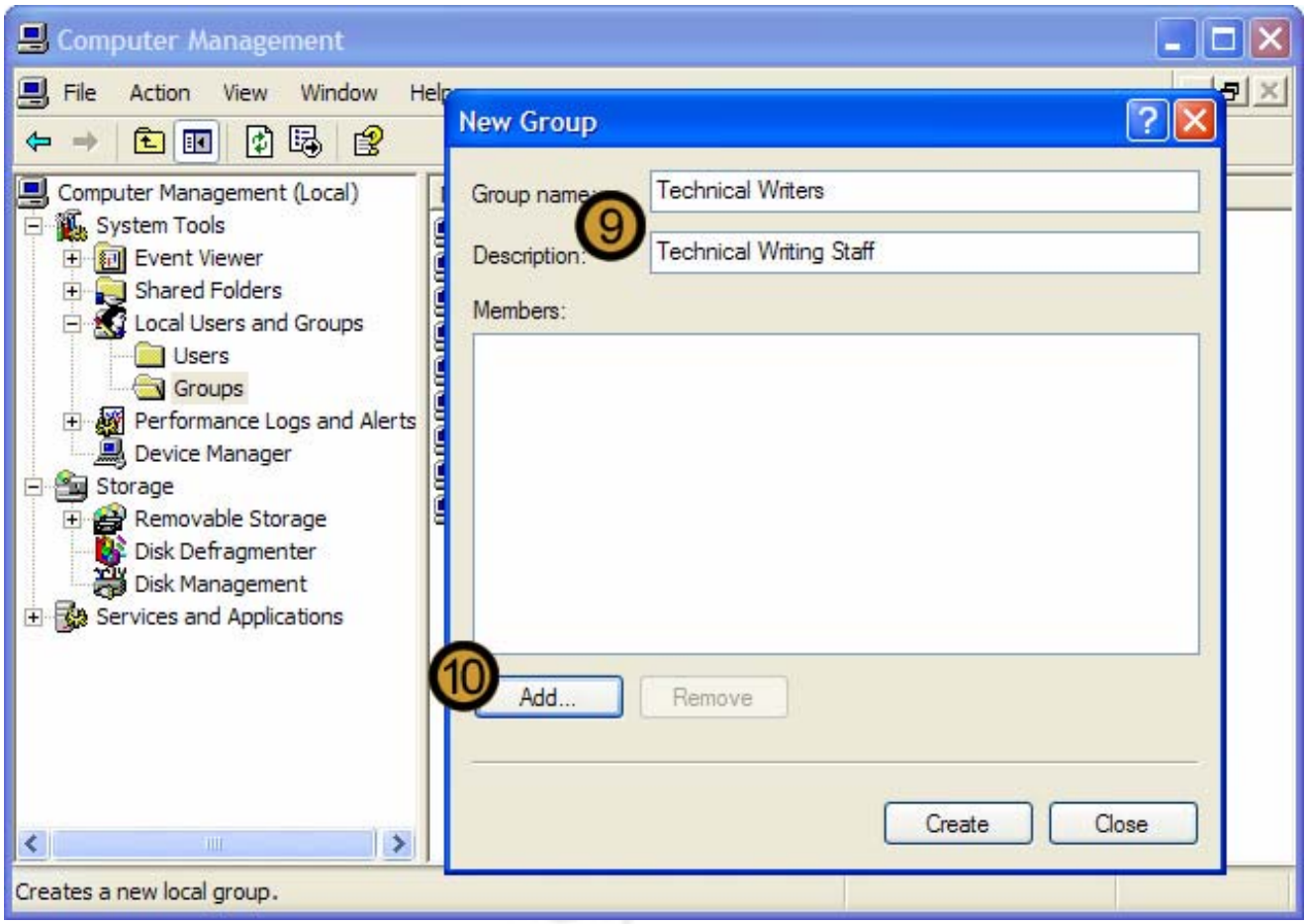


The **Computer Management Console** appears

6. In the COMPUTER MANAGEMENT CONSOLE, expand Local **Users and Groups**

7. Right click **GROUPS**

8. On the drop down menu that appears, click **NEW USER …**

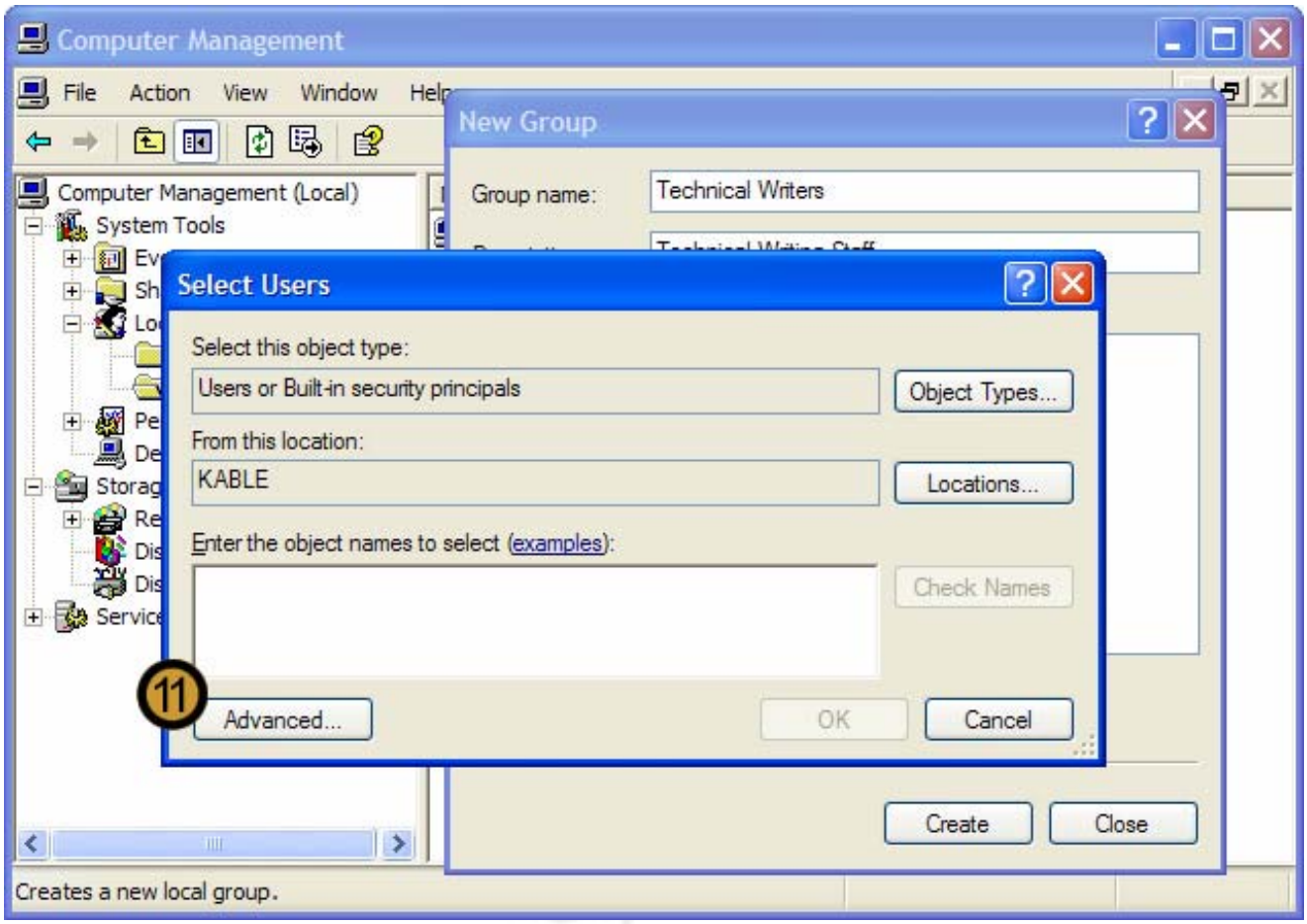


The New Group dialog box appears

9. In the NEW GROUP dialog box, provide a name and description for the new Group

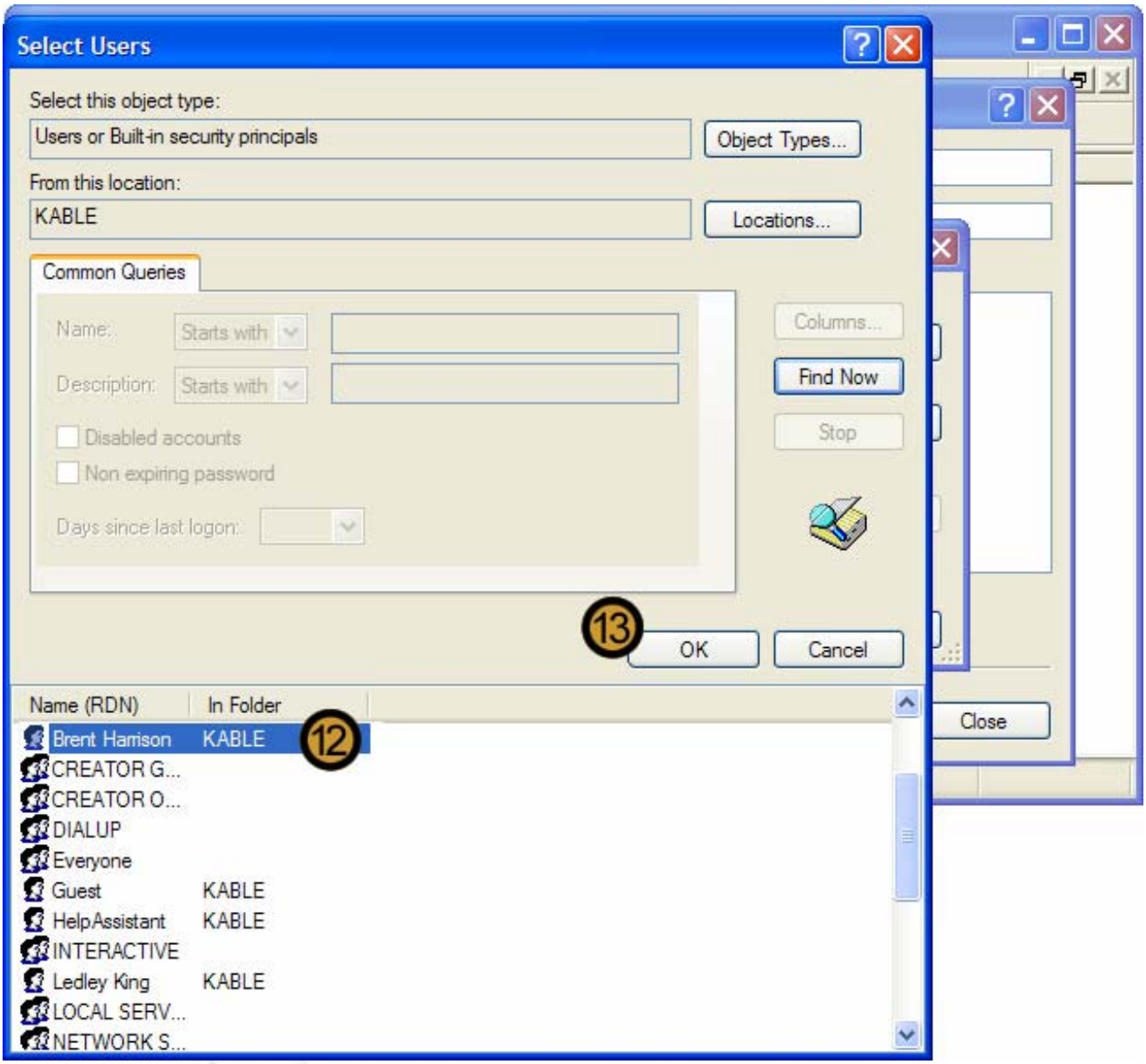
We can now either create the user group without assigning users to it by clicking CREATE; or we can first assign users to the group. In this example we will be performing the latter.

