Microsoft® Windows® xp Professional™

Step-by-Step Guide to Securing Windows XP Professional with Service Pack 2 in Small and Medium Businesses

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Overview

The ever-growing threat of malicious code – such as worms, viruses, and Trojan horses – makes it critical for all customers to take immediate action to help lock down their desktop and laptop systems. This guide explains how to implement the security measures recommended in the Microsoft® *Windows XP Security Guide* in a small or medium business environment without an Active Directory® directory service deployment. These recommendations help ensure that your desktop and laptop systems running Windows® XP Professional Service Pack 2 (SP2) are more secure from the majority of current security threats. These recommendations also help ensure that users can continue to be efficient and productive with their computers. In addition to the advanced step-by-step guidance in this document, you will also find information on the top security recommendations that Microsoft is making to all customers, from home users to enterprise workers. These recommendations include:

- Use a firewall such as Windows Firewall, which is included in Windows XP SP2 (and replaces the Internet Connection Firewall).
- Use Microsoft Windows Update to get and keep your PC up-to-date.
- Install antivirus software and ensure it is up-to-date.

This guide provides step-by-step deployment guidance and troubleshooting advice for information technology (IT) professionals and system administrators in a small to medium sized organization.

For more information on the particular settings that are applied by following this guidance and their potential impact, please refer to the complete *Windows XP Security Guide* at http://go.microsoft.com/fwlink/?LinkId=14839. To create customized security templates based on the specific needs of your organization, refer to the Threats and Countermeasures Guide at http://go.microsoft.com/fwlink/?LinkId=15159.

Who Should Read this Guide

You should read this guide if you are planning to deploy Windows XP, or if you are currently administering a number of computers running Windows XP Professional and want to implement a base level of security and protect your desktops and laptops with minimal impact on end users.

This guide is written for the average small or medium business administrator who may not have extensive training on Microsoft products but needs a quick, step–by–step guide to securing Windows XP in their organization.

This guide does not address the wide variety of needs and configurations that may be required in a large organization. Additionally, it may not fully address the specific security needs of some organizations. For additional security options and customization information, please refer to the *Windows XP Security Guide*.

What to Expect

As with any security recommendations, this guidance strives to find the right balance between enhanced security and usability. The recommendations provided in this document will work successfully for Windows XP Professional deployments in a wide variety of environments. However, there are several key points that you should note before implementing these recommendations.

This guide should not be used to secure Windows XP desktops or laptops that are members of a domain. A domain is a networked set of computers that share a common account database and can be managed as a group. Additionally, this guide should not be used for computers running Windows XP Home Edition.

This step-by-step guide is focused on organizations that manage individual user accounts on each Windows XP Professional computer. In organizations where all users share a common username and password, or organizations where users have multiple accounts on different computers that use the same password, additional steps must be taken prior to using this guidance. Such practices are not secure and the steps recommended in this guide will not work in these environments.

Connectivity to Windows 98 and Windows NT

If the recommendations in this guidance are used, your Windows XP desktops and laptops will be capable of communicating more securely with other computers running Windows XP, Windows 2000, and Windows Server™ 2003. However, Windows XP desktops and laptops may have difficulty sharing files, folders, or printers with Windows 98 or Windows NT® 4.0 systems. Windows 98 and Windows NT 4.0 are older technologies that are more difficult to secure against today's security threats.

The use of Windows XP, Windows 2000, and Windows Server 2003 provide small and medium businesses with a security solution that helps safeguard your important business documents from the threat of viruses and attackers while providing you with the most reliable Microsoft desktop to date. Windows XP Professional is the most reliable Windows operating system yet–much more reliable than Windows 98 SE. Only Windows XP, Windows 2000, and Windows Server 2003 include the new security features and functions used in this guide. For additional reasons to consider upgrading Windows 98 and NT clients to Windows XP, see "Top 10 Reasons Windows XP Professional Is Right for Small Business" at www.microsoft.com/windowsxp/pro/evaluation/whyupgrade/sorgtop10.mspx.

