



Microsoft Shared Computer Toolkit for Windows XP Handbook

The Microsoft Shared Computer Toolkit for Windows XP, v1.0

The information in this document and any document referenced herein is provided for informational purposes only, is provided AS IS AND WITH ALL FAULTS and cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user's particular environment. RELIANCE UPON THIS DOCUMENT AND ANY DOCUMENT REFERENCED HEREIN IS AT THE USER'S OWN RISK.

MICROSOFT CORPORATION PROVIDES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION CONTAINED IN THIS DOCUMENT AND ANY DOCUMENT REFERENCED HEREIN. Microsoft Corporation provides no warranty and makes no representation that the information provided is in this document or any document referenced herein is suitable or appropriate for any situation, and Microsoft Corporation cannot be held liable for any claim or damage of any kind that users of this document or any document referenced herein may suffer. Your retention of and/or use of this document and/or any document referenced herein constitutes your acceptance of these terms and conditions. If you do not accept these terms and conditions, Microsoft Corporation does not provide you with any right to use any part of this document or any document referenced herein.

Complying with the applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter within this document. Except as provided in any separate written license agreement from Microsoft, the furnishing of this document does not give you, the user, any license to these patents, trademarks, copyrights or other intellectual property.

© 2005 Microsoft Corporation. All rights reserved.

Microsoft, MS DOS, MSN, Windows XP Professional Edition, and Windows XP Home Edition are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Overview	7
Audience.....	7
Tools Summary	8
Supported Environments.....	9
Workgroups.....	9
Domains.....	9
Chapter Summary	9
Style Conventions	11
Resources and Community	12
Download the Toolkit	12
Support Information.....	13
Other Support Resources.....	13
Chapter 1: Installation.....	15
Software Requirements.....	15
Software Recommendations.....	16
Install the Toolkit from the Download Center	16
Install the Toolkit from CD.....	17
Work with Script Blocking Software	17
Getting Started.....	17
Uninstall the Toolkit.....	19
Preserve User Documents	20
Chapter 2: Prepare the Disk for Windows Disk Protection.....	21
Windows Disk Protection Requirements.....	21
Resize an Existing Partition	23
Size the Disk During Windows XP Setup.....	24
Chapter 3: Profile Management.....	27
Create Local Limited User Accounts	27
Set Up Local User Profiles	28
Optional Activity: Customize the All Users Start Menu	30
Optional Activity: Customize a User's Start Menu	31

Chapter 4: User Restrictions	33
Restrict a Local User Profile	33
General Settings	34
Locking a Profile	35
Recommended Restrictions for Shared Accounts.....	35
Start Menu Restrictions	36
General Windows XP Restrictions.....	37
Internet Explorer Restrictions	37
Microsoft Office Restrictions.....	38
Software Restrictions	38
Optional Restrictions	39
Additional Start Menu Restrictions.....	39
Additional General Windows XP Restrictions	39
Additional Internet Explorer Restrictions.....	39
Additional Software Restrictions.....	39
 Chapter 5: A Restricted User Experience.....	 41
A Typical Restricted Desktop.....	41
How to Test Restricted User Profiles.....	41
Online Resources for Using Public Computers.....	43
The Accessibility Tool.....	43
 Chapter 6: Windows Disk Protection.....	 45
Turn On Windows Disk Protection.....	45
Hibernation and Windows Disk Protection	46
Windows Disk Protection Status.....	47
Critical Updates	47
Other Updates from Microsoft	48
Save Changes When Windows Disk Protection Is On	48
Retain Changes When Windows Disk Protection Is On.....	49
Retain Changes Indefinitely When Windows Disk Protection Is On...	49
Improve the Performance of Windows Disk Protection.....	49
Defragment the Windows Partition.....	50
Move the Virtual Memory Paging File	50
Placing Event Logs on a Persistent Partition.....	51
Manage the Protection Partition	52
Place the Protection Partition on a Different Disk	52
Specify the Size of the Protection Partition.....	53

Chapter 7: Security Checklist	55
Setup Checklist	55
Maintenance Checklist (Monthly)	55
Toolkit Administrator Security	56
Physical Network Security	56
Physical Security	56
BIOS Protection	57
Software Updates	57
Firewalls	58
Antivirus Software	58
Antispyware	58
Web Filtering	58
 Chapter 8: Troubleshooting	 59
Install and Uninstall	59
Script-Blocking Security Software	60
Profile Management	61
User Restrictions	62
Windows Disk Protection	63
General Errors	66
 Chapter 9: Advanced Scenarios	 67
Store Persistent User Data	67
Storing Persistent User Data on a Separate Partition	67
Using Removable USB Drives or Network Locations	69
Quickly Install Software for a Restricted User	70
Configure a User Start Menu to Not Use the All Users Profile	70
Restrict a Shared Administrative Account	71
Block ActiveX Controls in Internet Explorer	72
Use Simple Site Filtering to Control Internet Access	73
Use a Central Script for Common Client Updates	73
Restrict Children on a Family Computer	74
Example 1: Restrict a Young Child	74
Example 2: Restrict a Teenager	75
Automate User Restrictions Using Restrict.wsf	75
Create a Mandatory Profile for Multiple Users	76
Image or Clone a Toolkit-Secured Computer	77
Configure a Reference Computer	77
Use the System Preparation Tool	78
Create and Transfer a Hard Disk Image	78
Post-Imaging Activities	79

Chapter 10: The Shared Computer Toolkit in Domain Environments.....	81
The Shared Computer Toolkit and Active Directory.....	81
Windows Disk Protection on Domain-Joined Computers.....	82
Machine Account Passwords in a Domain Environment.....	82
Central Software Management and Windows Disk Protection..	82
Mobile Computers and Windows Disk Protection.....	83
Managing Windows Disk Protection Using DiskProtect.wsf	83
Create a Persistent Local User Profile for a Domain Account.....	83
Create Persistent Local User Profiles for all Accounts.....	83
Group Policy Restrictions for Domain Accounts	84
Using Group Policy to Configure Software Restriction Policies .	85
Restart at Logoff Using a Logoff Script.....	87
User Restrictions for Unrestricted Domain Accounts.....	88
User Profiles in Other Languages.....	89
MUI Requirements.....	90
How to Install MUI.....	90
How to Change the Input Language	90
Appendix A: Technical Primer.....	93
User Accounts and Profiles	93
How the Profile Manager Tool Works.....	95
How the User Restrictions Tool Works.....	95
Disks and Partitions.....	95
How the Windows Disk Protection Tool Works	96
The Protection Partition.....	96
The Critical Updates Process	97
Acknowledgements	99
Links	101
Shared Computer Toolkit Web Pages	101
Microsoft Web Sites.....	101
Third-Party Tools and Resources.....	102
Helpful Articles.....	103
Index	105



Overview



shared computers

Also known as public access computers, Internet kiosks, lab computers, and instructional computers, depending on their purpose.

Shared computers are commonly found in schools, libraries, Internet and gaming cafés, community centers, and other locations. Often, staff members who lack technical training are asked to manage shared computers in addition to their primary responsibilities.

Managing shared computers can be difficult, time-consuming, and expensive. Unrestricted, users can change the desktop appearance, reconfigure system settings, and introduce spyware, viruses, and other harmful programs. Fixing damaged shared computers costs significant time and effort.

User privacy is also an issue. Shared computers often use shared accounts where Internet history, online documents, and cached Web pages are available from one person to the next.

The Microsoft® Shared Computer Toolkit for Windows® XP provides a simple and effective way to defend shared computers from untrusted users and malicious software, restrict untrusted users from system resources, and enhance and simplify the user experience. The Toolkit runs on genuine copies of Windows XP Professional, Windows XP Home Edition, and Windows XP Tablet PC Edition.

This overview section covers the following topics:

- Audience
- Tools summary
- Supported environments
- Chapter summary
- Style conventions
- Resources and community
- Download the toolkit
- Support Information



operators

People who are responsible for managing shared computers.

Audience

The Microsoft Shared Computer Toolkit for Windows XP is designed for people who install, configure, and manage shared computers in either public or private settings.

Throughout this Handbook, people who manage shared computers are referred to as *operators*. Shared computer operators include teachers, technology coordinators, librarians, and café staff who have technology skills that span from beginner to expert.

Tools Summary

The Toolkit includes the following graphical tools:



Important

Windows Disk Protection has special disk partitioning prerequisites. For more information, see Chapter 2, "Prepare the Disk for Windows Disk Protection."