10. Click **ADD …**



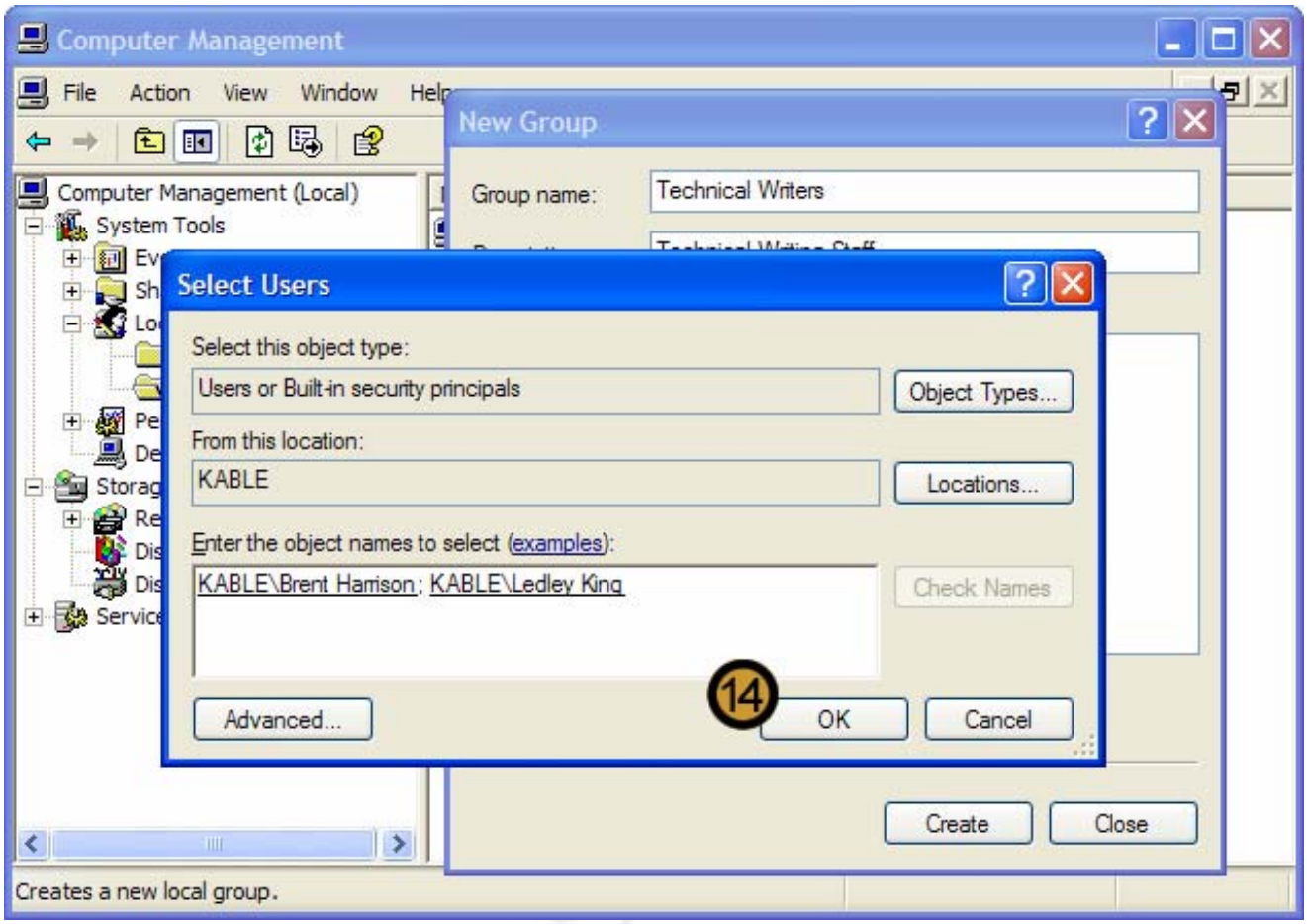
The **Select Users** dialog box appears

11. In the SELECT USERS dialog box, click **ADVANCED …**

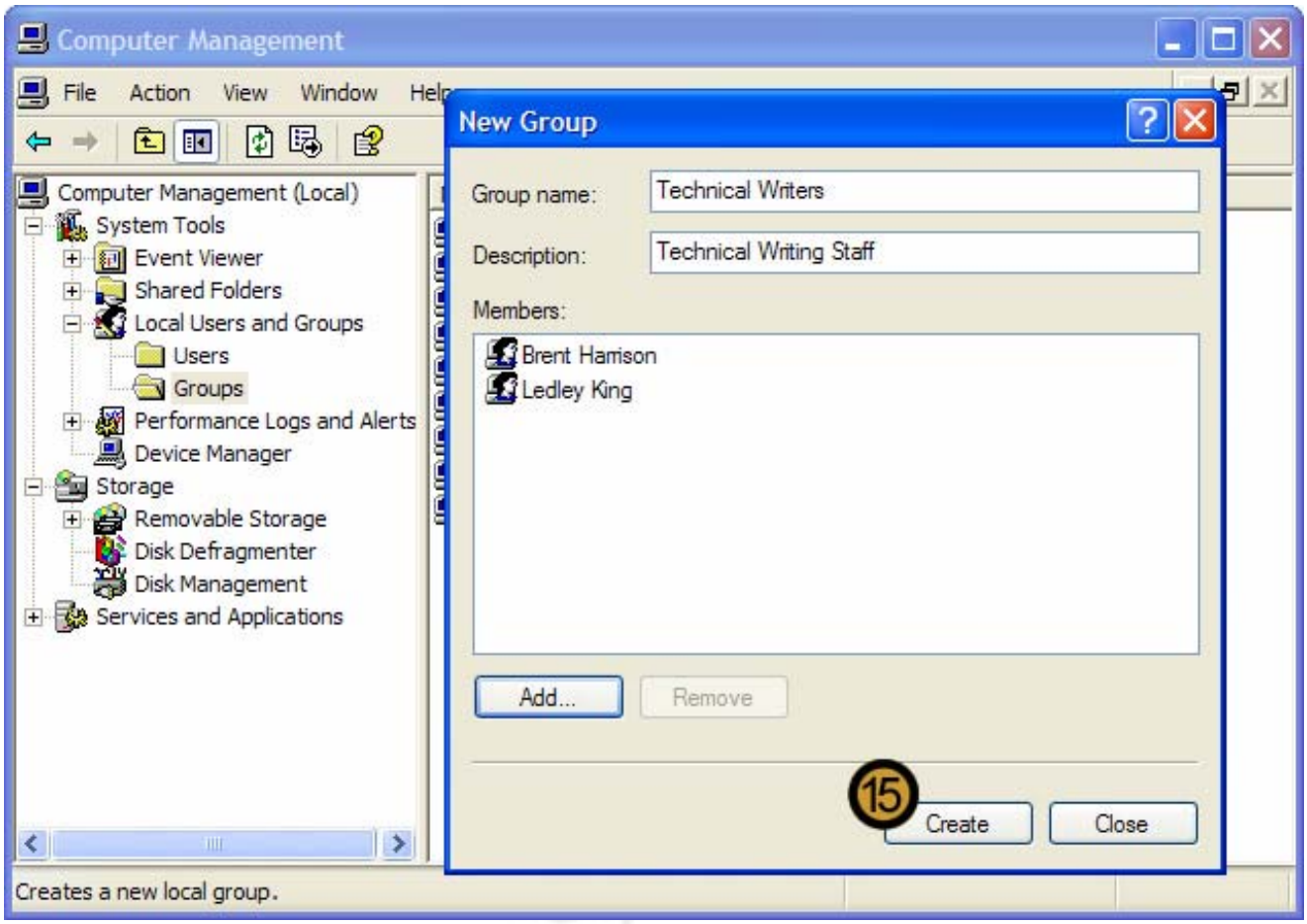


12. Select the Users that you can to assign to the group from the list that appears

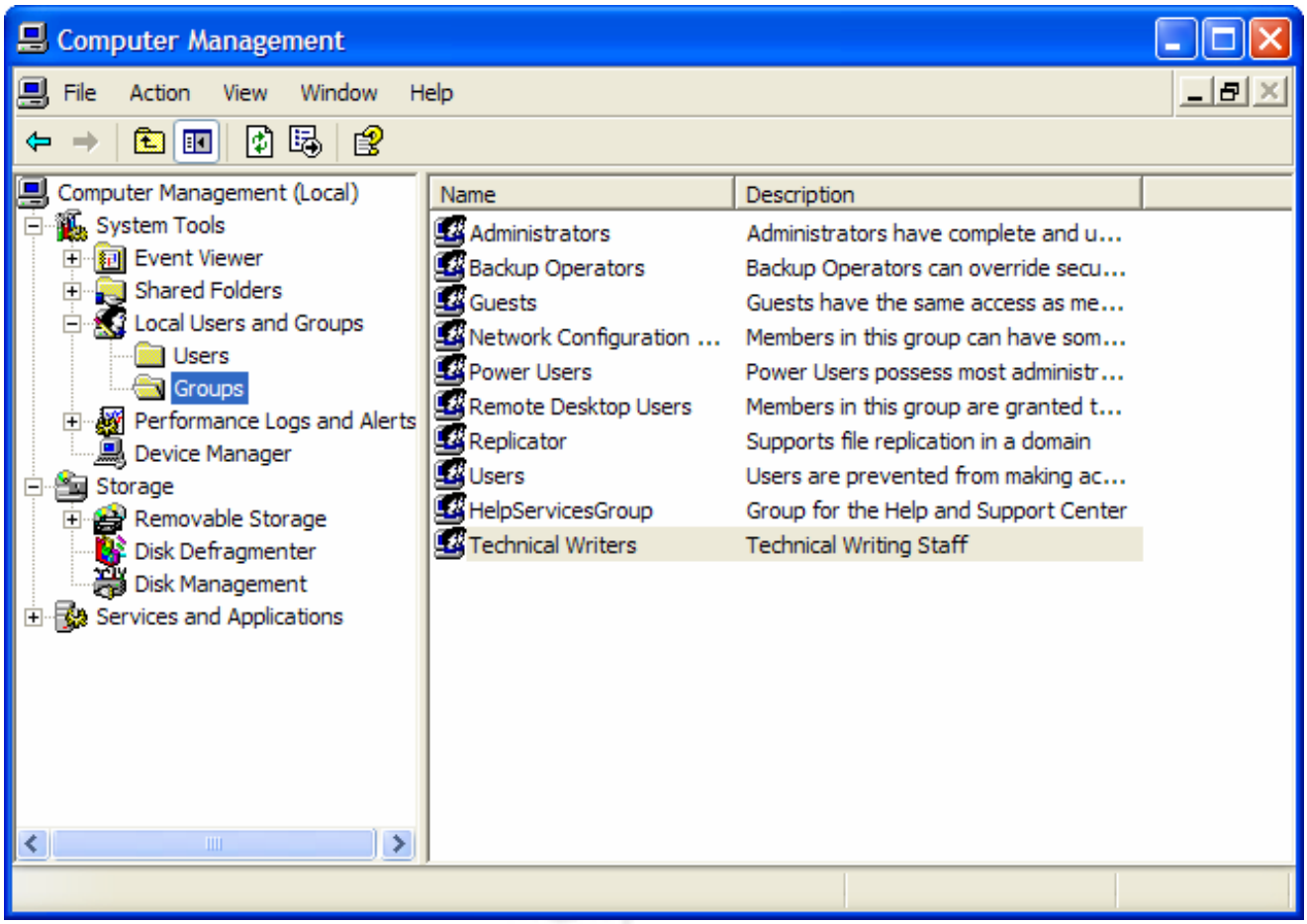
13. Click **OK**



14. Once you have selected all the users you want to added to the group, click **OK**

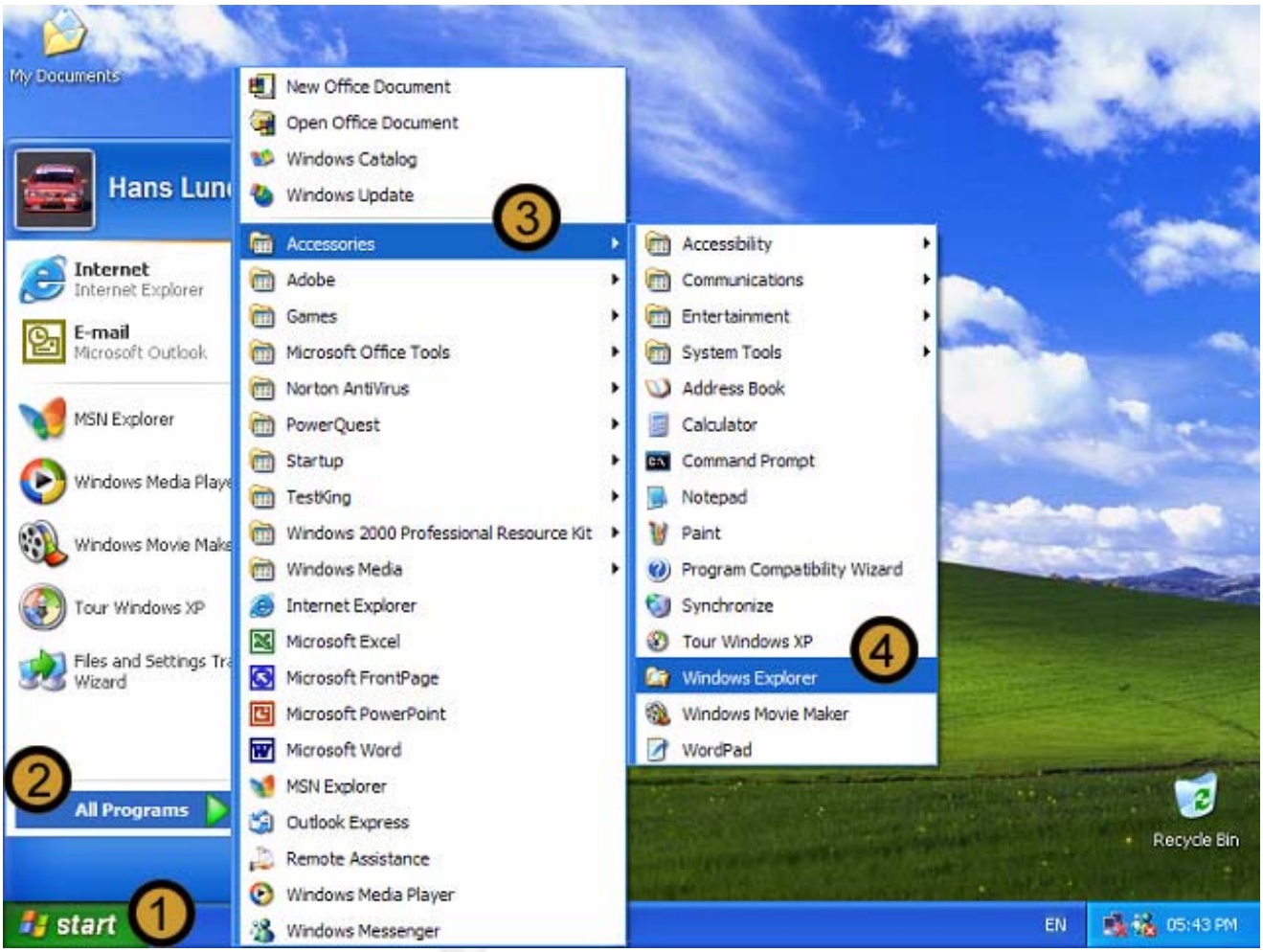


15. Click **CREATE** to create the new group



The user group has now been created

9.9 Configuring Disk Quotas

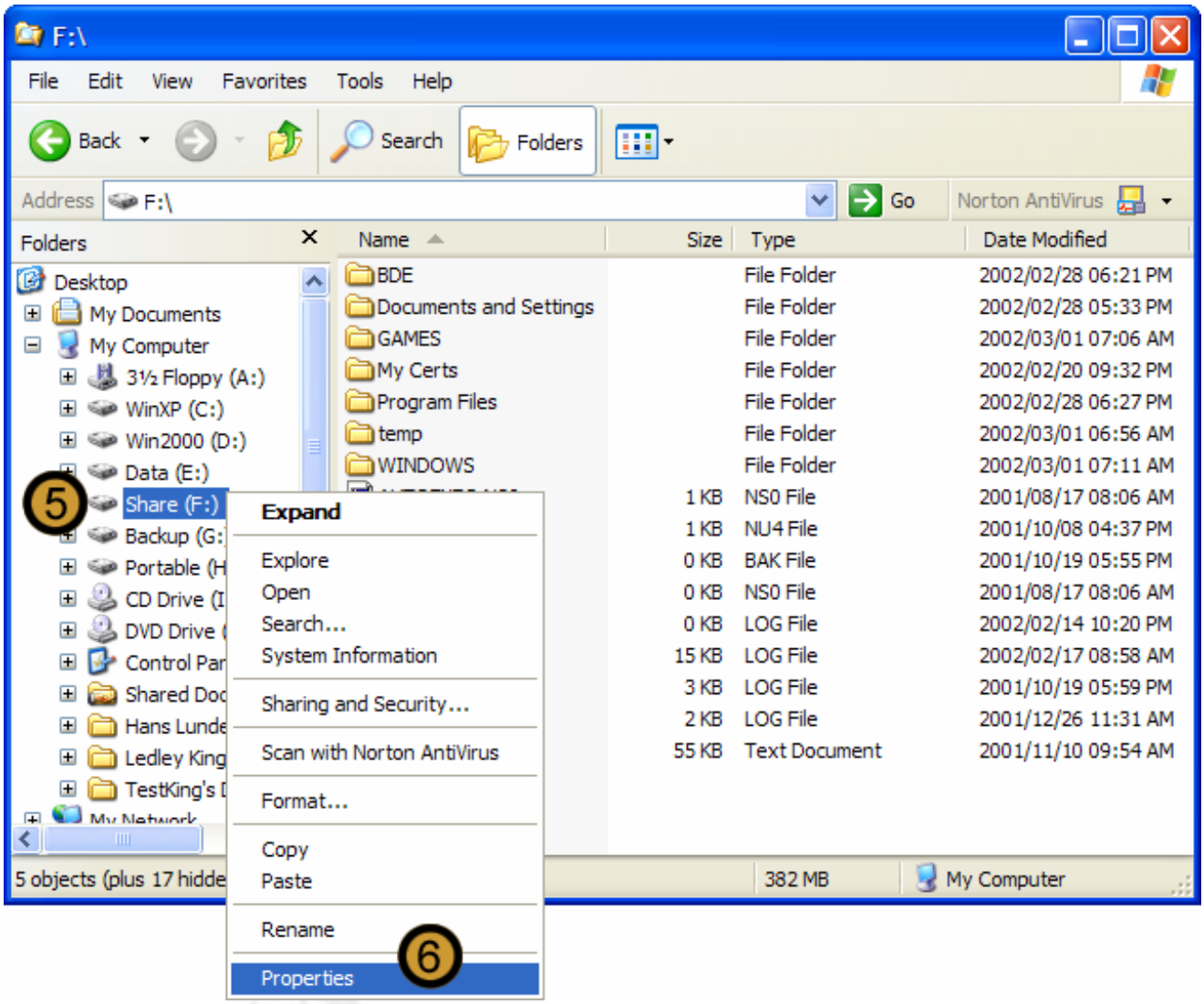


1. Click on the **START** button

2. Click **ALL PROGRAMS**