For information regarding how to secure Windows XP systems that are members of a domain, or that need to communicate with Windows NT 4.0 workstations and servers or Windows 98 clients, please refer to the complete *Windows XP Security Guide*.

Changes to Password Requirements

After implementing this guidance, your users will be required to maintain a complex password of at least 8 characters and to change that password every 42 days.

In addition to changing passwords frequently, the most productive security change that you can implement is encouraging your users to choose strong passwords. Weak passwords are one of the greatest security risks in any organization. Help your users by explaining that they can use "pass phrases" instead of passwords. An easy to remember phrase that includes numbers, uppercase and lowercase letters, and spaces or symbols is much more secure than a single word.

Running Programs as a Local User

A common issue in many organizations is the prevalence of users that log on to their laptop or desktop with administrative credentials. All user accounts should be members of the Users group. Users should not be allowed to log on routinely with accounts that are members of the Administrators group. By enforcing this change, users will not be able to install unapproved software that may contain viruses or other types of potentially dangerous code.

Implementing this requirement may be challenging, but Windows XP Professional with logo certified applications makes implementation easier. Applications that are not logo-certified may not run correctly for users without administrative privileges. For a list of logo-certified applications, look for software labeled "Designed for Windows XP" in the Windows Catalog at www.microsoft.com/windows/catalog/.

An administrator must implement the recommendations in this guide, but the settings provide the necessary functionality to allow the laptop or desktop to be run by someone who is not a member of the Administrators group on a day-to-day basis. After the security settings recommended in this guide are implemented, they apply to all users logging on to the desktop or laptop computer, including the Local Administrator.

Verifying Windows XP Service Pack 2

This guide is written for users of Windows XP with SP2 installed. Before following the steps in this guide, you should verify that you are running the correct version of Windows XP.

▶ **To determine what version of Windows XP you're running**

1. Log on to the Windows XP client.
2. Click **Start**, click **Run**, type **Winver** and then press **ENTER**.

The version information that displays should indicate that you are running SP2. If you are not running SP2, you need to download and install it before proceeding. Windows XP SP2 can be obtained from the Windows XP Service Pack 2 page on Microsoft.com at www.microsoft.com/technet/prodtechnol/winxppro/maintain/winxpsp2.mspx.

Securing your Laptops and Desktops

The following sections provide you with step–by–step instructions for downloading and installing the password and security tools and templates provided with the *Windows XP Security Guide*. Subsequent sections provide additional instructions to help you secure your Windows XP systems. The main tasks are:

1. Downloading the security tools and templates to your desktop or laptop computer.
2. Importing the password and security policy templates to your computer.
3. Applying the policies to your computer.

1. Downloading the Windows XP Security Tools and Templates

A security template is a file that represents a recommended security configuration. Security templates are applied to a system by importing them to a desktop or laptop computer. This section shows you how to download the pre-built security tools and templates (detailed in the *Windows XP Security Guide*) to secure your desktop and laptop systems.

▶ **To download the security tools and templates**

1. Log on to the Windows XP client with an account that has administrative rights.
2. Open a Web browser and navigate to the *Windows XP Security Guide* page on the Microsoft Download Center at http://go.microsoft.com/fwlink/?LinkId=14840.
3. On the bottom of the page, in the **Files in this Download** section, select the **Windows_XP_Security_Guide_v1.5.exe** file.

4. In the **File Download - Security Warning** dialog, click **Save**.
5. When prompted for a location, select **Desktop** and click **Save**.
6. In the **Download Complete** window, click **Run**.
7. In the **Internet Explorer - Security Warning** dialog, click **Run**.
8. In the **WinZip Self-Extractor** window, click **Browse**.
9. Select **My Documents** and click **OK**.
10. In the **WinZip Self-Extractor** window, click **Unzip**.
11. After all files have finished extracting click **OK**.
12. In the **WinZip Self-Extractor** window, click **Close**.

2. Importing the Password and Security Policies

After you have downloaded and extracted the security tools and templates, perform the following steps to import the password and security policies to your stand-alone computer.