- **Windows Disk Protection.** Protects the Windows partition (typically the C: drive) that contains the Windows operating system and other programs from being permanently modified during a user session. Disk changes made are cleared with each restart unless an administrator chooses to save them.
- **User Restrictions.** Restricts user access to programs, settings, Start menu items, and locks shared local user profiles against permanent changes. This tool is specifically for use in environments that do not use the Active Directory® directory service and Group Policy.
- **Getting Started.** Provides access to computer settings and utilities and helps first-time operators learn the Toolkit basics quickly.
- **Profile Manager.** Creates and deletes user profiles. Using the tool, you can create user profiles on alternative drives to allow the profiles to persist data even though Windows Disk Protection is on. You can also use the tool to comprehensively delete profiles that have been locked by the User Restrictions tool.
- **Accessibility.** Makes Windows accessibility options and utilities such as StickyKeys, FilterKeys, and Magnifier available to users who have been restricted from accessing Control Panel and other system settings.

The Toolkit also provides several command-line tools. In addition to a scriptable command-line version of each of the graphical tools, the Toolkit has the following:

- **Accounts.** Allows you to enable, disable, and list local user accounts.
- **AutoDemo.** Configures a computer with accounts and profiles so that you can demonstrate the Toolkit. This command should be run only on a demonstration computer, because it configures accounts and performs other Toolkit functions.
- **AutoLogon.** Configures an account to log on to the computer automatically. This tool is useful if you use third-party authentication software in place of Windows authentication (which is typical in some libraries and Internet cafés).
- **AutoRestart.** Configures an account so that a program runs automatically each time a user logs on with that account.
- **AutoRunOnce.** Configures an account so that a program runs automatically the next time a user logs on with that account. Subsequent logons are unaffected.
- **CriticalUpdates.** Forces the computer to download and install critical updates without waiting for the next critical updates cycle in Windows Disk Protection.
- **ForceLogoff.** Allows you to log off users or restart the computer.
- **SCTReport.** Creates a Shared Computer Toolkit report that can be used by Microsoft Support when troubleshooting issues with the Toolkit.
- **SleepWakePC.** Puts a shared computer into a sleep state at a specific time (to conserve energy) and then wakes it to perform scheduled critical updates.
- **Welcome.** Removes accounts listed on the Welcome screen, to ensure that users are not confused or tempted by administrative accounts in the Welcome logon list.

**domain**

Networked computers that share a central directory that contains user accounts and security information.

**Active Directory**

The Windows directory service for managing users and computers. For more information, see the official [Windows Server 2003 Active Directory](#) Web site.

Supported Environments

The Toolkit can be used in either workgroup or domain environments.

Workgroups

All of the tools in the Toolkit have been designed to help manage individual computers or computers that are members of Windows workgroups. The Toolkit does not need a server infrastructure— you can use it on one computer or hundreds of computers without requiring any server-based management tools.

To use the Toolkit on multiple computers, each computer must have the Toolkit installed. This will allow you to set up each computer as you like using User Restrictions, Windows Disk Protection, and the other tools. Chapters 1 through 7 describe the end-to-end process for using the Toolkit on workgroup computers.

Domains

The Toolkit was designed to help protect computers that are part of an Active Directory domain.

The Windows Disk Protection tool can be used in domain environments to protect computers from unwanted changes. Windows Disk Protection works well on domain-joined computers running Windows XP.

The User Restrictions tool was not designed for domain environments. If you provide, or want to provide, unique accounts and passwords to your patrons, or your computers are already part of a Windows domain, using Active Directory with Group Policy is a better solution for restricting user activities. Group Policy has the added benefits of greater flexibility and central management, whereas the User Restrictions tool is only intended for managing local shared accounts.

Domain account restrictions can be managed centrally using the Group Policy template included with the Toolkit, which offers most of the settings and restrictions available through the User Restrictions tool.

Operators of domain-joined computers should also read Chapter 10, “The Shared Computer Toolkit in Domain Environments.”

Chapter Summary

The first seven chapters in the Handbook follow the basic process that you will use to install and use the Toolkit and improve the security of your shared computer environment. The remaining chapters and appendix provide additional information that will help you to troubleshoot, perform advanced scenarios, and learn about topics related to the Toolkit.

Chapter 1: Installation

This chapter covers the prerequisites that a computer must meet before you install the Toolkit. It also covers how to validate Windows XP through the [Windows Genuine Advantage](#) program, install the Toolkit, and use the Getting Started tool.

**Important**

The first seven chapters represent the steps you should follow to install and use the Toolkit and improve the security of your shared computer environment.

Chapter 2: Prepare the Disk for Windows Disk Protection

This chapter helps you understand the requirements for using Windows Disk Protection. It covers the two best methods for ensuring sufficient unallocated disk space exists for Windows Disk Protection:

- Using a third-party partitioning utility such as PartitionMagic 8.0 to resize an existing partition that contains the Windows operating system and program files.
- Using Windows XP Setup to configure a primary partition and leave unallocated space on the disk.

Chapter 3: Profile Management

This chapter covers the creation of local shared accounts, creating profiles for each user account, and configuring each profile by customizing Windows settings, Start menus, and programs. The Profile Manager tool is used to create and copy user profiles on a shared computer.

Chapter 4: User Restrictions

This chapter describes how to use the User Restrictions tool to restrict and lock user profiles on the computer; to protect against unknown, untrusted users.

Chapter 5: A Restricted User Experience

This chapter illustrates the experience that typical users will have using a shared account that has been restricted with the User Restrictions tool. It provides an example of a typical restricted desktop, an introduction to the Accessibility tool, and describes available user resources. It covers how to test user accounts by logging on as each user to make sure that restrictions work as you intend.

Chapter 6: Windows Disk Protection

This chapter describes how to turn on Windows Disk Protection to clear changes to the disk with every restart and schedule critical software update installations. It also describes how to save disk changes or retain disk changes when Windows Disk Protection is on.

Chapter 7: Security Checklist

This chapter provides important information to improve the security of shared computers and the surrounding environment beyond what the tools in the Toolkit can automate.

Chapter 8: Troubleshooting

This chapter provides troubleshooting advice for each of the tools in the Toolkit.

Chapter 9: Advanced Scenarios

This chapter focuses on the most common advanced scenarios that operators may need when using the Toolkit to help manage a shared computer environment.

Chapter 10: The Shared Computer Toolkit in Domain Environments

This chapter describes using the Toolkit in environments that have one or more of the following:

- Active Directory and Group Policy
- Central software distribution services
- A need to provide multiple languages on each computer

Appendix A: Technical Primer

This appendix covers several technologies and features that are important to understand when you work with the Toolkit.

Acknowledgements

This section lists the people involved in developing the Shared Computer Toolkit.

Links



This section lists the full URL for all of the hyperlinks in this Handbook; for people reading a printed copy.

Index

The section lists common terms used in the Handbook with page number references.

Style Conventions

The following table lists the style conventions that are used in the Handbook.

Element	Meaning
Bold	Bold is applied to file names and user interface elements.
<i>Italic</i> - or - <Italic>	<p>Italic is applied to characters that the user types, but which they can choose to change. Italic characters that appear within angled brackets are placeholders which need specific values. Example:</p> <p><Filename.ext> indicates that you should replace the italicized <i>filename.ext</i> with another file name that is appropriate for your configuration.</p> <p>Italic is also used to represent new terms. Example: A <i>disk partition</i> is a logical compartment on a physical disk drive.</p>
Screen Text font	This font defines output text that displays on the screen.
Left margin text	The left margin is used for terms and definitions.
 Note	A Note alerts you to information that can help you to complete a task or understand a concept.
 Important	An Important notice alerts you to information that is essential to completing a task. This notice might also be used to warn you to take or avoid a specific action.
Procedures	Procedures appear in shaded boxes so that they stand out on the page.

Resources and Community

The Toolkit includes a number of resources with useful information about the Toolkit. The following resources are available in the Microsoft Shared Computer Toolkit program folder on the Start menu after you install the Toolkit:

- **Shared Computer Toolkit Handbook.** This Handbook provides detailed instructions for installing and using the Toolkit. The Handbook also covers advanced topics, best practices, and technical information.
- **Shared Computer Toolkit Help.** The help files included with the Toolkit detail the features and functionality of each tool.
- **Toolkit FAQ.** This Web page provides answers to frequently asked questions about the Toolkit.
- **Resources for Managing Shared Computers.** A Web site and newsgroup dedicated to helping organizations that have shared computers help and learn from each other—while meeting others in the shared access community.

To participate in discussions with other operators, see the [Windows Shared Access Newsgroup](#). It is intended as a place for you post questions, help others, and provide feedback on the Toolkit and this Handbook, including your ideas for future releases.

For users, the Toolkit installation adds two new resources to the All Users Start menu:

- **Online Resources for Using Public Computers.** An online Web site that contains links to resources for children, teenagers, and adults about how to use computers, learn more about Windows XP, and use the Internet safely.
- **Accessibility.** A shortcut to the Accessibility tool so that all users can access the accessibility features of Windows, even if they have been restricted.

Download the Toolkit

To download the Toolkit, visit the [Microsoft Shared Computer Toolkit for Windows XP](#) page of the Microsoft Download Center.