3. Point to **ACCESSORIES**

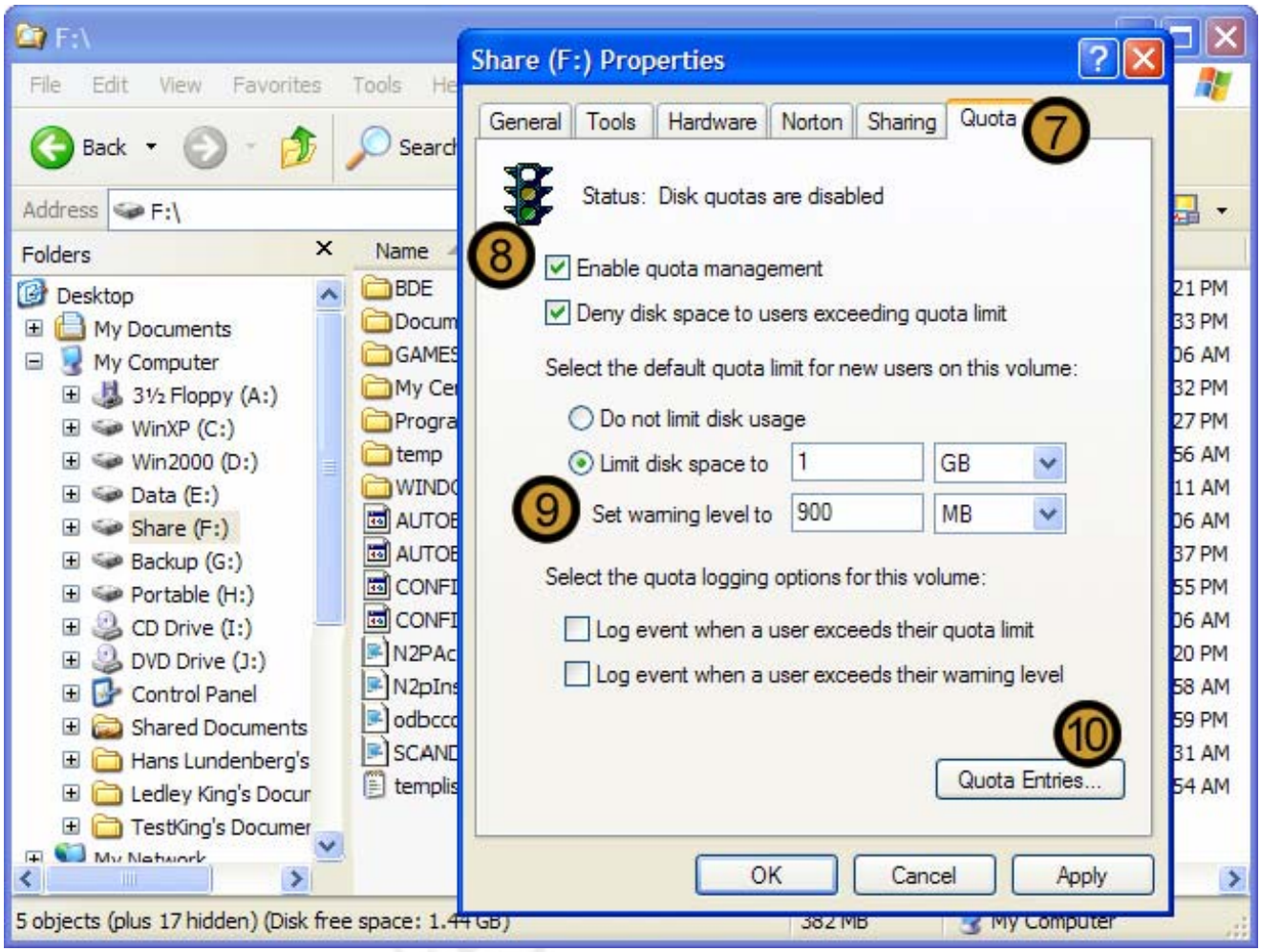
4. Open **WINDOWS EXPLORER**



5. In WINDOWS EXPLORER, Right-click the VOLUME you want to set quotas for

> **Note:** You can only configure Disk Quotas on volumes that have been formatted with the NTFS file system

6. On the drop down menu, click **PROPERTIES**



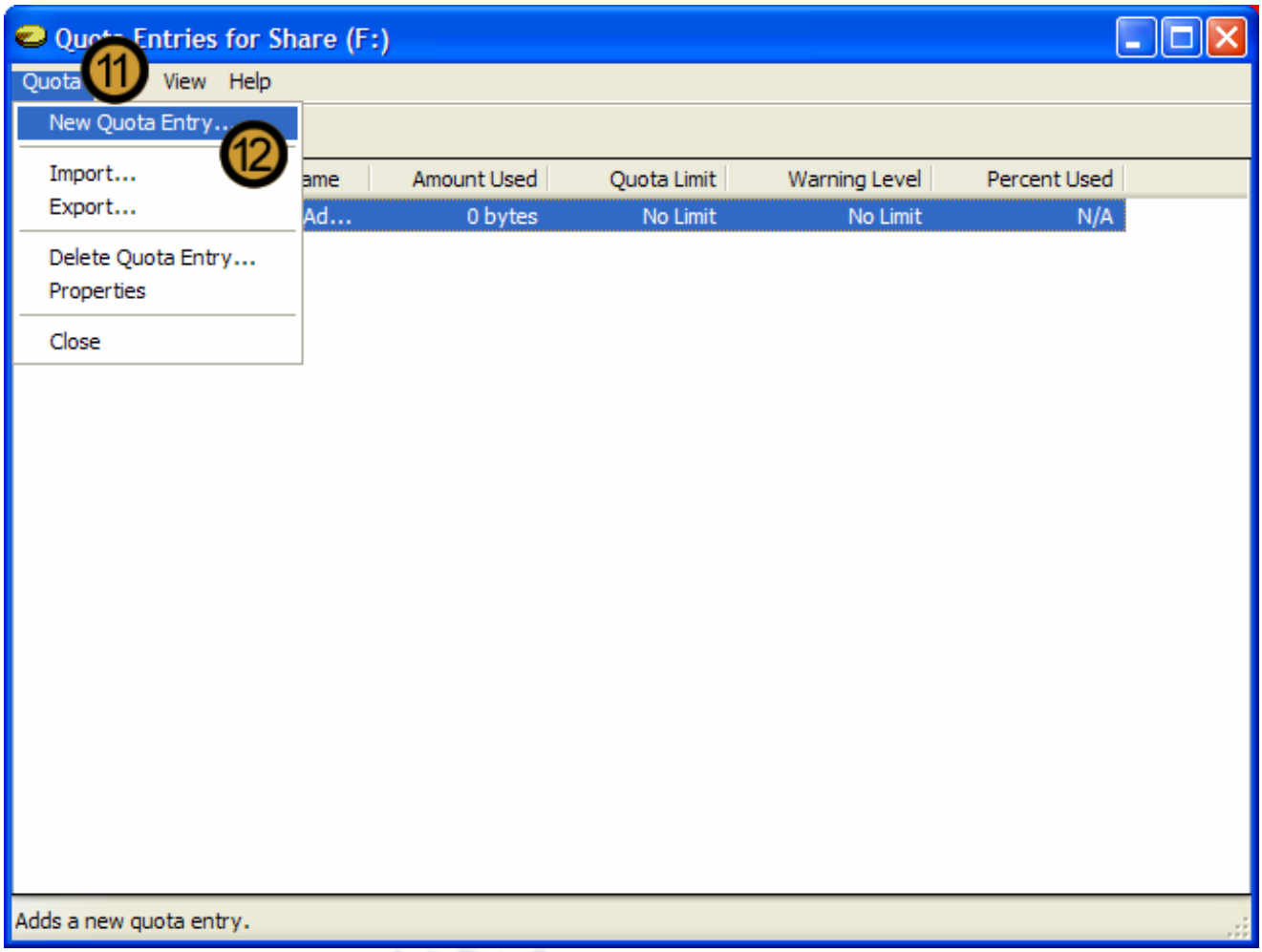
The VOLUME PROPERTIES dialog box appears

7. On the VOLUME PROPERTIES dialog box, click the **QUOTA** tab

8. Select the **ENABLE QUOTA MANAGEMENT** and **DENY DISK SPACE TO USERS EXCEEDING QUOTA LIMIT** check boxes

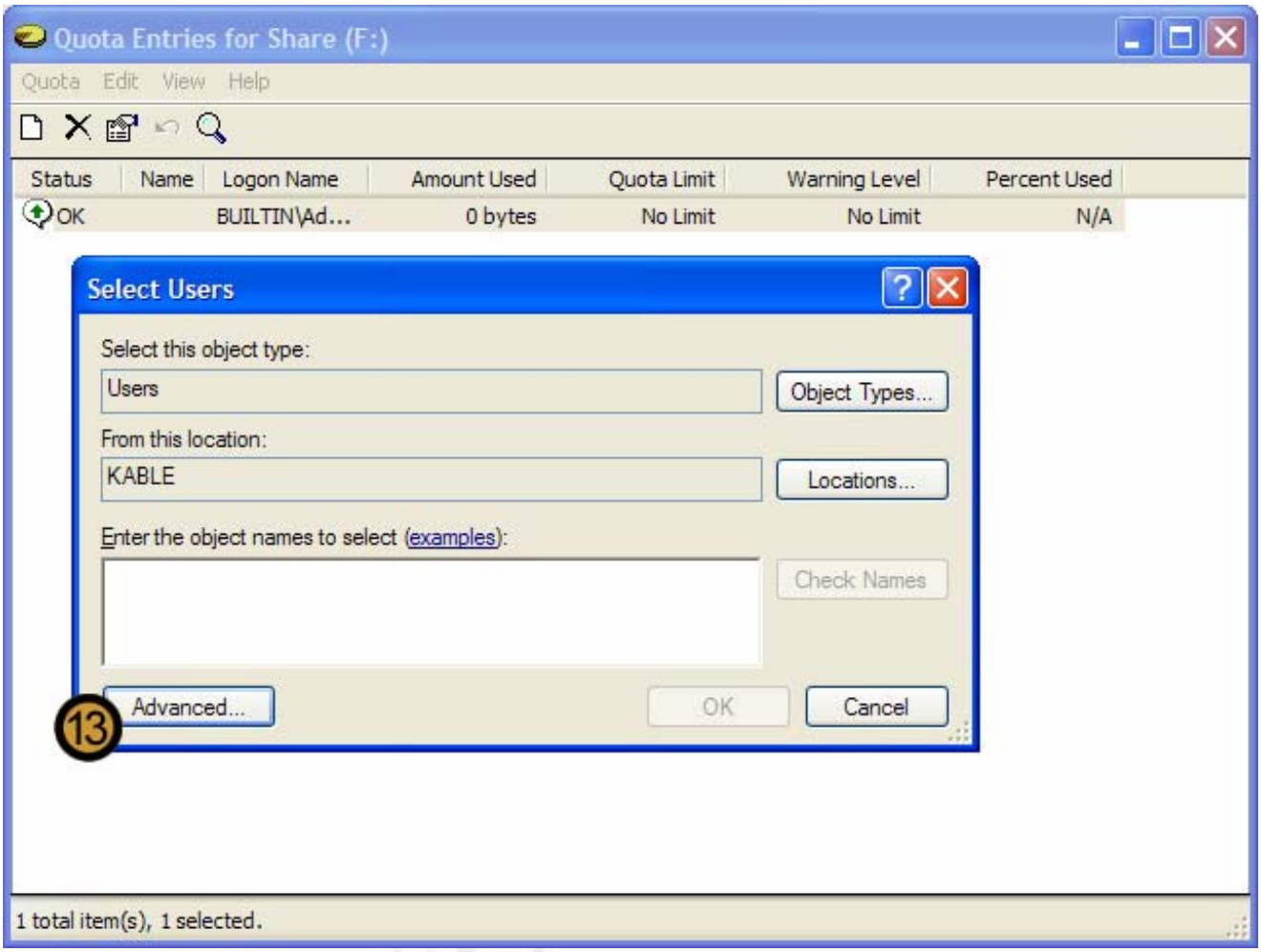
9. Set the quota limit and the warning level