The password policy template enforces the requirement that users choose complex passwords that are greater than 8 characters in length. In addition, it requires users to change their password every 42 days. The policy monitors for failed attempts to log on to the computer. If 50 failed logon attempts occur within 30 minutes, the account is locked for 30 minutes, or until an administrator manually unlocks it.

The security policy template configures settings that ensure only valid users can connect to the computer, that only administrators can back up and restore files on the computer, and that only administrators can add new drivers to the computer.

You will use the **SA Enterprise XP Client - Desktop.cmd.txt** or the **SA Enterprise XP Client - Laptop.cmd.txt** file (both are included with the *Windows XP Security Guide*) to perform this task.

▶ **To import the recommended password and security policies**

1. From **My Documents**, open the **\Windows XP Security Guide\Tools and Templates\Security Guide\Stand Alone Clients** folder.
2. On the **Tools** menu, click **Folder Options**.
3. Click the **View** tab, clear the **Hide extensions for known file types** checkbox, and then click **OK**.
4. Right-click the **SA Enterprise XP Client - Desktop.cmd.txt** file and select **Rename**.
5. Rename the file to **SA Enterprise XP Client - Desktop.cmd**, press **ENTER**, and click **Yes** in the **Rename** dialog box.
6. Double-click the **SA Enterprise XP Client - Desktop.cmd** file to import the password and security policies

Note: If you are configuring a laptop, rename and double-click the SA **Enterprise Client-Laptop.cmd.txt file** instead of the **SA Enterprise XP Client - Desktop.cmd.txt** file.

Important: Do **not** select the High Security scripts unless you have read the Windows XP Security Guide and understand the impact they may have on usability.

3. Applying the Policies

To apply the password and security policies to your desktop or laptop computer, restart the computer. When it restarts, the new policies will be applied.

If you encounter any problems, refer to the "Troubleshooting" section later in this document.

Additional Recommendations

Implementing the recommended security templates is a great start to securing your desktop or laptop computer. In addition, there are several other security measures that you should consider taking, including:

- Converting your file system to NTFS
- Using Windows Firewall
- Using antivirus software
- Keeping up-to-date with security patches

These topics are discussed in the following sections.

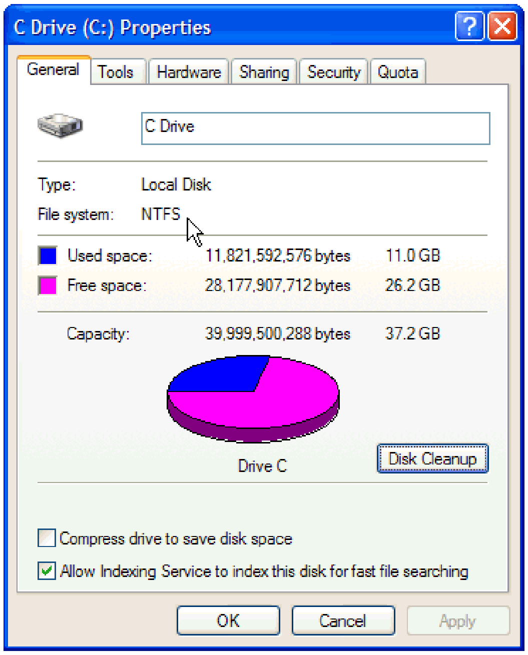
Converting your File Systems to NTFS

A file system organizes directories and files on a computer. During the Windows XP setup process, computers could either be configured to use the FAT32 or the NTFS file system.

FAT32 is an older technology used by previous versions of Windows. The NTFS file system is faster and more secure than previous file systems. For optimal performance and security of the operating system, you should use NTFS on all file system partitions on your computer.

▶ **To check the file system type on your computer**

1. On the **Start** menu, click **My Computer**.
2. Right-click the drive letter you want to check and select **Properties** from the menu.
3. The **File System** type should be NTFS. If it is not, you can use the **Convert.exe** utility to convert from FAT16 or FAT32 to NTFS.