Downloading the Toolkit requires [Windows Genuine Advantage](#) validation.

Support Information

Support information for the Microsoft Shared Computer Toolkit for Windows XP is available through the following resources:

- [Shared Computer Toolkit](#) Web site
- [Frequently Asked Questions for the Shared Computer Toolkit](#)
- Known issues list on the [Shared Computer Toolkit Download Page](#)
- [Shared Computer Toolkit Handbook](#), particularly Chapter 9, "Troubleshooting"
- [Windows Shared Access Newsgroup](#), for posting free support queries and product questions
- [Product Support Services \(PSS\)](#) can be contacted for paid support, or if you already have a support agreement. Use the Shared Computer Toolkit Product ID when contacting PSS: **77695-100-0001260-04309**.

Other Support Resources

Other support resources related to shared computers, security, and Windows XP:

- [Resources For Managing Shared Computers](#)
- [Security Help and Support for IT Professionals](#)
- [Support Options for Windows XP Users](#)



Chapter 1: Installation

This chapter covers the following topics:

- Software requirements
- Software recommendations
- Install the Toolkit from the Download Center
- Install the Toolkit from CD
- Work with script-blocking software
- Getting started
- Uninstall the Toolkit



Important

These software requirements must be fulfilled before you install the Toolkit.



Important

Only the account that installs the Toolkit will have Start menu icons for the tools.



Note

Internet access is required to perform Windows Genuine Advantage validation.

Software Requirements

The Microsoft® Shared Computer Toolkit for Windows® XP requires the following:

- Windows XP Professional, Windows XP Home Edition, or Windows XP Tablet PC Edition.
- Windows XP [Service Pack 2 \(SP2\)](#) installed.
- Internet access to perform [Windows Genuine Advantage](#) validation.
- The [User Profile Hive Cleanup Service](#) is installed and running. This service ensures that profiles are fully unloaded upon logoff, which is required for the proper operation of the Toolkit.
- NTFS file system in place. FAT32 and other file systems do not meet the security requirements of shared computers. If your computer is not using NTFS, see [Knowledge Base article 307881](#) to learn how to convert it to NTFS before you install the Toolkit.

The Toolkit requires the Windows partition, the Program Files directory, and the default location for Documents and Settings to be on NTFS volumes. Typically these are all located on the C: drive, in which case the C: drive needs to use NTFS. For more information about NTFS, see the [Advantages of Using NTFS](#) section in the Windows XP Resource Kit.

Additionally, Windows Scripting and Windows Management Instrumentation (WMI) must be working correctly. The installer will ensure that all of these requirements are met and provide guidance if they are not.

Whether you download the Toolkit from Microsoft or install it from CD, Internet access is required to perform [Windows Genuine Advantage](#) validation. Validation is required for the tools to work.

**Important**

Some security software may report a suspicious or malicious script error during installation and when you use the Toolkit. If this happens, you need to authorize Toolkit scripts to execute. For more information, see Chapter 8, "Troubleshooting."

Software Recommendations

The Shared Computer Toolkit will not remove or stop malicious software that is already on the computer. The computer must be trustworthy before you install the Toolkit.

Microsoft recommends you have the following software installed:

- All of the latest critical updates from the [Microsoft Update](#) Web site.
- Ensure the computer is free of malicious software by having up-to-date antivirus and antispyware software installed and running.
- [Adobe Acrobat Reader](#) to view the PDF version of this Handbook.
- Trusted programs and Microsoft ActiveX® controls your patrons may require.

Some software is generally inappropriate for shared computers, depending on your specific usage scenarios. You should consider not installing or removing the following types of programs from shared computers:

- Desktop search utilities, because they may reveal information on the computer you don't want users to see.
- E-mail clients that require configuration, such as Microsoft Outlook® or Outlook Express, because they may take too long for users to use.
- Windows components, such as Fax Services and Internet Information Services (IIS).

**Toolkit administrator**

The administrative account that is used to install and use the Shared Computer Toolkit.

Install the Toolkit from the Download Center

You can download the Toolkit from the [Microsoft Download Center](#).

To download and install the Toolkit

1. Log on as the *Toolkit administrator*; a local administrative account that will use the tools in the Toolkit.
2. Download the installation file named **Shared_Computer_Toolkit_ENU.msi** from the [Shared Computer Toolkit](#) download page.
3. If prompted, first validate your copy of Windows XP through [Windows Genuine Advantage](#).
4. Double-click the downloaded installation file to start the installation.
5. Review the License Agreement page, and, if the terms are agreeable to you, click **I Accept the terms in the License Agreement**, and then click **Next**.
6. On the Customer Information page, you can click **Register Now** to complete the optional registration process.
7. On the Installation Folder page, click **Next**.
8. On the Ready to Install page, click **Install**.
9. On the Installation Complete page, click **Finish** to exit. If you leave the **View Getting Started** check box selected, the Getting Started tool should open.

Install the Toolkit from CD

If you received the Toolkit on CD with a physical copy of the Handbook, you can install the Toolkit from this CD.

To install the Toolkit from CD

1. Log on as the *Toolkit administrator*; a local administrative account that will use the tools in the Toolkit.
2. Insert the CD into the CD-ROM drive on your computer. If the CD does not start automatically, browse to the CD, and then double-click **AutoRun.hta**.
3. If required, click the [Windows Genuine Advantage](#) validation link to perform the validation process.
4. Click **Install the Toolkit**.
5. Review the License Agreement page, and, if the terms are agreeable to you, click **I Accept the terms in the License Agreement**, and then click **Next**.
6. On the Customer Information page, you can click **Register Now** to complete the optional registration process
7. On the Installation Folder page, click **Next**.
8. On the Ready to Install page, click **Install**.
9. On the Installation Complete page, click **Finish** to exit. If you leave the **View Getting Started** check box selected, the Getting Started tool should open.



Note

Some script-blocking software does not allow you to permanently approve scripts. Script blocking must be turned off if you cannot permanently approve Toolkit scripts.

Work with Script Blocking Software

Many security, antispyware, and system protection tools block access to scripts to help safeguard your computer. If you recognize a script as belonging to the Shared Computer Toolkit, you must authorize it to run or unexpected behavior will result.

To ensure the proper operation of the Toolkit and critical updates with script blocking software in place—allow all scripts by running **RunAllScripts.bat** from the Scripts folder of the installation and approve each script as the Toolkit administrator.

To enable the execution of Toolkit-required scripts for users, review the "Set Up Local User Profiles" section in Chapter 3, "Profile Management."

Getting Started

After the installation process finishes, the Getting Started tool will open (unless you cleared the **Show Getting Started** check box during installation). Getting Started also opens by default each time you log on to the shared computer with the Toolkit administrator account, which is the account you used to install the Toolkit. Getting Started provides an overview of and shortcuts to the tools and resources available in the Toolkit. Getting Started presents the following steps and advice to help you start using the Toolkit quickly:

- **Step 1. Prepare the Disk for Windows Disk Protection.** In this section, the Getting Started tool indicates whether the shared computer's disk is properly configured for Windows Disk Protection. If it is not, the tool provides advice for configuring

the disk. The tool also shows whether Windows Disk Protection is currently on or off. You can learn more about preparing a disk for Windows Disk Protection in Chapter 2, “Prepare the Disk for Windows Disk Protection.”

- **Step 2. Select Computer Security Settings.** This section provides valuable options for improving the security of the shared computer. Unlike the restrictions available in the User Restrictions tool, which are applied on a per-user basis, the options in this section apply to anyone who uses the shared computer. Options you can select in this section include:
 - **Prevent account names from being saved in the CTRL+ALT+DEL logon dialog.** By default, Windows displays the user name that was last used to log on to Windows in the traditional logon dialog box shown when you press CTRL+ALT+DEL at the Windows Welcome screen.
 - **Force Windows to store passwords in a secure format (not using LMHash).** This setting promotes secure password storage by disabling the LanMan hash form of each password. LanMan hash (or LMHash) is an easily defeated encryption mechanism used for backward compatibility with older operating systems.
 - **Prevent Windows from caching Passport or domain credentials within user profiles.** When this check box is selected, users must enter their Passport and domain credentials each time they are required. Windows does not save them between user sessions.
 - **Prevent users from creating files and folders in C:\.** This setting changes the access control list (ACL) in the root of C: to prevent users from creating files and folders within it. The setting does not affect the ACLs for other folders.
 - **Prevent logon to locked (or roaming) user profiles that cannot be found.** Usually, Windows creates a new (and potentially unrestricted) user profile when a person tries to log on with a profile that Windows cannot locate. This option prevents that from happening.
 - **Remove cached copies of locked (or roaming) user profiles to improve privacy and save disk space.** When this option is selected, Windows does not save the profiles for locked (or roaming) user profiles. This prevents other people from being able to browse through the profiles of people who have previously logged on.
 - **Remove the Shut Down and Turn Off Computer logon options.** This option removes the ability to turn off the computer from the Start menu and the Windows Welcome screen.
 - **Prevent Microsoft Office documents from opening with Internet Explorer.** This option ensures that Office applications host their own documents so the optional Microsoft Office software restriction works correctly.
 - **Use the Welcome screen to simplify the log on process for users.** This option turns on the Windows Welcome screen, which displays a list of available user accounts on the computer when Windows starts up.
 - **Remove <Toolkit administrator> from the Welcome screen.** This option prevents the Toolkit administrator account (the account used to install and administer the Toolkit) from being displayed on the Welcome screen. You can press CTRL+ALT+DEL twice to access the traditional logon dialog box, in which you can type the user name and password directly to log on with any user account not shown on the Welcome screen.