10. Click **QUOTA ENTRIES**



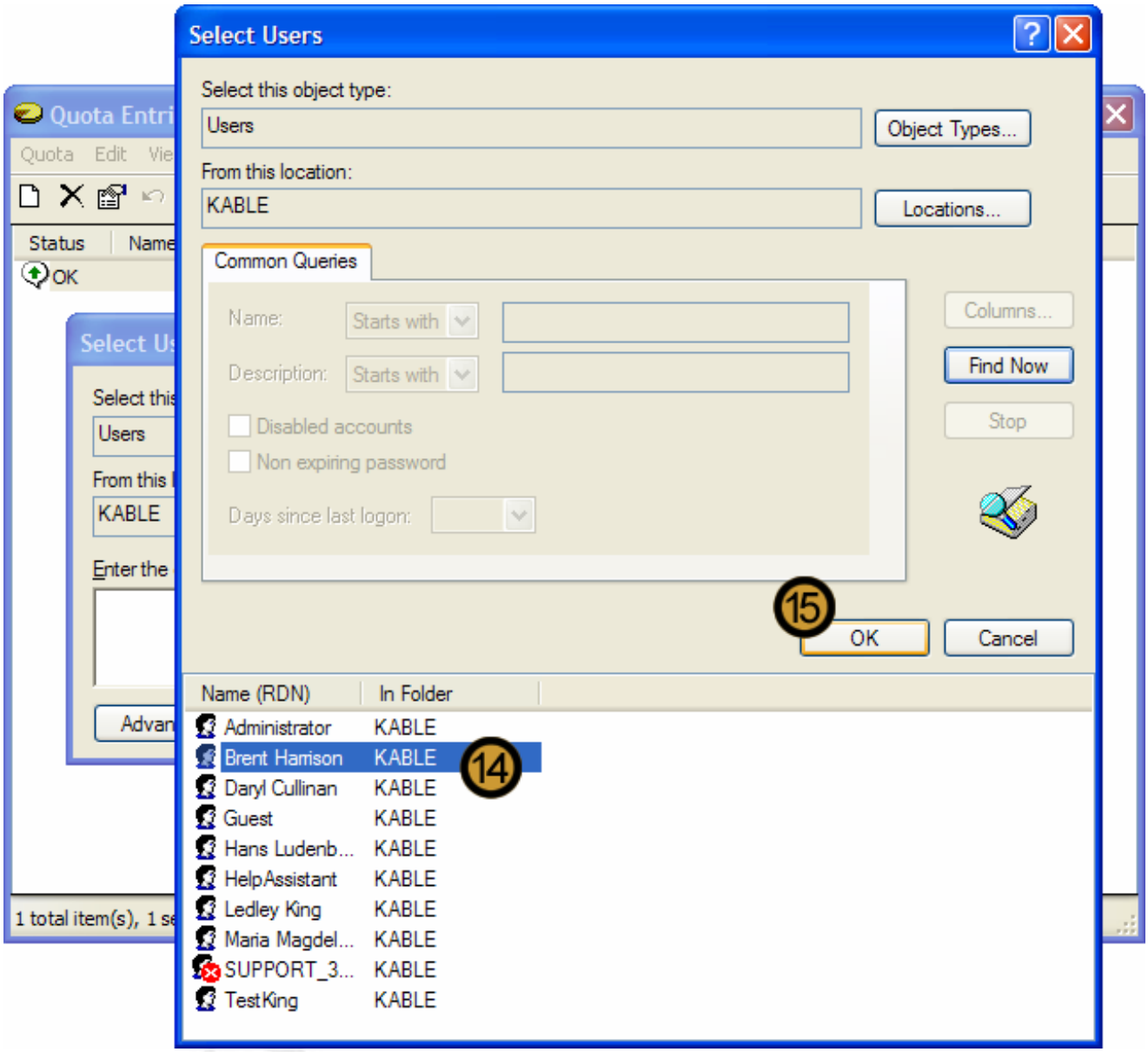
11. On the QUOTA ENTRIES dialog box, click on the **QUOTA** menu

12. On the drop down menu, click **NEW QUOTA ENTRY ...**



The SELECT USERS dialog box appears

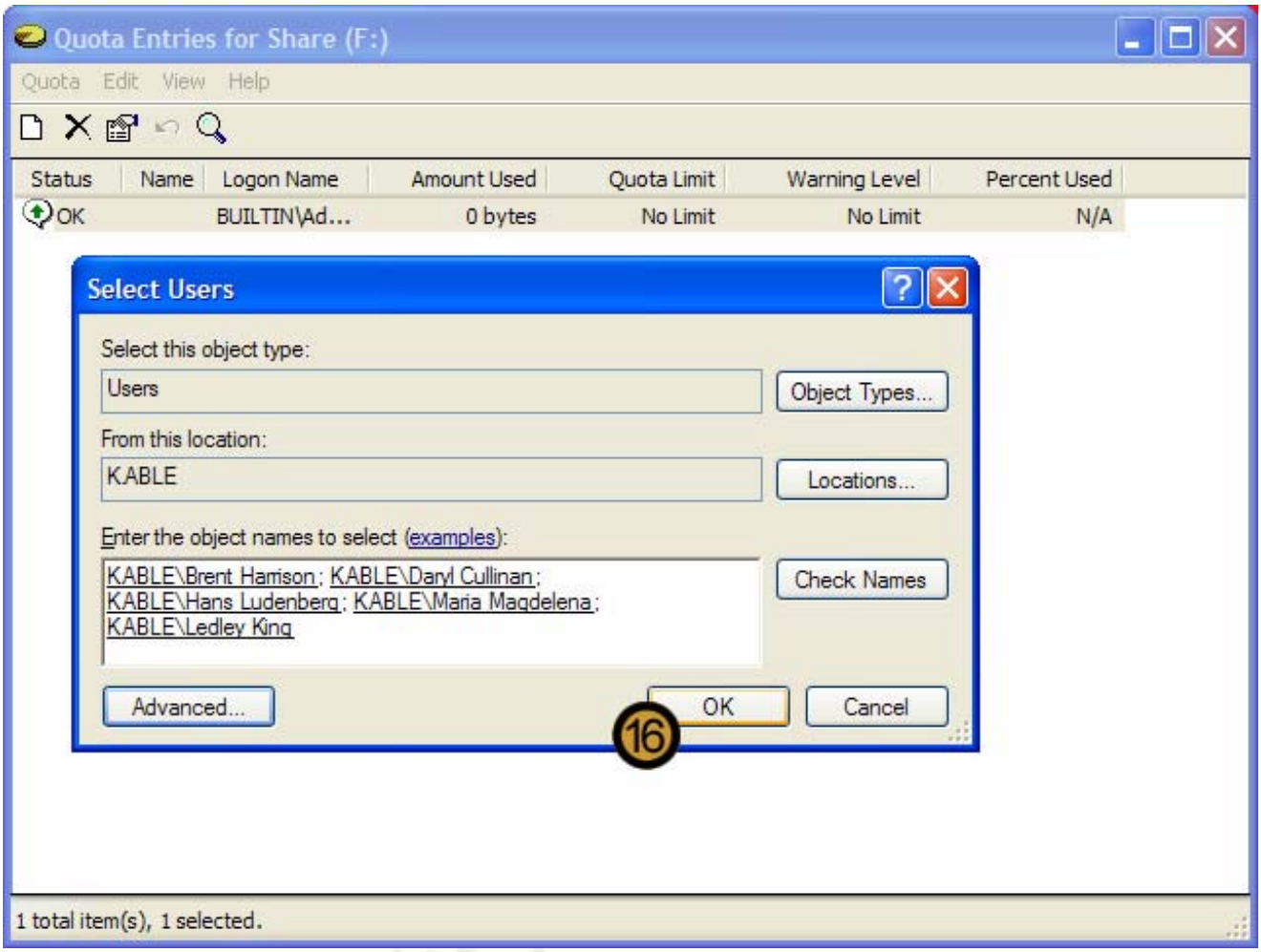
13. On the SELECT USERS dialog box, click **ADVANCED**



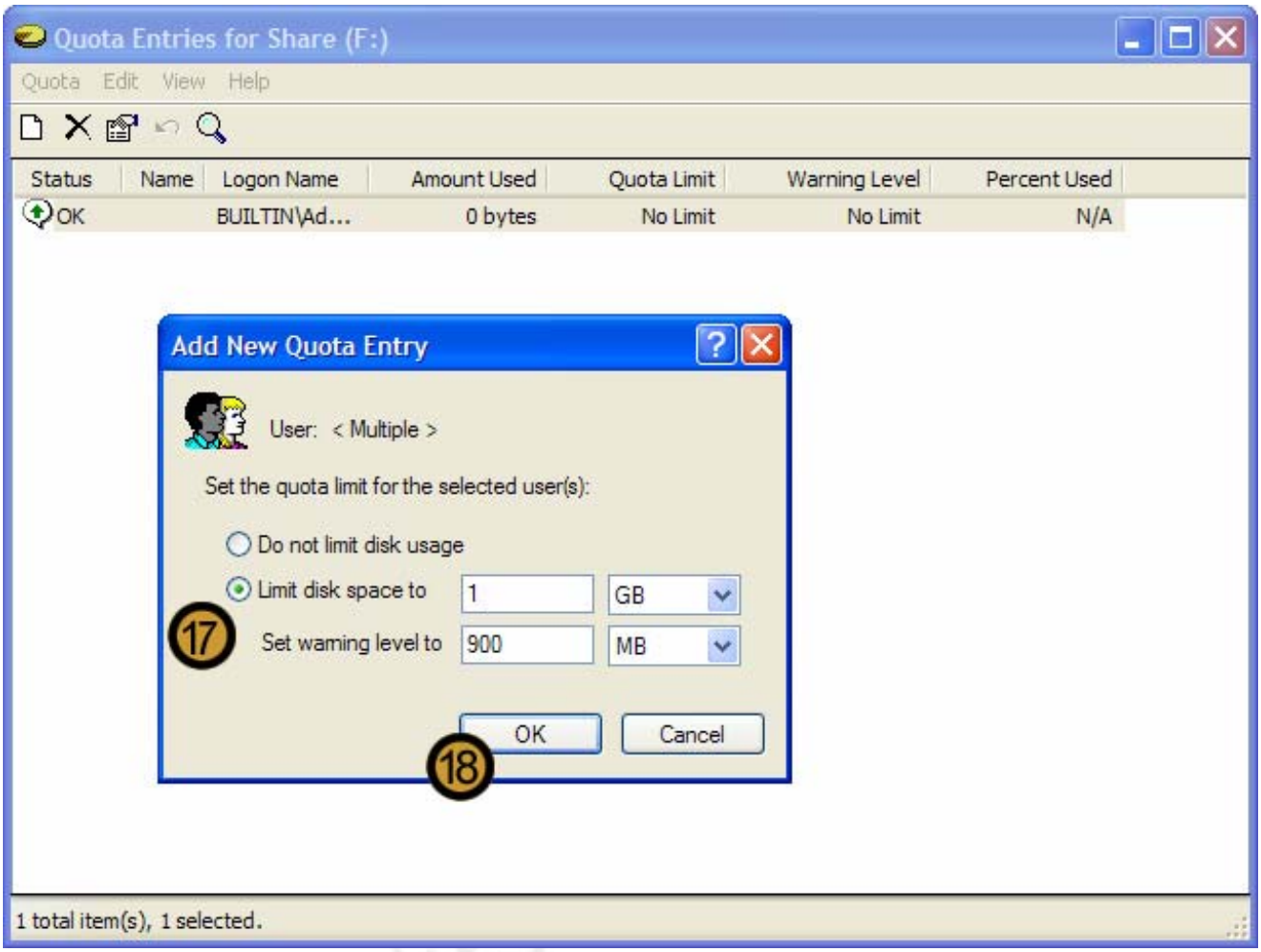
14. Select the Users whose disk usage you want to limit

Note: You can specify disk quotas on a per user per volume basis. Therefore only users are listed in the SELECT USERS dialog box and not user groups.