C Drive

Type: Local Disk

File system: NTFS

🟦	Used space:	11,821,592,576 bytes	11.0 GB
🟪	Free space:	28,177,907,712 bytes	26.2 GB
	Capacity:	39,999,500,288 bytes	37.2 GB

□ Compress drive to save disk space

☑ Allow Indexing Service to index this disk for fast file searching

Figure 1
Displaying drive properties

Repeat this process for all disks on the computer. Even if the file system was configured as FAT32 when the operating system was installed, it can be easily converted to NTFS to provide additional security.

To convert the file system to NTFS, take note of the name of the disk otherwise known as the volume label (**C Drive** in the preceding example) and complete the following steps.

▶ **To convert the file system to NTFS**

1. On the **Start** menu, click **Run**, type **cmd**, and then click **OK**.
2. At the command prompt, type the following, where *drive letter* is the drive you want to convert:

   Convert *drive letter*: **/fs:ntfs**

3. You will be prompted to enter the current volume label for the drive. Type the volume label that was identified earlier. Press **ENTER**.
4. When the conversion is complete, exit the command prompt by typing **EXIT**.

> **Note:** If you are attempting to convert the drive where the operating system is installed, you may be prompted to schedule the conversion to occur the next time the system is restarted. If this occurs, type **Y** and reboot the computer.

Using Windows Firewall

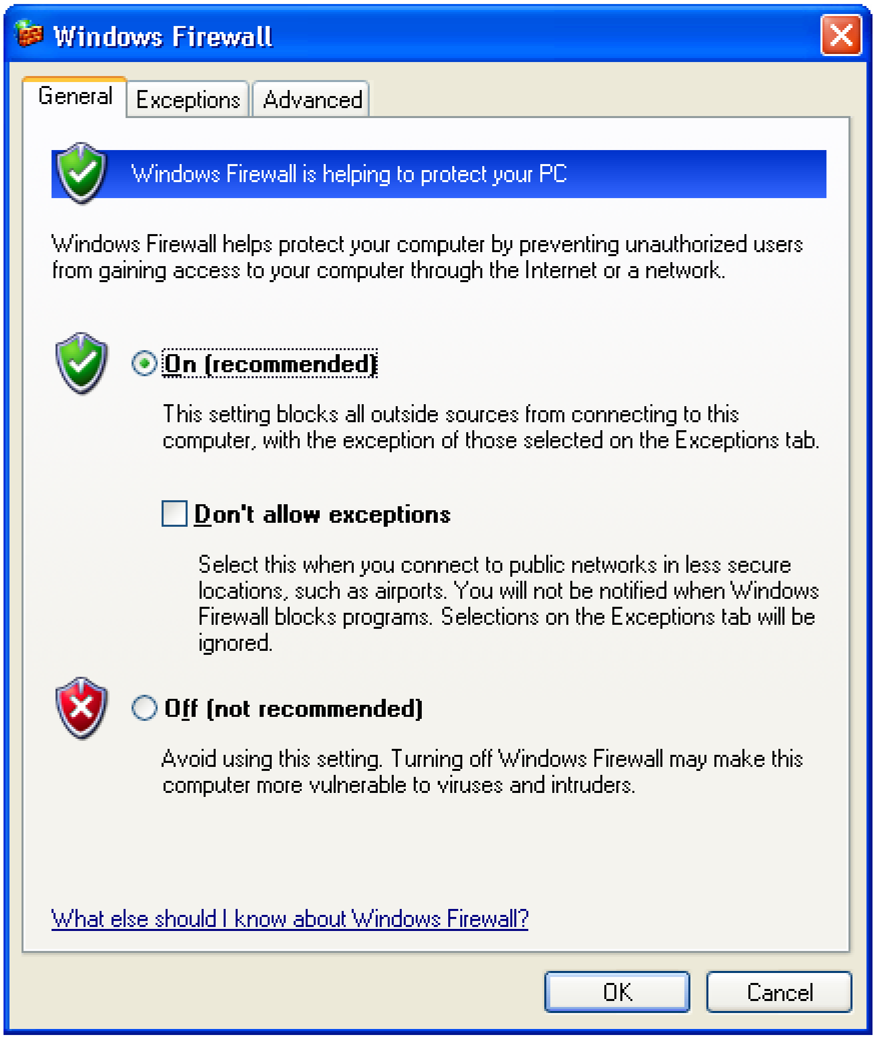
An Internet firewall can help prevent outsiders from accessing your computer through the Internet. Firewalls come in two forms, software and hardware, and they provide a protective boundary that helps screen out unwanted Internet invaders.