Important

Press CTRL+ALT+DEL twice to access the traditional logon dialog box. This allows you to log on to accounts not listed on the Welcome screen.

- **Step 3. Create a Public Account for Shared Access.** This section provides guidance for creating a local limited user account to be used for shared access to the computer. On many shared computers, there is just one user account that is shared by everyone who uses the computer. This section provides a shortcut to the User Accounts tool with which you create the account.
- **Step 4. Configure the Public User Profile.** This section provides guidance for logging on with the new Public account to configure Windows settings, printers, and programs for the account. After you configure the Public user profile, you will need to log off and then log back on as the Toolkit administrator to continue with the Getting Started tool.
- **Step 5. Restrict and Lock the Public User Profile.** This section provides a shortcut to the User Restrictions tool and guidance for using the tool to lock and restrict the Public user profile.
- **Step 6. Test the Public User Profile.** This section provides guidance for logging on to the Public user profile so that you can test the effectiveness of your configuration and restrictions for the account. After testing the Public user profile, you will need to log off and then log back on as the Toolkit administrator to continue with the Getting Started tool.
- **Step 7. Turn on Windows Disk Protection.** This section provides a shortcut to the Windows Disk Protection tool, along with guidance for turning on the tool and configuring it to download and install critical updates.
- **Step 8. You're Done! Learn More About the Toolkit.** This section provides links to the Shared Computer Toolkit Handbook and Shared Computer Toolkit Help.

Uninstall the Toolkit

You can uninstall the Toolkit at any time by using the Add or Remove Programs item in Control Panel. However, certain features of the Toolkit will no longer be available after the Toolkit is uninstalled, such as all aspects of Windows Disk Protection.

If Windows Disk Protection is on, the uninstall process will save changes to disk and restart the computer. This is expected behavior.

Before you uninstall the Toolkit, turn off the following specific features within all user profiles that use them:

- **Session Timers.** You must turn off timers for mandatory logoff and idle logoff (make sure that each entry is blank) in the General Settings section of the User Restrictions tool.
- **Restart at Logoff.** Clear the check box for this setting in the General Settings section of the User Restrictions tool.
- **AutoRestart.** Set this command-line tool to disabled, if you used it to automatically restart a specific program.

The following features will still be available after you uninstall the Toolkit:

- **Recommended Restrictions for Shared Accounts.** Any restrictions selected in the Recommended Restrictions for Shared Accounts section of the User Restrictions tool remain in effect.
- **Optional Restrictions.** Any restrictions selected in the Optional Restrictions section of the User Restrictions tool remain in effect.

- **Locked Profiles.** Profiles that have been locked with the User Restrictions tool will remain locked.
- **AutoLogon Settings.** Any account configured to log on automatically with the AutoLogon command-line tool will remain in effect.
- **Getting Started.** Computer security options selected in the Getting Started tool will remain in effect.
- **Welcome.** Settings specified with the Welcome command-line tool will remain in effect.

To uninstall the Toolkit, returning most settings to their original configuration

1. Use Step 2 of the Getting Started tool to remove any security settings that were applied after installation.
2. Use the User Restrictions tool to unlock and remove restrictions from all user profiles.
3. Use the Profile Manager tool to delete any user profiles you do not plan to retain. This will remove all documents and folders stored for the affected user profile.
4. Delete any user accounts you do not plan to use.
5. If you have used Shared Computer Toolkit command-line tools to make any configuration changes to your system, use those tools to undo any changes you want to remove.
6. Click **Start**, point to **All Programs**, point to **Microsoft Shared Computer Toolkit**, and then click **Uninstall the Shared Computer Toolkit**.

Uninstall will remove Windows Disk Protection and the Shared Computer Toolkit. You can continue to use your system with any remaining Windows user accounts and profiles.

Preserve User Documents

If you want to preserve user documents when you delete a user profile or delete profile folders (as described in the previous section), you can either copy the documents to a safe location or use the Files and Settings Transfer Wizard to store the documents until the new profile folder is established.

To open the Files and Settings Transfer Wizard, click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Files and Settings Transfer Wizard**.



Chapter 2: Prepare the Disk for Windows Disk Protection



Note

If the terms in this chapter are difficult to understand, you might want to review the "Disks and Partitions" section in Appendix A, "Technical Primer."

The Windows Disk Protection tool protects the Microsoft® Windows® XP operating system and program files from being permanently changed on the *Windows partition*—typically the C: drive. When Windows Disk Protection is on, users can work as usual and Windows behaves as expected. However, all disk changes made aren't actually being made to the Windows partition—they are stored temporarily in another location.

When the computer restarts, Windows Disk Protection returns the Windows partition to its original condition, clearing the changes made since the previous restart. This is a powerful security feature for shared computers.

Windows Disk Protection requires special preparation of the hard disk on the computer, which is explained through the following topics:

- Windows Disk Protection requirements
 - Resize an existing partition
- Or
- Size the disk during Windows XP Setup



Note

An alternative to increasing the size of the protection partition for burning CDs and DVDs is to configure your disk-burning software to place its temporary files off the Windows partition.

Windows Disk Protection Requirements

Windows Disk Protection requires a minimum of 1 GB of unallocated disk space. This unallocated disk space will become the *protection partition*—for storing disk changes temporarily when Windows Disk Protection is turned on. Some computer uses—such as burning CDs and DVDs—require large amounts of disk space (double the size of the project being written to disk). Keep this in mind and ensure that sufficient unallocated disk space exists when you configure computers that will be used for this purpose.

To turn on Windows Disk Protection, you must fulfill the following requirements:

- Ensure that at least 1 GB or approximately 10 percent of the *Windows partition* (whichever is greater) is available as unallocated disk space.
- The unallocated disk space must *follow* a primary partition; it cannot be at the beginning of the disk.
- The disk that contains unallocated disk space may have no more than three primary partitions.
- The Windows partition must be a basic disk. Dynamic disks are not supported by Windows Disk Protection.

You can use the Disk Management utility to view the current partitions on the hard disk.



Note

The protection partition can also be created in free space in an extended partition, or you can use unallocated disk space on a second physical disk. For more information about each of these techniques, see the "Manage the Protection Partition" at the end of this chapter.

To use the Disk Management utility in Windows XP to view current partitions

1. Log on as the Toolkit administrator.
2. If Getting Started does not open automatically, click **Start**, point to **All Programs**, point to **Microsoft Shared Computer Toolkit**, and then click **Getting Started**.

- In Step 1 of the Getting Started tool, click the **Open Disk Management** link at the bottom of the topic. A shortcut to Disk Management is also included in the **Quick access** section near the top of the Getting Started window.

Alternatively, you can right-click **My Computer**, click **Manage**, and then click **Disk Management**.

The following figure shows the Disk Management utility on a computer with a single 40-GB hard disk. The hard disk has a 36-GB Windows partition (the C: drive) and 4 GB of unallocated disk space for Windows Disk Protection.