15. Click **OK**



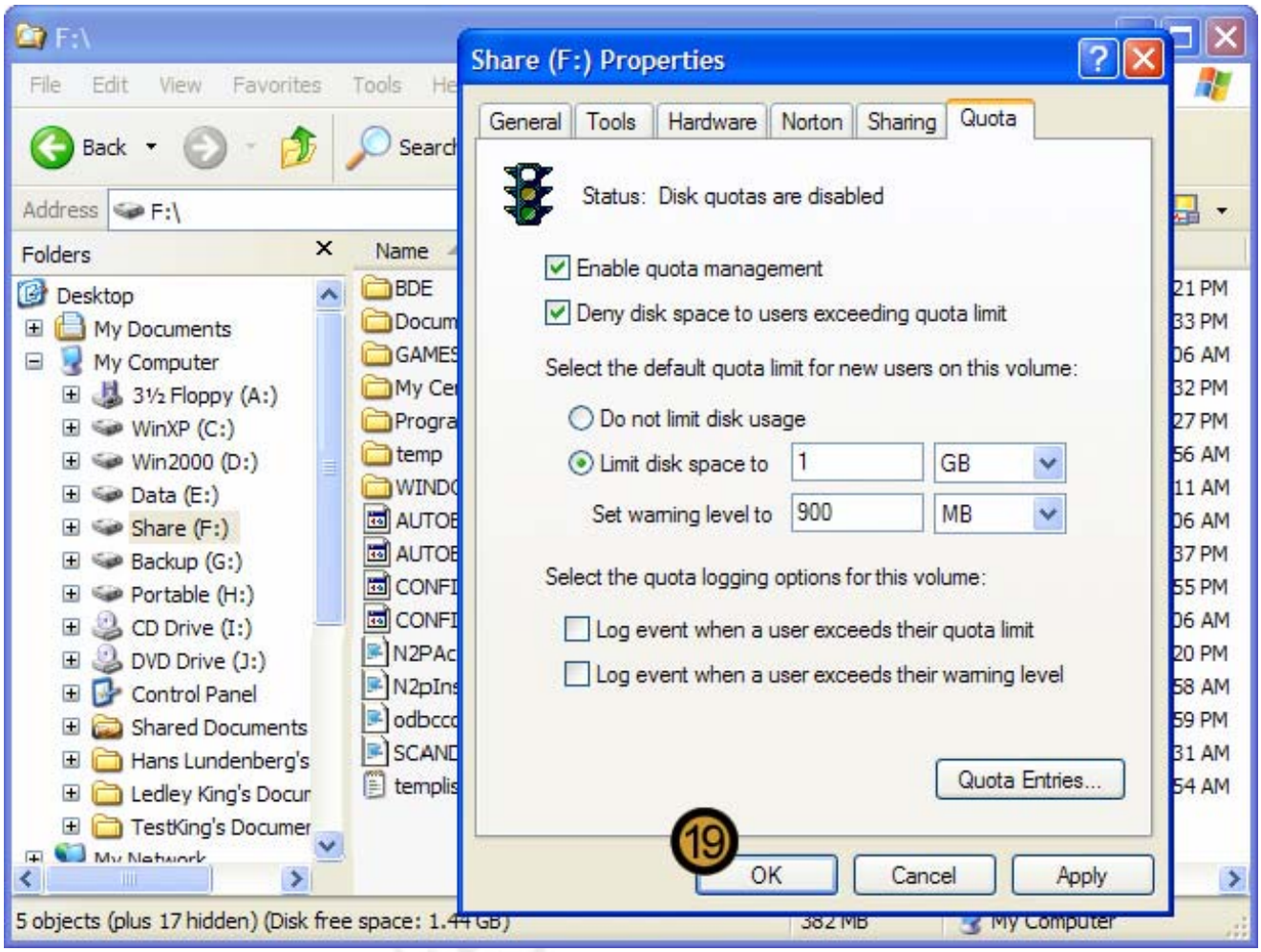
16. Once you have added all the Users whose disk usage you want to limit, click **OK**



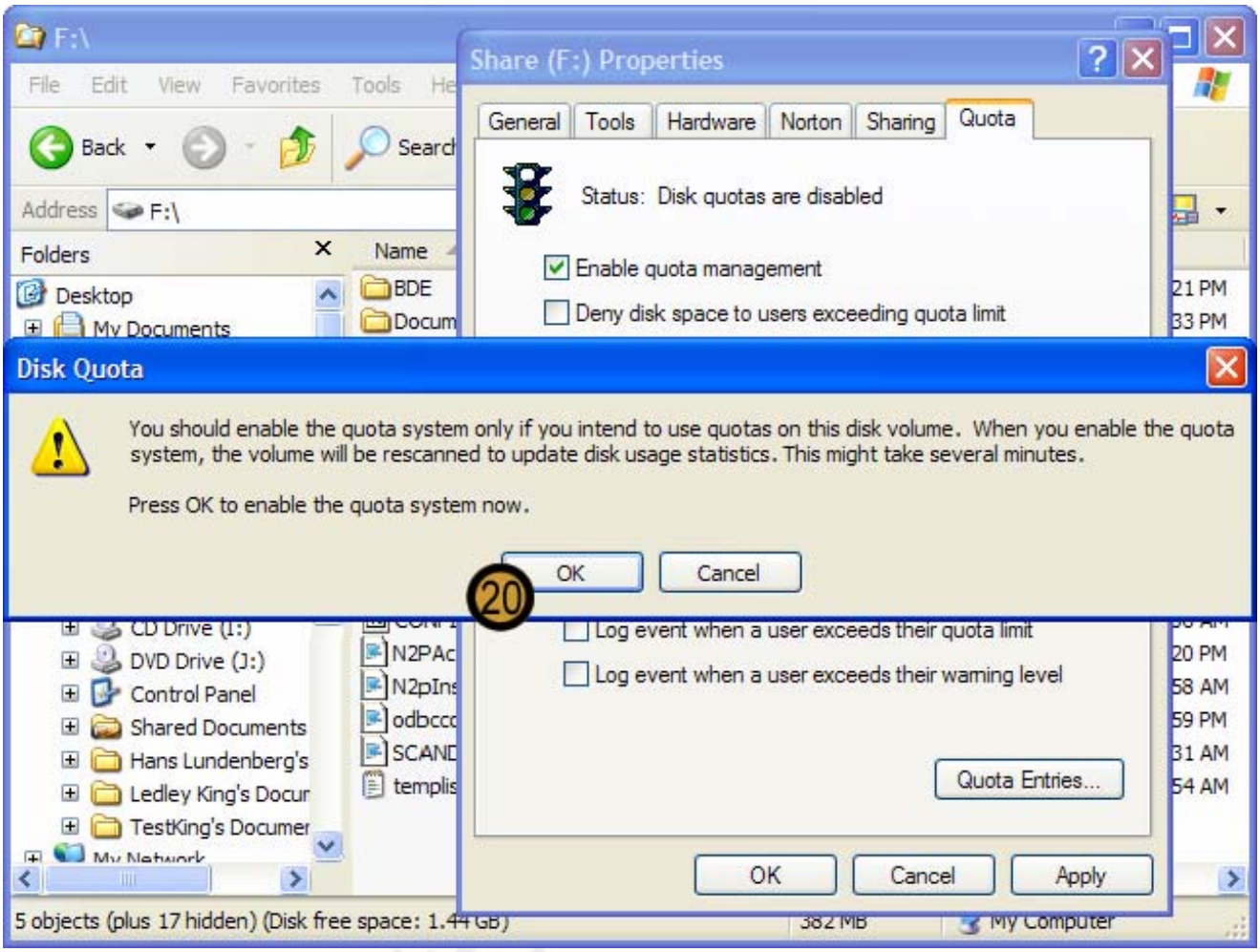
The ADD NEW QUOTA ENTRY dialog box appears