A firewall can screen for malicious Internet traffic such as human attackers, worms, and certain types of viruses before they can cause problems on your system. In addition, some firewalls can help keep your computer from participating in attacks on others without your knowledge. A firewall is especially important if you are always connected to the Internet, such as when you have a broadband cable or digital subscriber line (DSL or ADSL) connection.

The Microsoft Windows Firewall (formerly called Internet Connection Firewall or ICF) is a feature included in SP2 to help protect your system or network connection to the Internet. Windows Firewall is on in most configurations and should be left on. To enable or verify the Windows Firewall settings, you can use the following steps.

▶ To enable Windows Firewall

1. On the **Start** menu, click **Control Panel**.
2. In the **Control Panel**, double-click **Windows Firewall**.
3. Select **On (recommended)**.



Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

● **On (recommended)**

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ **Don't allow exceptions**

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

○ **Off (not recommended)**

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

Figure 2
Turning on Windows Firewall

4. Click **OK**.

These changes will take effect immediately and protect your network connection against many types of attacks. Windows Firewall is very powerful and it is highly recommended that you enable it. However, to protect the primary Internet connection of an organization, Windows Firewall is not a replacement for a true dedicated firewall. For more information on protecting your network with a firewall, see the Internet Security and Acceleration page at www.microsoft.com/ISAServer/.

Note that after you install SP2, some programs may seem not to work. By default, Windows Firewall is enabled and blocks unsolicited connections to your computer as well as unauthorized applications that open ports for inbound connections. For more information on this type of situation and how to fix it, see Microsoft Knowledge Base article 842242, "Some programs seem to stop working after you install Windows XP Service Pack 2" at http://support.microsoft.com/?kbid=842242.

Using Antivirus Software

An antivirus software program will help protect your computer against most viruses, worms, Trojan horses, and other malicious code. Many new computers come with antivirus software already installed. However, antivirus software requires a subscription to stay up-to-date. If you don't have a current subscription for these updates, your computer is probably vulnerable to new threats.

Computer viruses are programs that are designed to replicate themselves and spread to as many computers as possible. Viruses and other forms of malicious software have been around for years. Today's viruses can replicate themselves and use the Internet and e-mail applications to spread across the world within hours.

Antivirus software continually scans your computer for viruses and helps detect and remove them. It performs these scans based on identifying *signatures* of known viruses and malicious code. Installing antivirus software only solves part of the problem; keeping the antivirus signature files up-to-date is critical to maintain a secure desktop or laptop computer.

User education regarding safe e-mail practices is another critical step in preventing virus attacks. Users should not open e-mail messages or take action on an e-mail attachment unless they are expecting the file and it is sent from a trusted source. All e-mail attachments should be scanned with antivirus software prior to its execution. Most antivirus software programs perform this type of scan automatically, but users should be made aware of this necessity.

For a list of the software vendors who provide antivirus software that is compatible with Windows XP, see Microsoft Knowledge Base article 49500, "List of Antivirus Software Vendors" at http://support.microsoft.com/?kbid=49500. For more information about complete antivirus solutions and strategies, see the Antivirus Defense-in-Depth Guide at http://www.microsoft.com/downloads/details.aspx?FamilyID=f24a8ce3-63a4-45a1-97b6-3fef52f63abb&displaylang=en.

Keeping Up-to-Date with Security Patches

Your Windows XP operating system includes the Automatic Updates feature, which can automatically download the latest Microsoft security updates while your computer is on and connected to the Internet. To get the most out of Automatic Updates, run a Windows Update scan on your computer first.

▶ To run a Windows Update scan

1. Click **Start**, click **All Programs**, and then click **Windows Update**.
2. Follow the directions on your screen. Windows Update will scan your computer and provide a pre-selected list of critical updates.