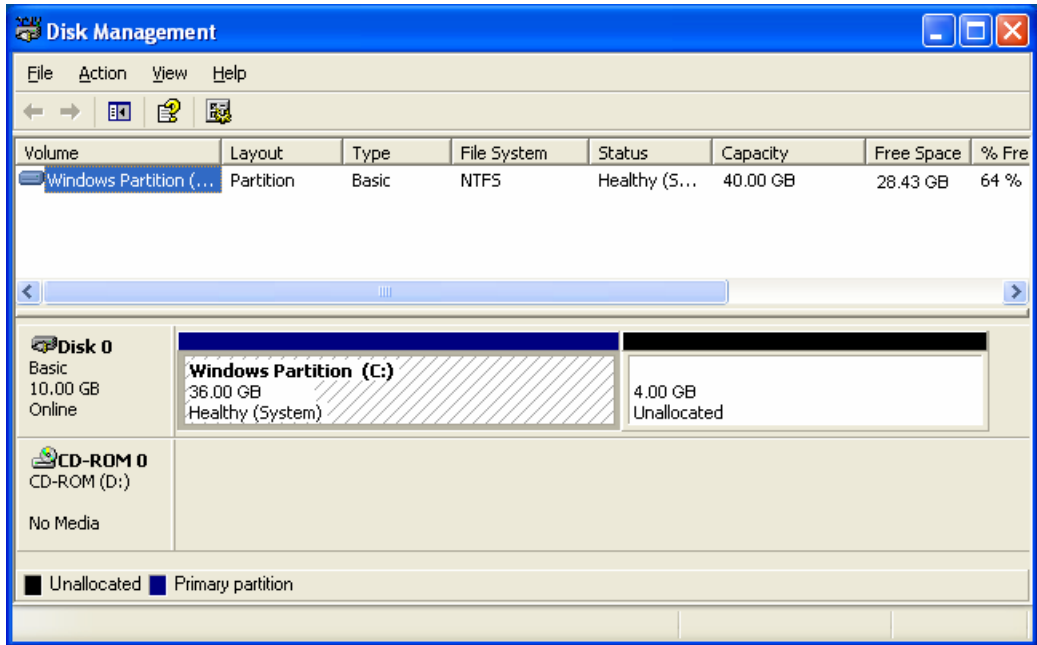


Figure 2.1 Unallocated disk space should be 1 GB or approximately 10 percent of the size of the Windows partition, whichever is greater

To calculate required size of unallocated disk space

If you need to determine the required size of the unallocated space, you can use one of the following procedures:

- Windows partition uses the entire disk.** Divide the disk size in GB by 10. If the result is more than 1 GB, that is the required size of the unallocated space.
- Windows partition uses part of disk.** Divide the size of the Windows partition by 10. If the result is more than 1 GB, that is the required size of the unallocated space.

If the tool you use to resize partitions reports space in MB, multiply the calculated figures by 1024 to convert gigabytes to megabytes.

The following table provides several hard disk configuration examples:

Hard Disk	Partition for C: Drive	Unallocated disk space (1 GB = 1024 MB)
30 GB	27 GB	3 GB (3,072 MB)
80 GB	72 GB	8 GB (8,192 MB)
120 GB	108 GB	12 GB (12,288 MB)
250 GB	225 GB	25 GB (25,600 MB)

Note
If you leave unallocated space equivalent to the size of the Windows partition, Windows Disk Protection will not be restricted by disk space and will be able to track all changes made to the Windows partition.

Note
Most shared computers do not offer users a way to store persistent data locally, but some environments may want to offer this capability. Alternatives for storing persistent user data when Windows Disk Protection is on are described in Chapter 9, "Advanced Scenarios."

Note
Some tasks, such as creating or copying CDs, use significant amounts of disk space on a temporary basis. If your computer will be used for these tasks, ensure enough unallocated disk space exists before the protection partition is created to contain the full contents of two CDs or DVDs.

**Note**

Microsoft does not provide support for third-party disk partitioning products. Please contact the product vendor regarding any support issues with these products.

**Note**

Start PartitionMagic 8.0 by starting the computer from the program CD—not by starting the program from within Windows. You should also make a full backup before you begin this procedure.

Resize an Existing Partition

Most computers do not come with unallocated disk space—the entire disk is typically fully partitioned, often as a single C: drive. This section provides two options for creating the unallocated disk space necessary for Windows Disk Protection.

If your computer already has Windows XP installed and you do not want to reinstall and reconfigure Windows and other programs, you need a third-party disk utility to resize the Windows partition and leave unallocated disk space for Windows Disk Protection.

This section describes how to use [Symantec Norton PartitionMagic 8.0](#) to create the unallocated disk space required for Windows Disk Protection.

Alternatively, you can use [TeraByte Unlimited BootIt Next Generation](#). Full instructions and downloadable trial software are available on the [TeraByte Unlimited Web site](#).

You can locate other disk partitioning utilities by searching [Windows Marketplace](#).

To resize a partition using PartitionMagic 8.0

1. Insert the PartitionMagic CD into the CD-ROM drive on the computer.
2. If the program starts automatically, click **Exit**.
3. Click **Start**, click **Turn Off Computer**, and then click **Restart**. Ensure the computer starts from the PartitionMagic CD.
4. After PartitionMagic starts, at the command prompt, type **1** for Norton PartitionMagic, and then select the language you want to use.
5. In the main window for the program (shown in the following figure) choose a hard disk by clicking the drop-down menu on the main toolbar. The example in the following figure shows a 40-GB hard disk with a single primary partition.

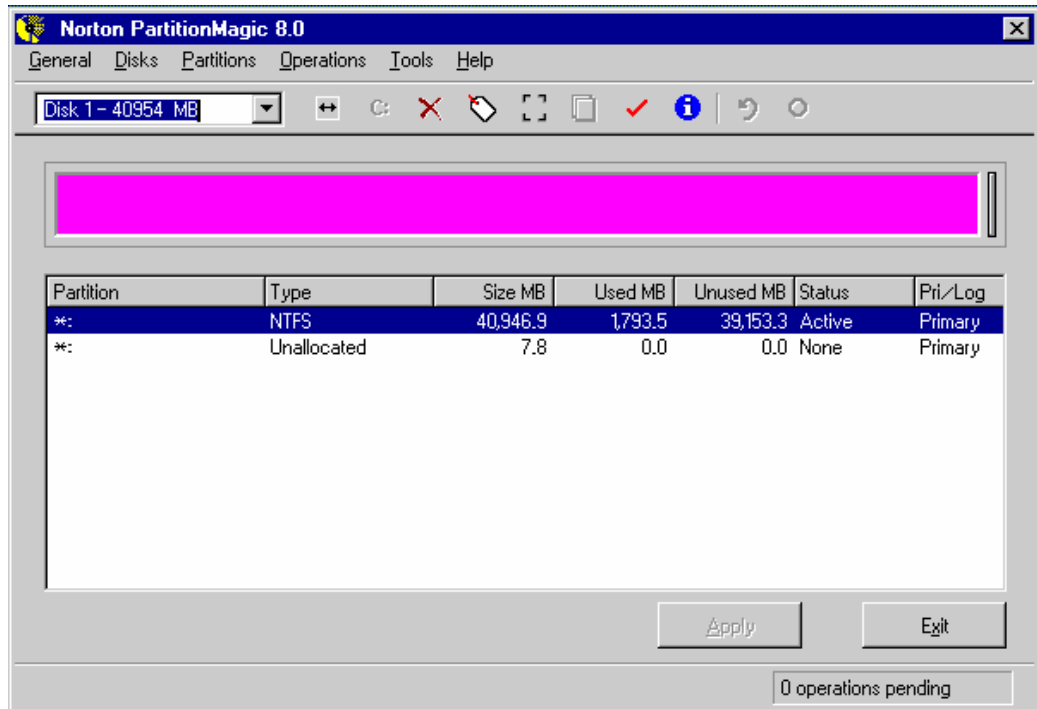


Figure 2.2 The PartitionMagic 8.0 main window

**Note**

Make sure you leave enough room for Windows XP and all necessary programs, typically at least 10 GB for the Windows partition. In this example, the 40 GB partition is resized to 36 GB.

**Note**

In its user interface, PartitionMagic 8.0 refers to the required unallocated disk space as **Free Space After**.

6. Click the partition that you want to resize, click **Operations**, and then click **Resize/Move**.
7. In the **Resize/Move Partition** dialog box (shown in the following figure), in the **Free Space After** box, type the amount of unallocated space to reserve. Use this formula: Number of GB * 1024. The following example shows 4096 (4*1024). The exact number is not important, as long as it is greater than 1024 (1 GB).