17. On the ADD NEW QUOTA ENTRY dialog box, set the quota limit and the warning level

18. Click **OK**

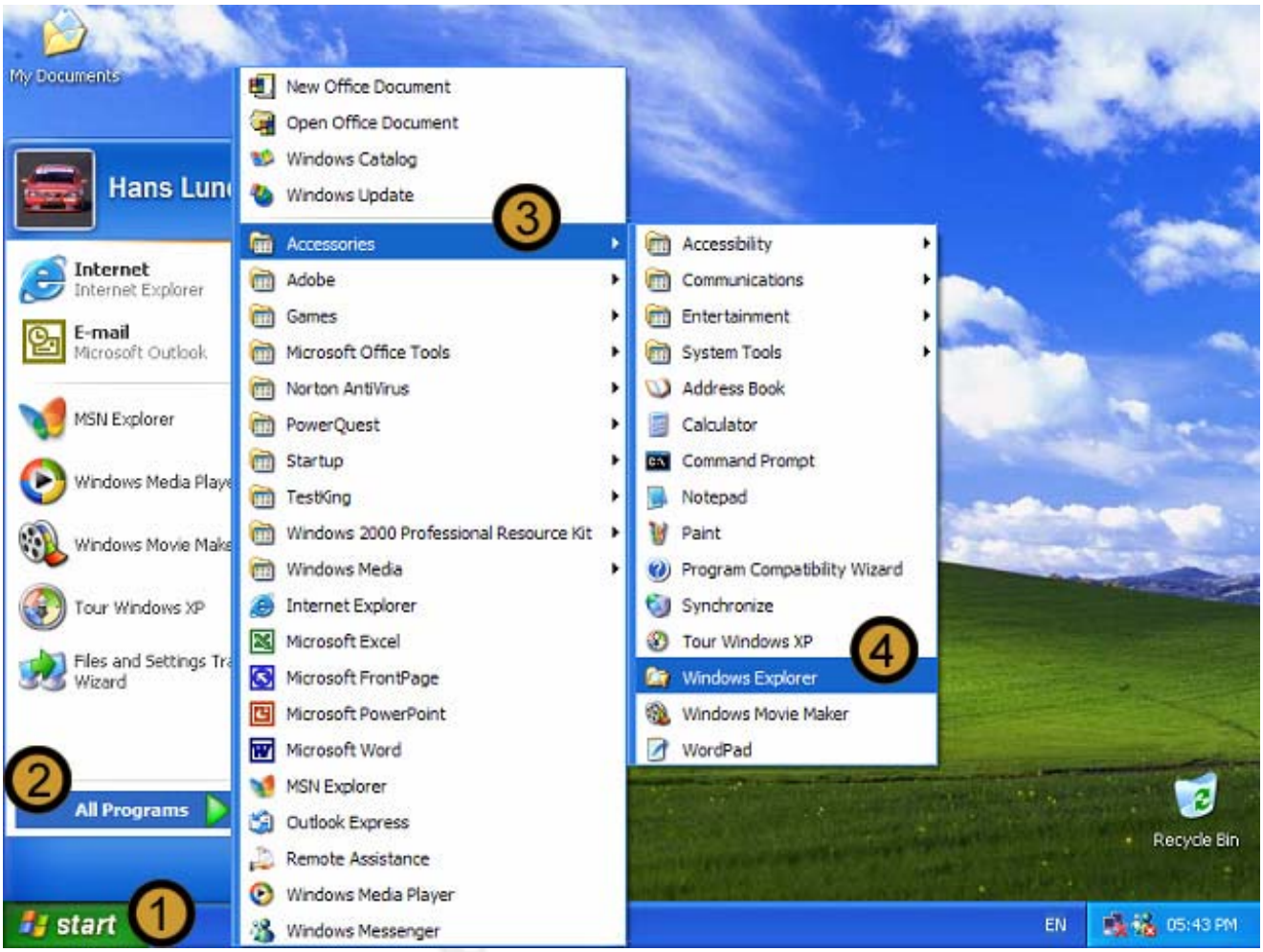


19. Click **OK** to close the VOLUME PROPERTIES dialog box



20. Click **OK** to confirm disk quotas

9.10 Compressing files and folders

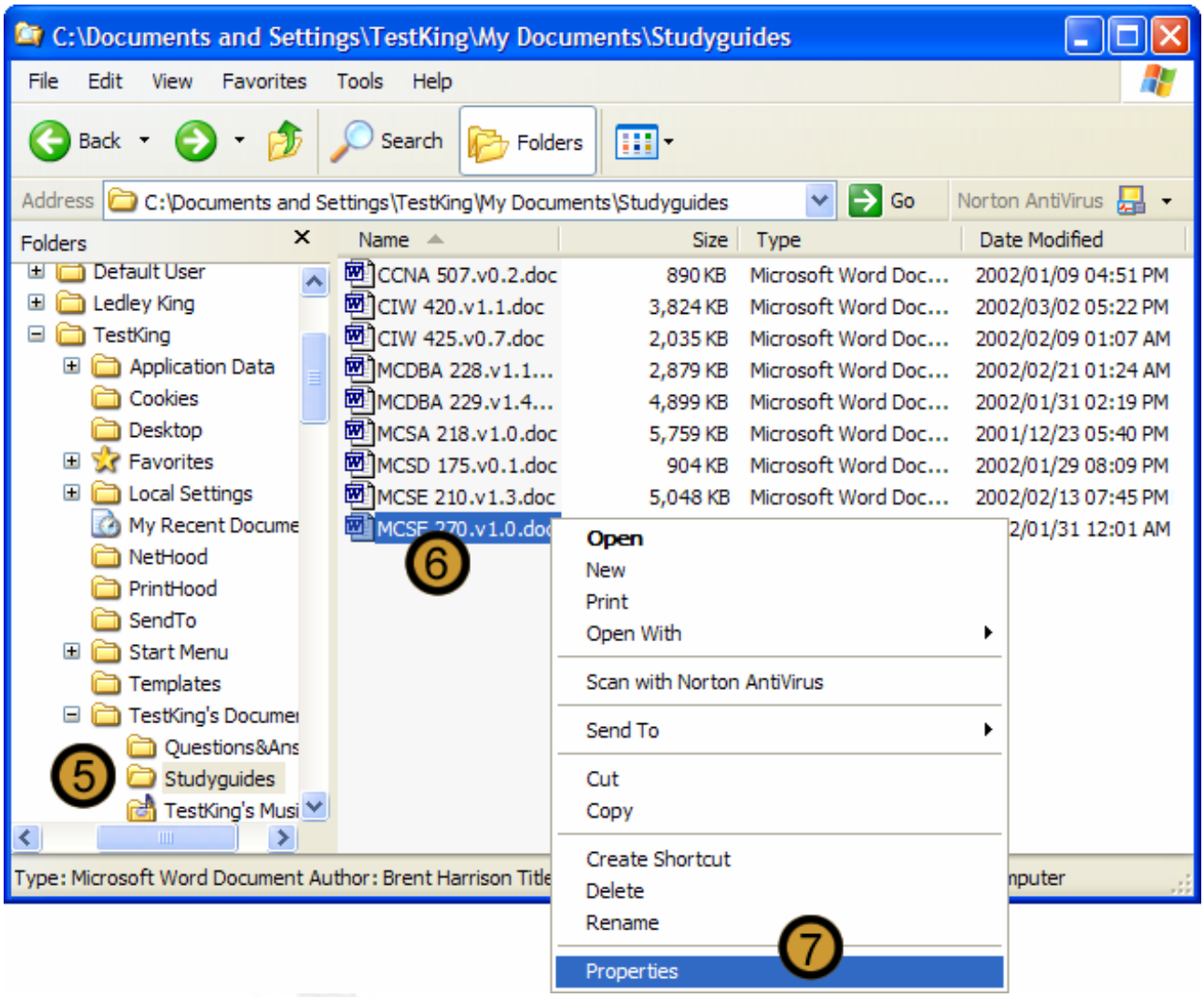


1. Click on the **START** button

2. Click **ALL PROGRAMS**

3. Point to **ACCESSORIES**

4. Open **WINDOWS EXPLORER**

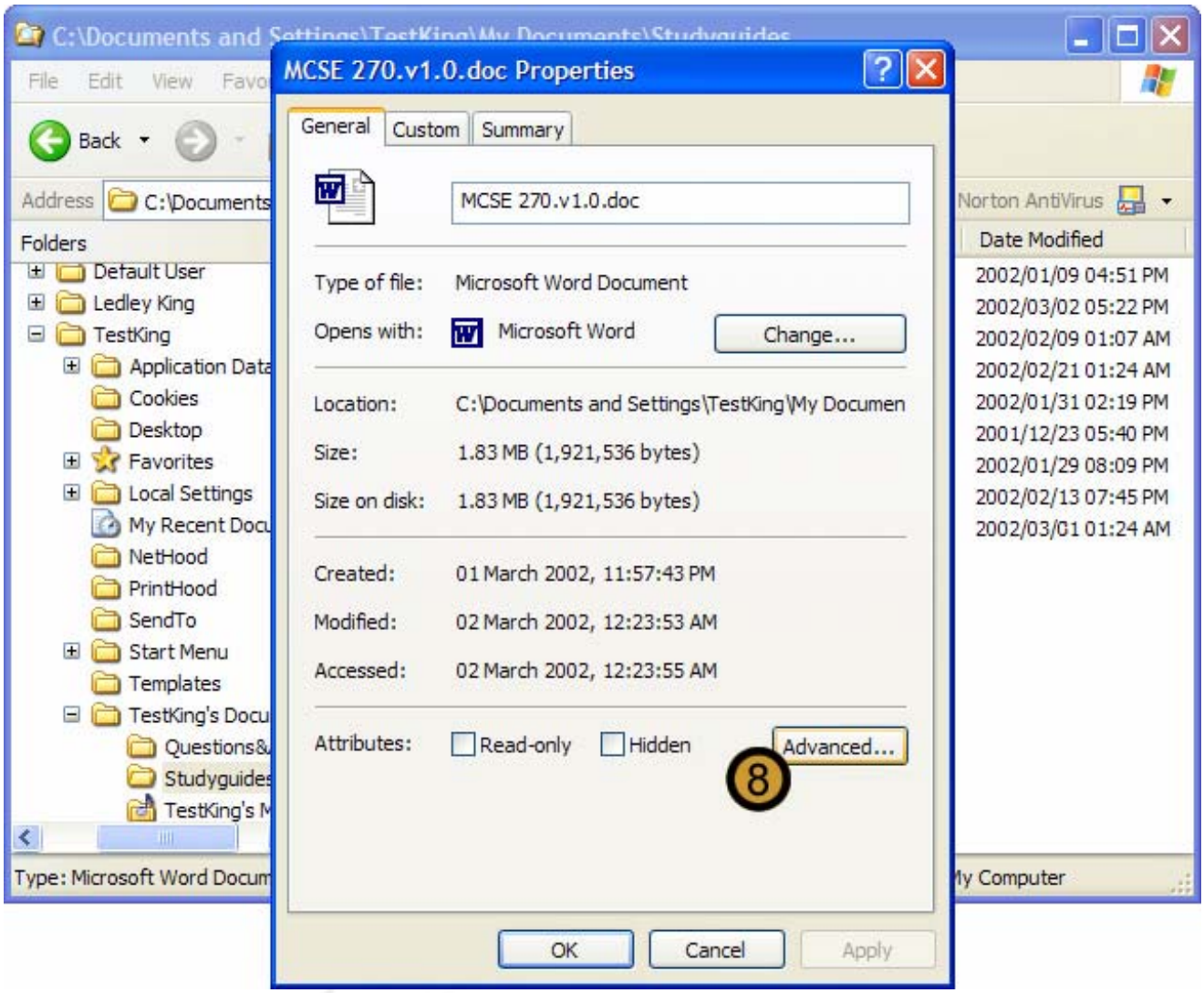


Note: You can only compress files and folders that are located on volumes that have been formatted with the **NTFS file system**.

5. In Windows Explorer locate and open the folder that contains the file you want to compress

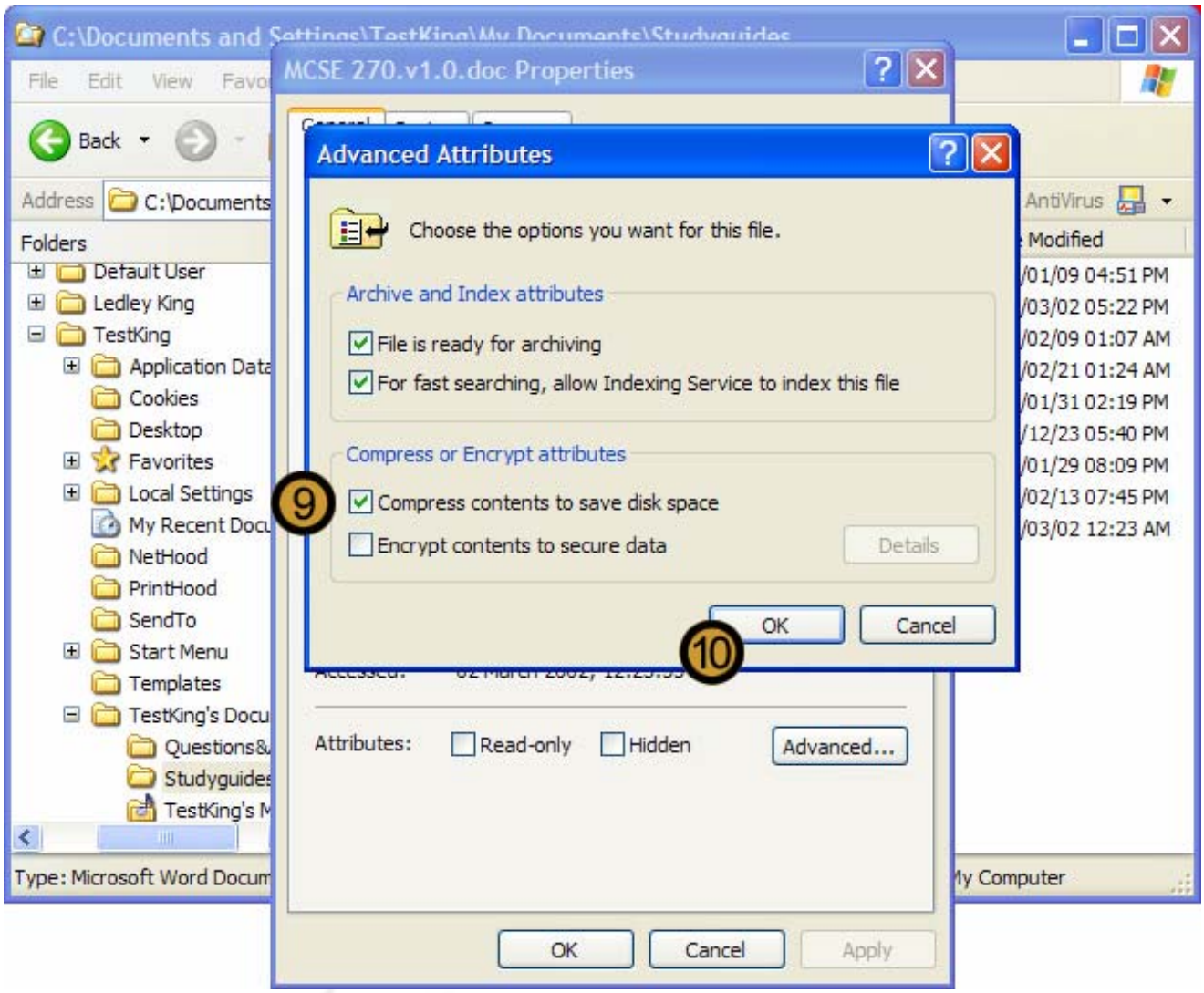
6. Right-click on the file you want to compress. You can also compress the folder by right-clicking on the folder.

7. On the drop down dialog box, click **PROPERTIES**



The selected FILE OR FOLDER dialog box appears

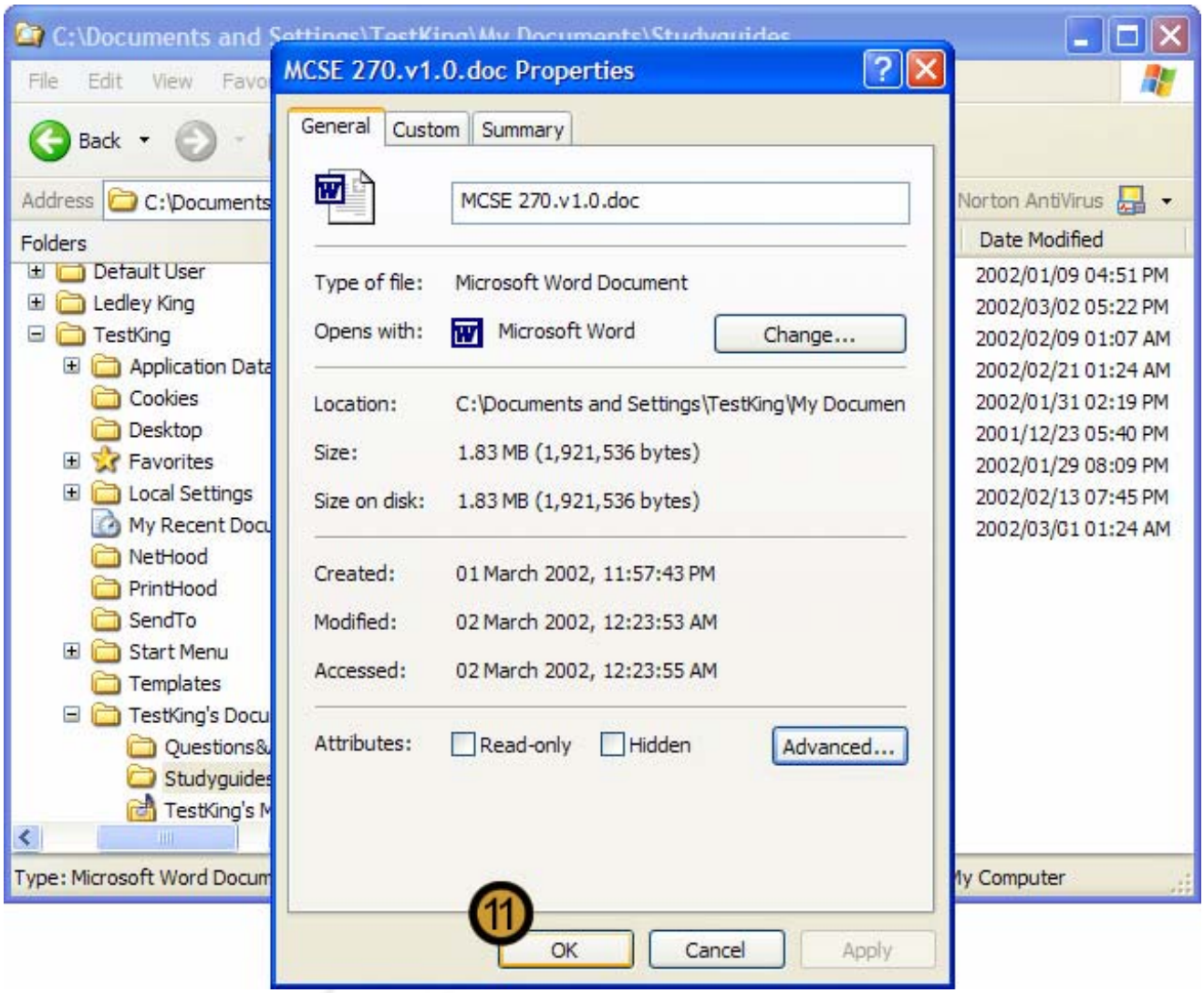
8. On the selected FILE OR FOLDER dialog box, click **ADVANCED ...**



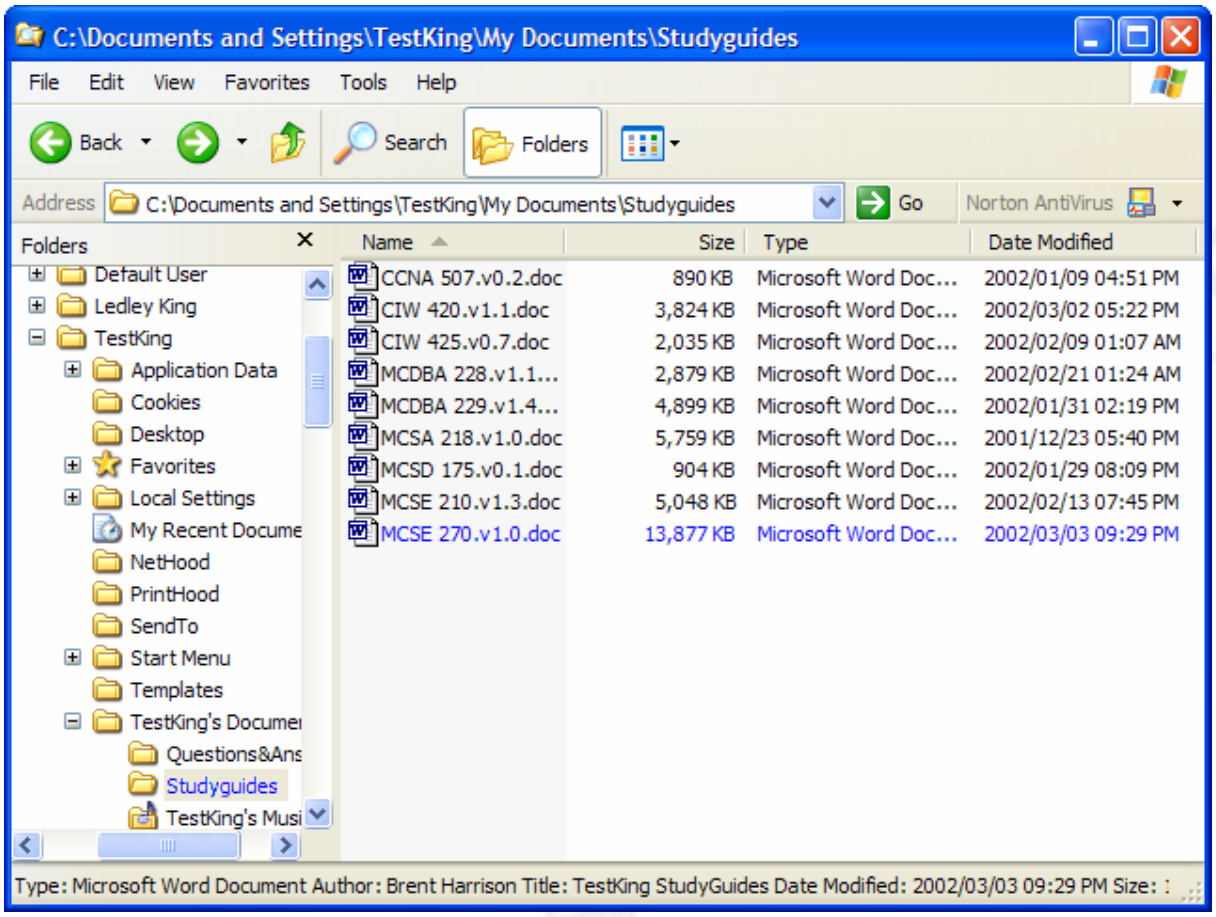
The ADVANCED ATTRIBUTES dialog box appears