   Tip: To reduce download times, run Windows Update when you will not be using your computer for other tasks. Your download times will vary depending on how long it has been since you last updated your computer, the number and size of files being downloaded, and your modem speed. Slower modems may take several hours to download all recommended updates the first time you use Windows Update.

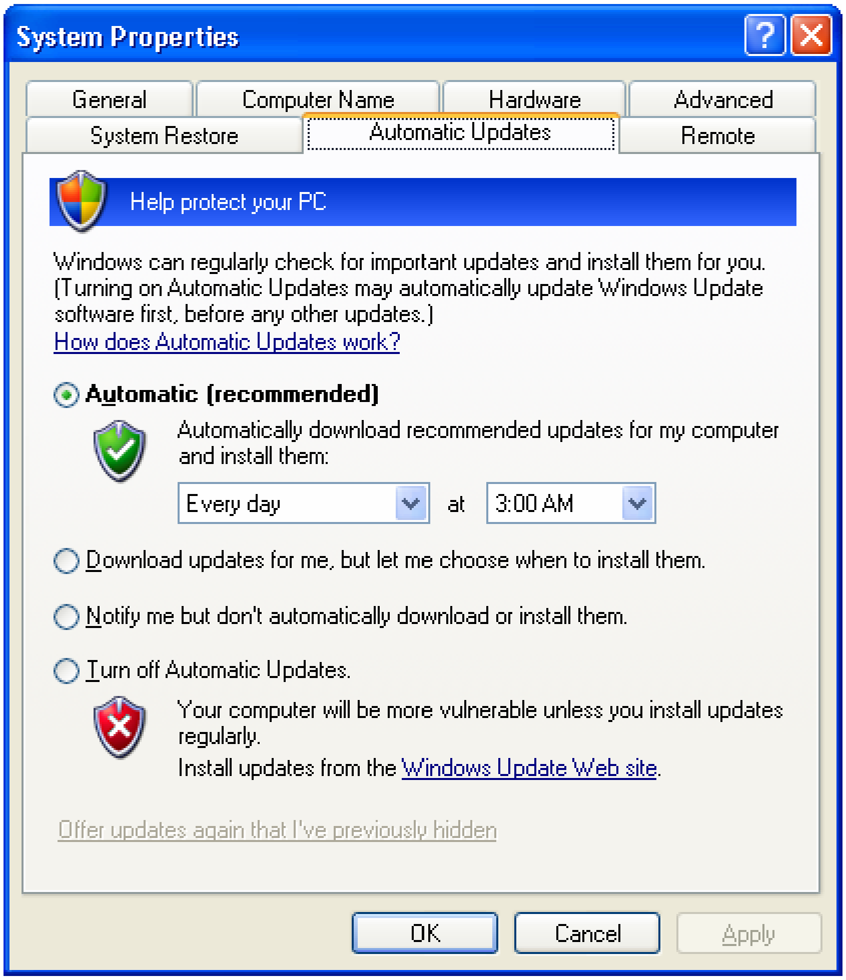
3. Install the updates.

   Tip: Some updates have prerequisites; therefore, you may be asked to install certain updates and then reboot your computer. Be sure to return to Windows Update after rebooting to check for any additional downloads. You may need to do this several times.

Now that your Windows XP is up to date, establish a regular maintenance schedule with Automatic Updates.

▶ To configure your computer for automatic updates

1. On the **Start** menu, click **Control Panel**.
2. Double-click **System**.
3. Click the **Automatic Updates** tab, and then select **Automatic (recommended)**.
4. Select the **day** and **time** for the updates to occur.
5. Click **OK** to close the **System Properties** window.



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

How does Automatic Updates work?

● **Automatic (recommended)**

Automatically download recommended updates for my computer and install them:

Every day at 3:00 AM

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

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

○ Turn off Automatic Updates.

Your computer will be more vulnerable unless you install updates regularly.

Install updates from the Windows Update Web site.

Offer updates again that I've previously hidden

Figure 3

Configuring automatic updates

After you enable Automatic Updates, a message will display above the Task Bar to notify you when new patches, fixes, and updates are available for download. The new updates will be automatically applied to the computer according to the schedule you specified.