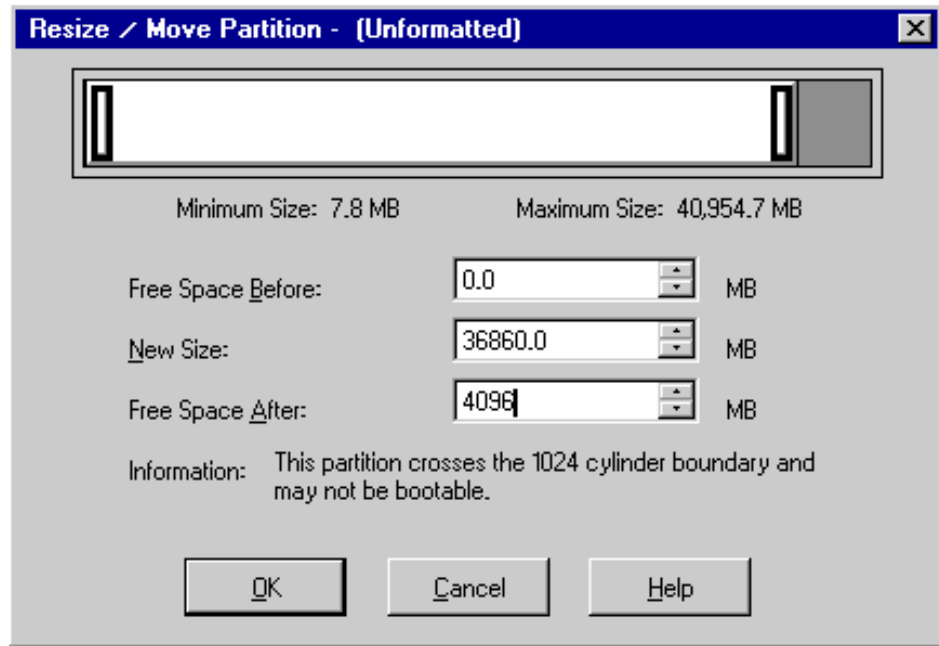


Figure 2.3 Resizing a partition in PartitionMagic 8.0

8. Click **OK** and then click **Apply** to resize the partition. It will take a few minutes to complete.
9. After it finishes, click **Exit**, remove the CD, restart the computer, and log on to Windows as the Toolkit administrator.
10. Within a minute after you log on to Windows, a **System Settings Change** dialog will appear that asks if you want to restart your computer. Click **No**.

The computer is now ready for Windows Disk Protection to be turned on.

After you complete these steps, proceed to Chapter 3, "Profile Management."

**Important**

Deleting partitions will destroy any data on that partition. Use this method only if you do not need to preserve any information on the computer and are willing to reinstall Windows, all necessary programs, and all necessary drivers.

Size the Disk During Windows XP Setup

If you plan to perform a clean installation of Windows XP, the best way to prepare the hard disk for Windows Disk Protection is to create a primary partition of the appropriate size during Windows XP setup. This option is only appropriate if you are willing to overwrite all programs, settings, and files on the computer's hard disk.

After you start Windows XP Setup (which you can do by starting the computer with the Windows XP installation CD in the CD-ROM drive), and after you accept the Microsoft Windows XP Licensing Agreement, Setup displays the page shown in the following figure.

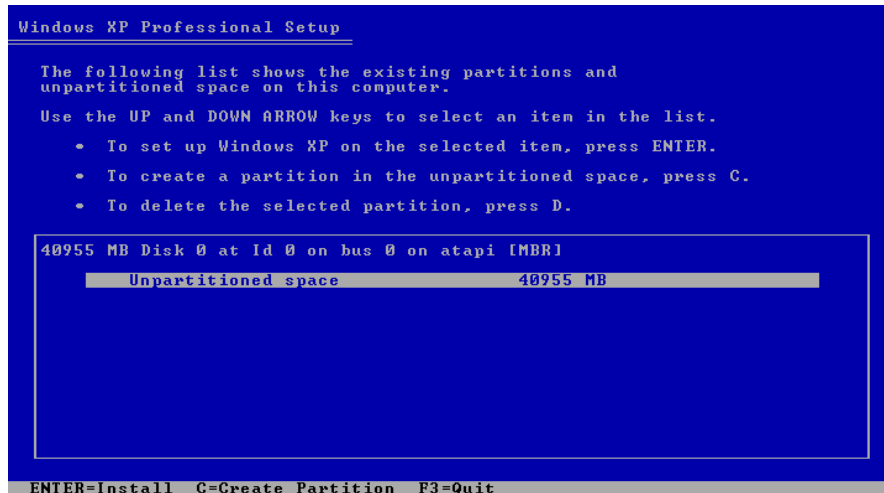


Figure 2.4 Configuring partitions during Windows XP Setup

To size a partition during Windows XP Setup

1. The example in the previous figure shows a single hard disk that has 40 GB (40,955 MB) of unallocated space. To create a partition, press **C** to display the page shown in the following figure. This page shows the minimum and maximum size you can designate for a new partition.
2. Type the appropriate size in MB for the partition you want to create and then press ENTER. For example, to create a 36-GB partition, you would type 36864 (36 * 1024). Leave the remaining space unallocated for use by Windows Disk Protection.
3. Use the arrow keys to select the partition into which to install Windows (if it is not already selected) and then press ENTER.
4. Use your arrow keys to select **Format the partition using the NTFS file system (Quick)** and then press ENTER.
5. Windows XP Setup copies the necessary installation files, and then restarts your computer. Continue with the installation of Windows.



Important

Create the C: partition only during Windows installation. You can create an optional persistent partition using the Disk Management tool after the Windows installation completes. This procedure is covered in Chapter 9, "Advanced Scenarios."

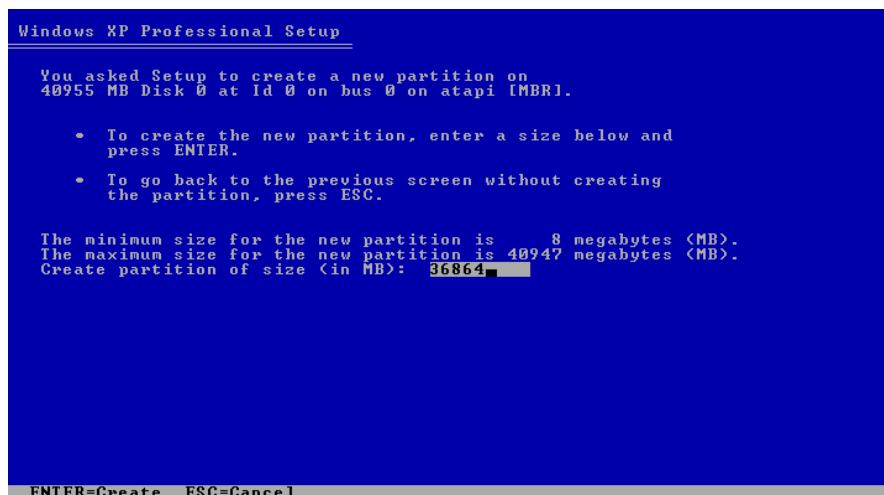


Figure 2.5 Creating a new partition during Windows XP setup



Chapter 3: Profile Management

Now that you have prepared the computer and installed the Microsoft® Shared Computer Toolkit for Windows® XP, it is time to address the needs of your users. To do this, you will create user accounts and then customize each user profile.

In this chapter, you will learn how to:

- Create local limited user accounts
- Set up local user profiles
- Optional activity: Customize the All Users Start menu
- Optional activity: Customize a user's Start menu



user profile

A collection of folders, files, and configuration settings that define the user's environment.

A *user profile* is a collection of folders, files, and configuration settings that define the environment for a user who logs on with a particular user account—each user account has an associated profile. Typically, a user profile is not created until the first time that a user logs on to the computer with a new user account. When this logon happens, Windows automatically creates a new user profile for that user account.

Create Local Limited User Accounts

The first step is to create accounts for the users of the computer. Depending on your environment, you can create:

- **A separate user account for each user.** This solution is useful when you have relatively few users, a single computer, and each user has different needs. When you have many users and computers, creating separate accounts is unwieldy. You should consider using the Active Directory® directory service instead.
- **A single user account to be used by all users.** This is known as a shared account.
- **A few categories of user accounts to be used by all users.** For example, in a library setting, you might create one account for children and a different account for adults.

How you structure accounts depends on your situation, but having fewer accounts typically means less management effort will be required.

If you plan to use a computer imaging or cloning approach in your environment, you could create a full array of different user accounts on your reference computer. Then, after you clone the original computer multiple times, disable the accounts not used on each cloned computer. This will reduce the number of original computer images you need to manage. For more information about cloning, see Chapter 9, “Advanced Scenarios.”



Note

Local user accounts are used on stand-alone or workgroup computers. If the computer is a member of an Active Directory domain, see Chapter 10, “The Shared Computer Toolkit in Domain Environments,” for more information.

**Note**

Windows XP Professional also supports groups to which various permissions and rights can be granted, providing a much more flexible configuration of user accounts. However, users of a shared computer should be given access only to limited user accounts whenever possible.

Windows XP supports two primary types of local user accounts:

- **Computer administrator.** A computer administrator account has the rights to install and uninstall software and device drivers, change Windows configuration settings, create and delete users, and change security settings. You will use an administrative account to manage Windows and the Toolkit options.
- **Limited.** A limited account does not, by default, have the rights to perform any of the actions listed for the administrator type account. By default, a limited user account can run programs, access the Internet and local network, change desktop settings, create folders and files, and perform other daily activities.

When you create accounts, you should create limited user accounts. You will then use the User Restrictions tool in the Toolkit to further restrict the activities of those users.