9. In the COMPRESS OR ENCRYPT ATTRIBUTES section of the ADVANCED ATTRIBUTES dialog box, select the **COMPRESS CONTENTS TO SAVE DISK SPACE** check box

10. Click **OK**

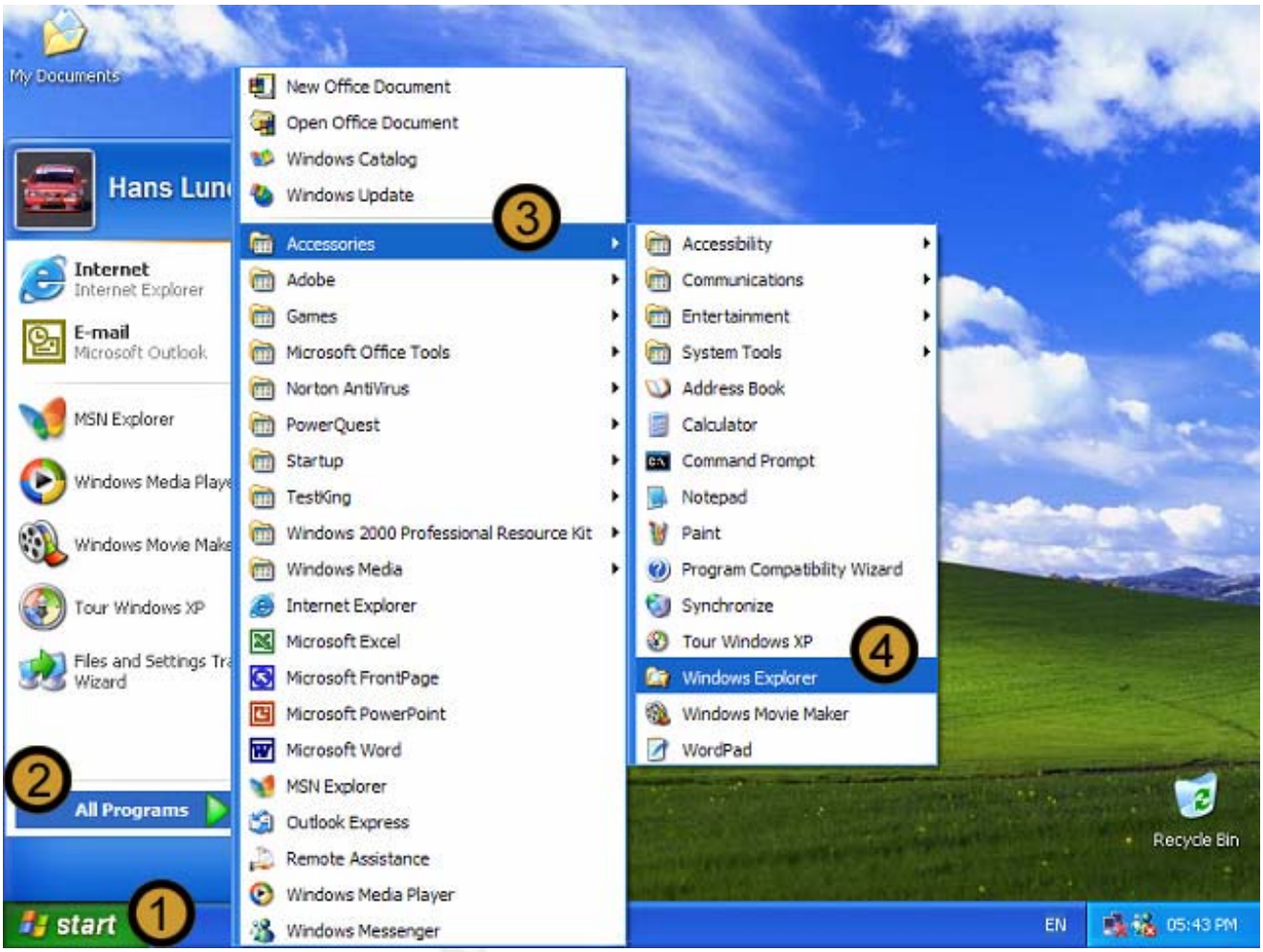


11. Close the selected FILE OR FOLDER dialog box by clicking **OK**



The file is now compressed and its compressed state is indicated by using an alternative colour

9.11 Encrypting Files and Folders

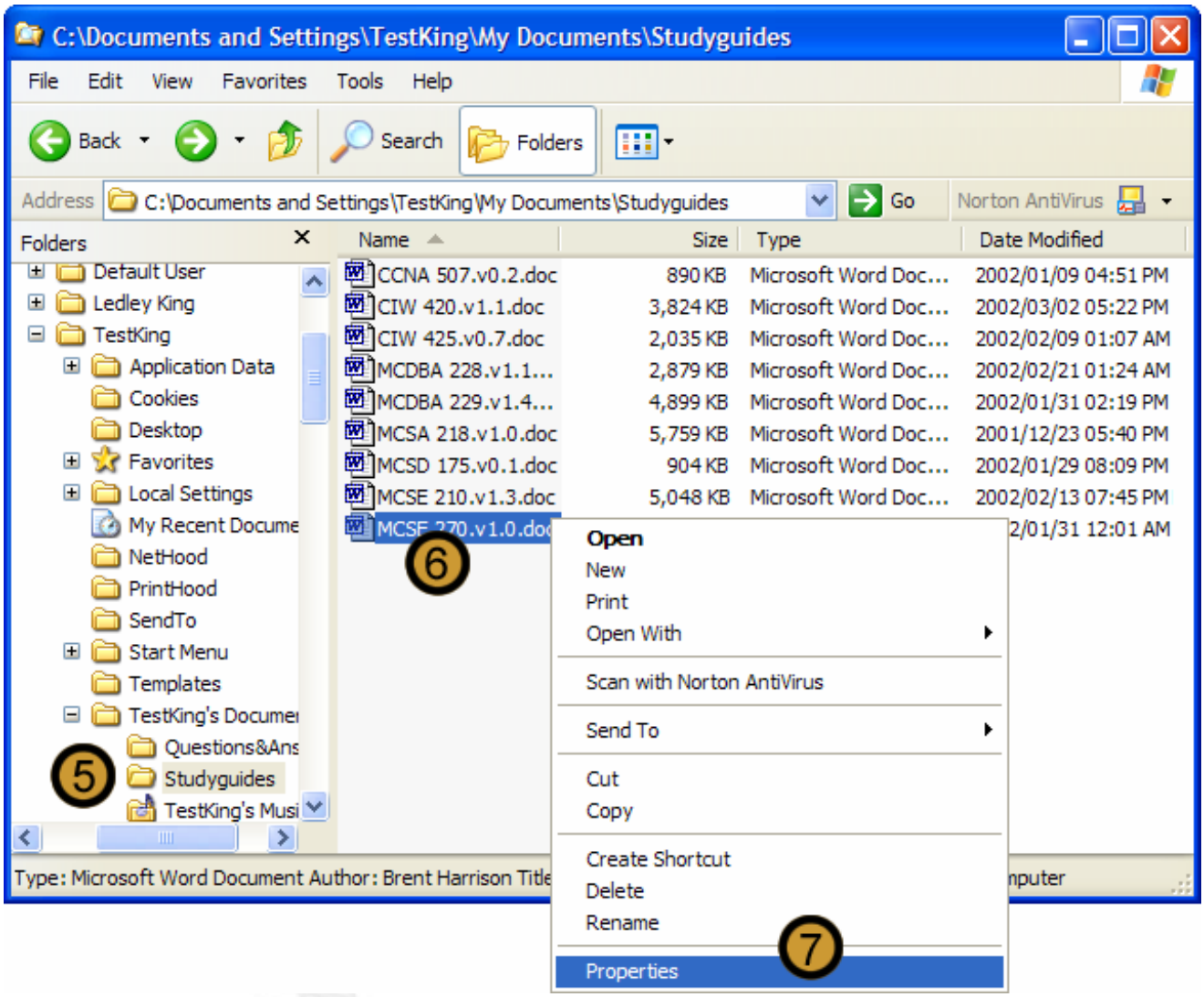


1. Click on the **START** button

2. Click **ALL PROGRAMS**

3. Point to **ACCESSORIES**

4. Open **WINDOWS EXPLORER**

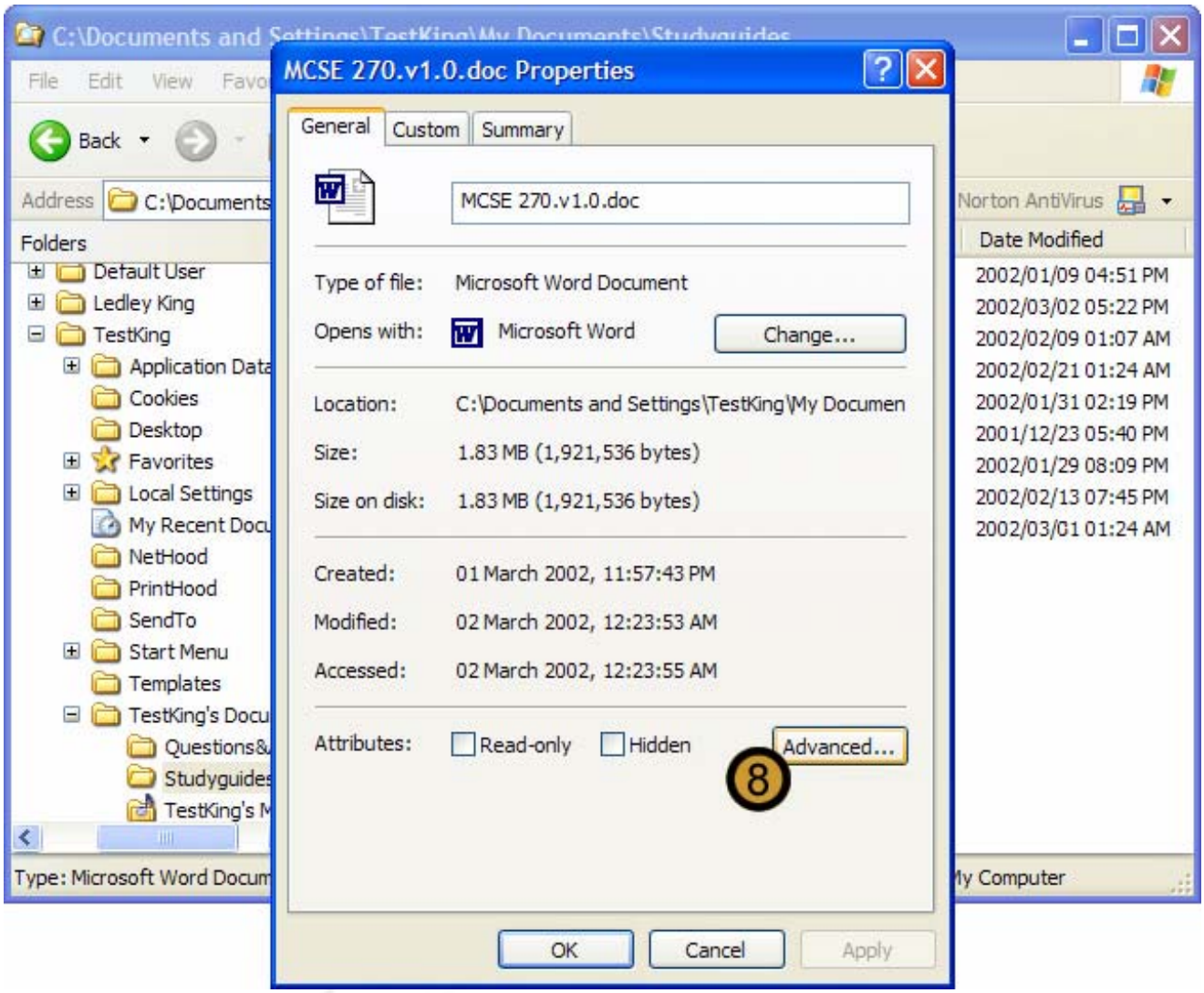


Note: You can only encrypt files and folders that are located on volumes that have been formatted with the **NTFS file system**.