Troubleshooting

When implementing these recommendations you may encounter error messages or, in severe cases, applications that do not work after the policies have been applied. This section provides you with information about several of the common error messages you may encounter, as well as information on returning the security configuration of the computer to a default state.

Common Error Messages

The following error messages may appear during the application of these policies.

Winzip Self-Extractor: Could not create…

When you attempt to extract the *Windows XP Security Guide*, you may see an error message that says, "Could not create "<Path Name>/Windows XP Security Guide"– unzip operation cancelled." This message likely means that the account you are using does not have access to the path you have chosen. To correct this situation, log off and then log back on with an account that has administrative rights on the laptop or desktop.

Security Configuration and Analysis snap-in: Access is denied. Import Failed

This message may occur when using the Security Configuration and Analysis snap-in. It is usually an indication that the person performing the import of the template does not have administrative rights. Please ensure that the account you are using to apply the security templates has administrative permissions on the client computer.

Security Configuration and Analysis snap-in: An unknown error occurred…

When attempting to open an existing database with the Security Configuration and Analysis snap-in, you may see the following error: "An unknown error occurred when attempting to open the database." This message means the database may be configured with read-only permissions. To resolve this error, either create a new database by specifying a different name or remove the read-only permissions on the existing database.

If this error occurs when creating a new database, ensure that you are attempting to create the database in a location where you have adequate permissions to create new files.

Dialog Box: It is an offense to continue…

This message is a generic, customizable statement that is used to deter unauthorized users from using your computer. Your legal advisor should approve this message for use on all of your desktop and laptop computers. For detailed information on how to modify this setting, please refer to page 61 of the *Windows XP Security Guide*.

NTFS Conversion: Convert cannot gain exclusive access…

When trying to convert a FAT16 or FAT32 partition to NTFS, you may see the following message: "Convert cannot gain exclusive access to the *drive letter* drive, so it cannot convert it now. Would you like to schedule it to be converted the next time the system restarts? <Y/N>."

This situation occurs when the volume that you are attempting to convert is in use–for example, if the drive that you want to convert is the same drive on which Windows XP is running. To resolve this issue, type **Y** at the command prompt. The volume or drive will be converted to NTFS the next time you start your computer.

Returning to the Default Settings

If you encounter problems after the security templates have been applied, you can reset the security settings to the operating system defaults.

▶ **To restore the default security settings**

1. On the **Start** menu, click **Run**, type **cmd**, and then click **OK**.
2. Type "**secedit /configure /cfg %windir%\repair\secsetup.inf /db secsetup.sdb /verbose**" (without the quotation marks), and then press **ENTER**.

This process may take several minutes to complete. After completion, you should see a message that states: "Task is completed. Some files in the configuration are not found on this system so security cannot be set/queried. It's ok to ignore." This message is expected and does not require you to do anything.

More Information

The following information sources were the latest available on topics closely related to securing Windows XP Professional at the time this guide was released to the public.

For more information about the extensive changes in SP2, see "Changes to Functionality in Microsoft Windows XP Service Pack 2" at http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2chngs.mspx.

For more information on the Windows XP Security Guide, see the Microsoft Windows XP Security Guide Overview at http://go.microsoft.com/fwlink/?LinkID=14839.

For more information on methods to help protect your PC, see the Protect Your PC page at http://www.microsoft.com/security/protect/default.asp.

For more information on security threats and countermeasures, see the Threats and Countermeasures Guide at http://go.microsoft.com/fwlink/?LinkID=15159.

For information on the Administrative Templates for Windows XP, see the article "The role of Administrative Templates" at http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/adminad.mspx.

For more information on Windows Automatic Updates, see Microsoft Knowledge Base Article 303525, "How to configure and use Automatic Updates in Windows XP" at http://support.microsoft.com/?kbid=306525.

For more information on upgrading to Windows XP, see the Windows XP Professional Upgrade Center at http://microsoft.com/windowsxp/pro/howtobuy/upgrading/default.asp.