To create a new limited user account on a workgroup computer

1. Log on as the Toolkit administrator.
2. If Getting Started does not open automatically, click **Start**, point to **All Programs**, point to **Microsoft Shared Computer Toolkit**, and then click **Getting Started**.
3. In Step 3 of Getting Started, click the **Open User Accounts** link at the bottom of the topic. A shortcut to User Accounts is also included in the **Quick access** section near the top of the Getting Started window.
4. In the **User Accounts** window, click **Create a new account**.
5. On the **Name the new account** page, type the name of the new user account, and then click **Next**.
6. On the **Pick an account type** page, click **Limited**, and then click **Create Account**.

Giving users access to administrative accounts presents a number of security vulnerabilities. Sometimes, however, your users may want to run programs that require an administrative account to run properly. Many games fall into this category. In these situations, you might need to create administrator type accounts for certain users and then restrict those accounts to limit their access to potentially damaging configuration tools. You can learn more about this option in the "Restrict a Shared Administrative Account" section in Chapter 9, "Advanced Scenarios."

**Note**

You can use the Profile Manager tool to create user profiles, but first-time profile setup is still required.

For more information about user profiles, see Appendix A, "Technical Primer."

Set Up Local User Profiles

After you create local user accounts, the next step is to create and configure the user profiles for those accounts. To complete this process, you log on with the user accounts you have created, run programs for the first time, and configure Windows settings. Running programs for the first time on behalf of the users allows you to accept license agreements and configure settings that users would otherwise have to reconfigure each time they use the program.

To set up a local user profile

1. Log on using one of the local user accounts you created. When you log on with an account for the first time, Windows automatically creates a new user profile.
2. Perform first time setup activities for programs such as Microsoft Office and Windows Media Player. Configure programs such as:
 - ◆ Microsoft Office
 - ◆ Windows Media Player

**Note**

The idle logoff timer in the User Restrictions tool uses screen saver settings. If you plan to set an idle logoff timer later for this user, don't configure their screen saver now.

- ◆ MSN Messenger
- ◆ MSN Games Loader
- ◆ Macromedia Flash
- ◆ Adobe Reader
- ◆ Other programs or utilities needed on the shared computer.

3. Configure any other important settings:

- ◆ Install and configure printers that the user will need.
- ◆ Install software and device driver settings the user may require.
- ◆ Configure desktop settings such as wallpaper and screen saver.
- ◆ Delete Windows Explorer shortcuts from the Start menu. Use My Computer shortcuts instead.

4. If the computer uses script-blocking software, execute all Toolkit scripts (as listed in the following table) that might be run within a restricted user profile. When the software prompts you to allow or block the script, allow the script permanently to prevent future prompts to the user.

Script file	Path
Accessibility.hta	%ProgramFiles%\Microsoft Shared Computer Toolkit\
Accessibility.wsf	%ProgramFiles%\Microsoft Shared Computer Toolkit\scripts
AutoRestart.vbs	%ProgramFiles%\Microsoft Shared Computer Toolkit\bin
SCTLogoff.vbs	%ProgramFiles%\Microsoft Shared Computer Toolkit\bin
Toast.hta	%ProgramFiles%\Microsoft Shared Computer Toolkit\bin
Toast.vbs	%ProgramFiles%\Microsoft Shared Computer Toolkit\bin

**Note**

Some script-blocking software does not allow you to permanently approve scripts. Script blocking must be turned off if you cannot permanently approve Toolkit scripts.

In addition to script-blocking warnings, there are other types of security software warnings or approvals that your environment might require. If such warnings occur, perform the following changes before you lock the profile:

5. **Internet Explorer Home Page changed warning.** Set the home page for Internet Explorer from within the profile (not from the User Restrictions tool) before you lock the profile.
6. **Registry Run keys added warning.** User Restrictions (specifically the mandatory logoff timer) and the AutoRestart tool add **Run** keys to the user's registry. Script-blocking software may warn the user about these applications. Make these changes and authorize them by logging on as the user and answering the script-blocking prompts before you lock the profile.
7. Repeat steps 1-6 for each local user account.

**Important**

Changes made to the All Users Start menu affect all users of the computer. Most programs install Start menu shortcuts in the All Users profile.

Optional Activity: Customize the All Users Start Menu

By default, the User Restrictions tool enables the Windows Classic Start menu—a menu similar to that featured in previous versions of Windows. Using the Classic Start menu makes it easier to customize what programs appear on the Start menu for a user profile.

You do not need to turn on the Classic Start menu manually, but you can arrange icons within the Start menu now so that they will appear in the right place after you run the User Restrictions tool later.

Windows XP builds the Start menu for a user based on program shortcuts that are stored by default in two locations:

- **The \Documents and Settings\All Users\Start Menu folder.** This folder contains program shortcuts that are included on the Start menu for all user accounts.
- **The \Documents and Settings\user name\Start Menu folder.** This folder contains program shortcuts that are specific to a particular user profile.

Windows analyzes the contents of these two folders when it generates the program shortcuts displayed on the Start menu. To customize (and secure) the Start menus for users, you should first make sure that the All Users\Start Menu folder contains only those program shortcuts that you want all users to have access to. Later in this section, you'll customize the Start menu for an individual user profile.

Some shared computer operators like to make sure that the All Users\Start Menu folder contains no programs and that the Start Menu folder for each profile includes the appropriate shortcuts instead. Note, however, that removing a shortcut from the Start menu does not necessarily make the program unavailable. For example, users could still double-click a .doc file to open Microsoft Word, even if a shortcut for Word is not available on the Start menu.

To customize the programs that appear on the All Users Start menu

1. Log on using an administrative account.
2. Right-click the **Start** button and then click **Explore All Users**. Shortcuts located in the Start Menu folder appear directly on the Start menu. Shortcuts in the Programs folder appear on the Programs submenu of the Start menu.
3. Use Windows Explorer to drag shortcuts to the Start Menu folder to make them appear directly on the Start Menu for all users.
4. Drag other shortcuts to and from the All Users folders to suit your needs.

**Important**

When you customize the All Users Start menu, remove access to utilities that users should not access, such as antivirus, antispyware, Microsoft Update, and disk utilities.

Remove the following icons from the All Users Start menu so they are not available to the shared accounts you create:

- Set Program Access and Defaults
- Windows Catalog
- Windows Update and Microsoft Update
- Command Prompt
- System Tools folder

**Note**

If you plan to restrict access to the C: drive, replace any Windows Explorer shortcuts with My Computer shortcuts in the user's Start Menu to avoid error messages. By default, Windows Explorer attempts to display profile folders, which are located on the C: drive.

Optional Activity: Customize a User's Start Menu

Just as you can configure shortcuts that appear on the All Users Start menu, you can also configure the shortcuts that appear on the Start menu for an individual user profile.

To customize the programs that appear on an individual profile's Start menu

1. Log on using an administrative account.
2. Right-click the **Start** button and then click **Explore**.
3. Inside the Documents and Settings folder, you will see a subfolder for each user profile on the shared computer. If you do not see folders for user accounts, you probably have not yet created the user profiles. To do so, log on as each user on the computer, as described in the "Set Up Local User Profiles" procedure covered earlier in this chapter.
4. Use Windows Explorer to copy shortcuts to the Start Menu folder for each user to make them appear directly on the Start menu for that user.
5. Drag other shortcuts to and from each user's folder to suit your needs.



Chapter 4: User Restrictions



Note

You must ensure the user account being restricted is logged off before applying restrictions. Fast user switching cannot be used to shuttle between the Toolkit administrator's account and the restricted account.

The User Restrictions tool allows you to restrict user actions. By default, users who have limited accounts cannot install software or hardware, but can run programs they download or bring with them on a USB drive—potentially causing problems on the computer. With the User Restrictions tool, you can define restrictions for Microsoft® Internet Explorer, Microsoft Office, the Microsoft Windows® XP operating system, the Start menu, and specify what software is permitted to run.

This chapter covers the following topics:

- Restrict a local user profile
- General settings
- Locking a profile
- Recommended restrictions for shared accounts
- Optional restrictions

Restrict a Local User Profile

You can use the User Restrictions tool to restrict and lock user profiles to prevent tampering with the computer. This section describes a typical user restriction scenario.



Note

The **Select a Profile to Restrict** dialog box shows all user accounts configured on the shared computer, including those that are disabled. It will only allow you to select accounts for which user profiles exist.



Important

All **Recommended Restrictions for Shared Accounts** must be used if you want to prevent user tampering with the computer. Individual restrictions will be insufficient.