5. In Windows Explorer locate and open the folder that contains the file you want to encrypt

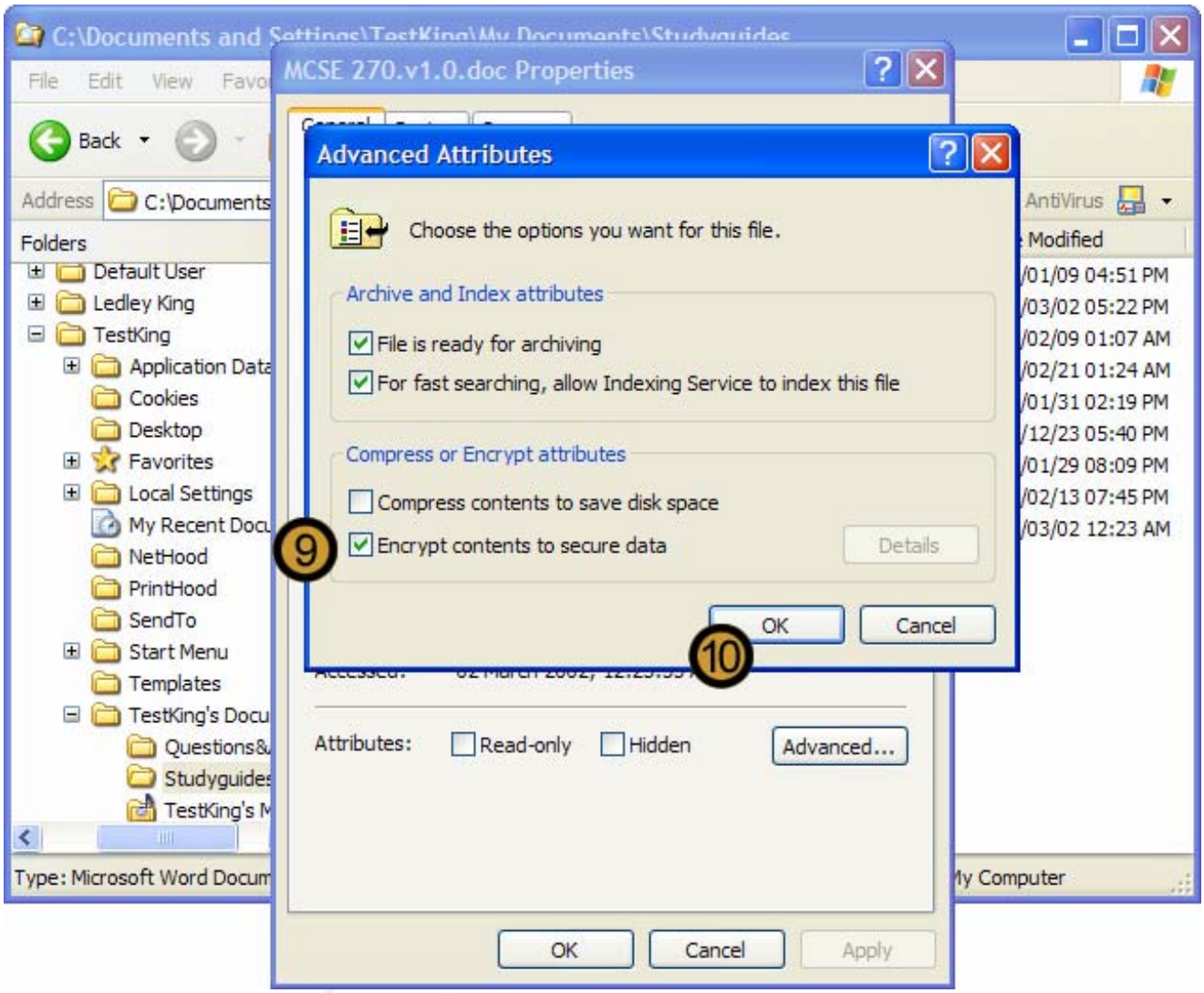
6. Right-click on the file you want to encrypt.

7. On the drop down dialog box, click **PROPERTIES**



The selected FILE OR FOLDER dialog box appears

8. On the selected FILE OR FOLDER dialog box, click **ADVANCED ...**

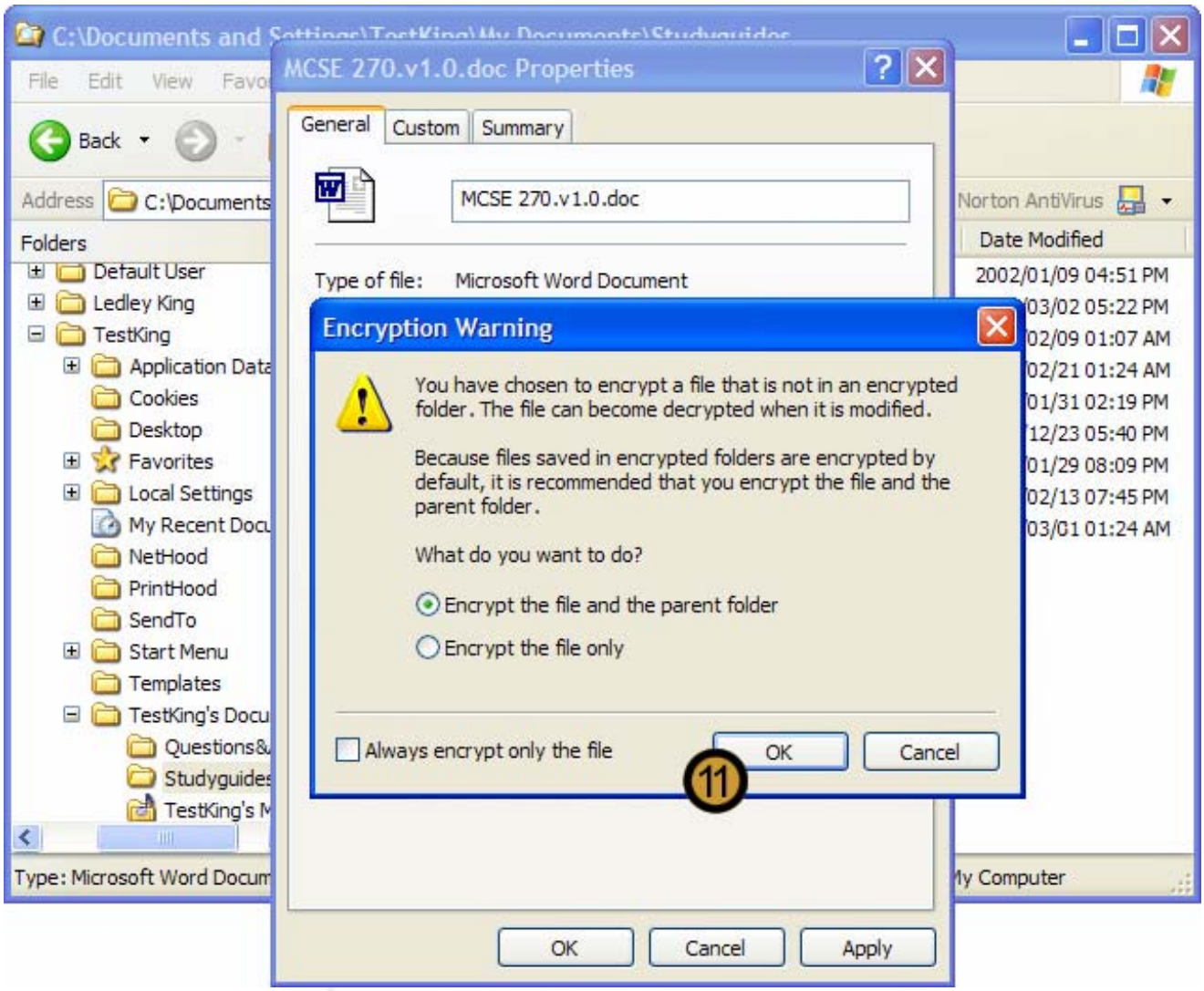


The ADVANCED ATTRIBUTES dialog box appears

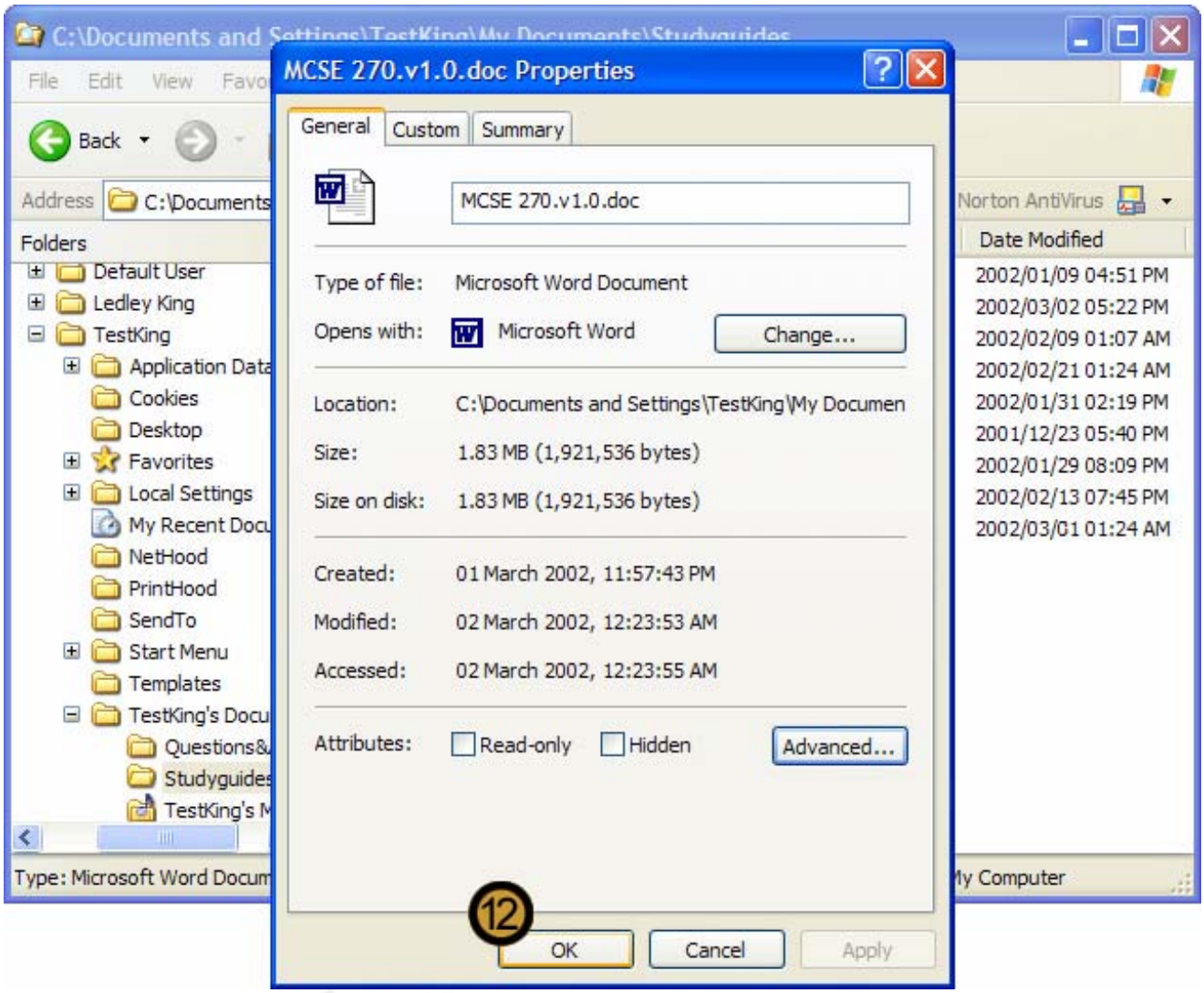
9. In the COMPRESS OR ENCRYPT ATTRIBUTES section of the ADVANCED ATTRIBUTES dialog box, select the **ENCRYPT CONTENTS TO SECURE DATA** check box

> **Note:** You cannot encrypt files that have been compressed and you cannot compress encrypted files. Therefore, when you attempt to encrypt a compressed file, as we are doing in this example, the COMPRESS CONTENTS TO SAVE DISK SPACE check box is automatically cleared.

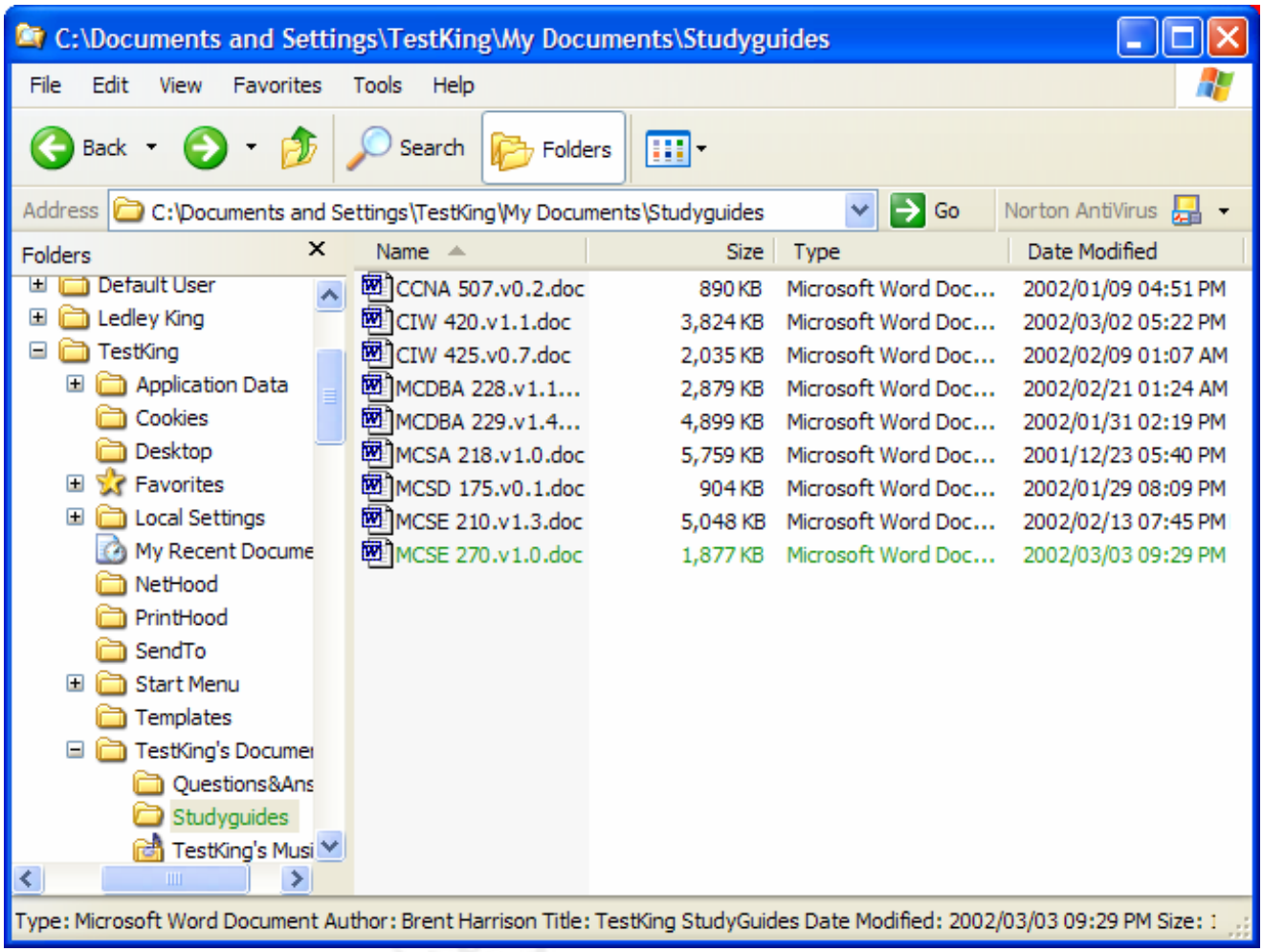
10. Click **OK**



11. Click **OK** to confirm that you want to encrypt the file or folder



12. Click **OK** to close the selected FILE OR FOLDER dialog box



The file is now encrypted and its encryption state is indicated by an alternative color

INDEX