To restrict a local user profile

1. Log on as the Toolkit administrator.
2. Click **Start**, point to **All Programs**, point to **Microsoft Shared Computer Toolkit**, and then click **User Restrictions**. Alternatively, you can click the **Open User Restrictions** link in Step 5 of Getting Started. A shortcut to User Restrictions is also included in the **Quick access** section near the top of the Getting Started window.
3. Click **Select a Profile**.
4. In the **Select a Profile to Restrict** dialog box, click the user profile that you want to restrict.
5. Select the **Lock this profile** check box to prevent users from being able to change settings while logged on with the user account. You can read more about locking profiles in the “Locking a Profile” section in this chapter.
6. Select the **Recommended Restrictions for Shared Accounts** check box. This enables the most important restrictions. You can read a complete description of the settings in the “Recommended Restrictions for Shared Accounts” section of this chapter.
7. In the **General Settings** section, type in the default home page, a proxy server (if necessary), and any applicable proxy exceptions.
8. In the **Session Timers** section, set limits on the number of minutes the user can use the computer or be idle before a forced logoff. You can also choose to leave these options blank.

**Note**

If you plan to restrict access to the C: drive, replace any Windows Explorer shortcuts with My Computer shortcuts in the user's Start Menu to avoid error messages. By default, Windows Explorer attempts to display profile folders, which are located on the C: drive.

**Note**

Some computer environments allow customers to use administrative accounts. This is not a recommended practice, but it can be improved upon. For more information about this topic, see the "Restrict a Shared Administrative Account" section in Chapter 9, "Advanced Scenarios."

9. Click **Select Drives to Restrict** and then restrict all of the drive letters to which the user should not have access. Microsoft highly recommends restricting access to the Windows partition where Windows and programs are installed (typically the C: drive).
10. Click **Apply** to apply the selected restrictions to the user profile and continue working with the User Restrictions tool or click **OK** to apply the selected restrictions to the user profile and close the User Restrictions tool.

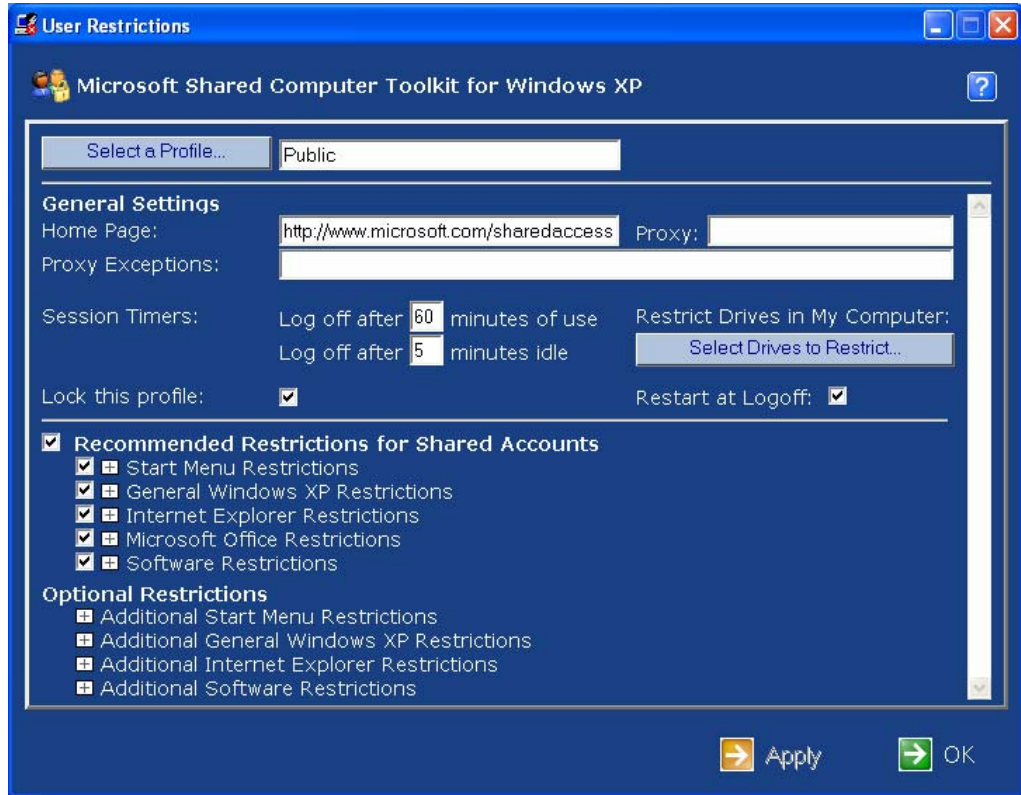


Figure 4.1 The main screen of the User Restrictions tool

General Settings

To get started, click **Select a Profile** and then, in the **Select a Profile to Restrict** dialog box, click the user profile that you want to restrict.

In the **General Settings** section of the User Restrictions tool, you can define the following settings:

- **Home Page.** This setting configures Internet Explorer to use a particular home page.
- **Proxy.** You can specify an address for a proxy server—a server that provides Internet access (and often content-filtering services) to the computer.
- **Proxy Exceptions.** You can specify sites or domains that bypass the configured proxy server. You can use this setting to allow certain sites to be visited even when restrictions do not allow general Internet access. This topic is covered in more detail in the "Use Simple Site Filtering to Control Internet Access" section of Chapter 9, "Advanced Scenarios."

**Important**

Locked user profile folders are renamed from \Documents and Settings\user name to \Documents and Settings\user name.Orig. Use this new folder name to locate Start menu icons after you lock the user profile.

- **Session Timers.** You can configure two time restrictions to apply to users:
 - **Log off after __ minutes of use.** This setting specifies how long users can use the computer before they are logged off automatically, after a pop-up warning.
 - **Log off after __ minutes idle.** This setting specifies how long users can be idle or inactive before they are logged off automatically, after a 15 second warning.
- **Restrict Drives in My Computer.** When you click the **Select Drives to Restrict** button, a dialog opens in which you can specify one or more drives to which this user is prevented from accessing.
- **Lock this profile.** This setting prevents users from making permanent changes to the user profile when they are logged on.
- **Restart at Logoff.** This setting forces Windows to restart when a user logs off of the selected profile. This setting is for use with Windows Disk Protection.

Locking a Profile

The **Lock this profile** setting prevents people from being able to make permanent changes to the user profile when they are logged on. This setting is useful for user profiles that are shared by multiple people. If you select this check box, it will not take effect until you click **OK** or **Apply**.

When a profile is locked, files that Windows generally stores on the user's behalf (typically in the Documents and Settings*user name* folder) are not available when the next user logs on. Locked profiles increase the privacy of users and make keeping a clean, standardized desktop much easier for operators of shared computers.

The following are items that are not kept between logons when a profile is locked:

- Internet history and cookies
- Favorites
- Files stored on the desktop
- Desktop wallpaper
- Changes to program settings
- Accessibility changes
- Start menu changes



Important

Clearing any recommended restrictions may have adverse, unintended effects and should only be done with extensive testing to ensure your environment does not become significantly less secure.

Recommended Restrictions for Shared Accounts

Because many of these restrictions work together to provide a more secure environment for shared accounts, it is better to enable all the recommended restrictions at once. For example, Windows XP Home Edition allows users to change passwords if they have access to Control Panel. This means you must use both the **Prevent password changes** restriction and the **Remove Control Panel icon** restrictions to effectively restrict password changes. Similarly, Software Restrictions provide an important security measure that prevents users from running unauthorized programs that can be used to bypass other restrictions.

Start Menu Restrictions

In the User Restrictions tool, click the **Start Menu Restrictions** heading to expand the entire list of restrictions that you can configure for the Start menu. The following list describes the Start Menu Restrictions:

- **Prevent right-click in the Start menu.** Prevents the user from accessing shortcut menus by right-clicking on items in the Start menu.
- **Force the Classic Start Menu (better for shared accounts).** The Classic Start Menu makes it easier for you to configure the programs available to a user on the Start menu.
- **Remove Control Panel, Printer, and Network Settings from Classic Start Menu.** Removes these icons from the Start menu to hide configuration tools from restricted users.
- **Remove My Documents icon.** Prevents users from accessing the My Documents folder through the icon on the Start menu to promote privacy between multiple users.
- **Remove My Recent Documents icon.** Prevents users from accessing recently opened programs through the icon on the Start menu. This helps to ensure that users cannot access programs to which they are denied access and protects the privacy of previous users.
- **Remove My Pictures icon.** Prevents users from accessing the My Pictures folder through the icon on the Start menu.
- **Remove My Music icon.** Prevents users from accessing the My Music folder through the icon on the Start menu.
- **Remove Favorites icon.** Prevents users from accessing the Favorites folder through the icon on the Start menu. This helps to prevent unwanted access to the Internet.
- **Remove My Network Places icon.** Prevents users from accessing My Network Places through the icon on the Start menu, helping to prevent viewing shortcuts to other computers, printers, and network resources that My Network Places displays.
- **Remove Control Panel icon.** Prevents users from accessing the tools in Control Panel through the icon on the Start menu.
- **Remove Set Program Access and Defaults icon.** Removes the Set Program Access and Defaults icon.
- **Remove Connect To icon.** Prevents users from connecting to network resources through the icon on the Start menu.
- **Remove Printers and Faxes icon.** Prevents users from accessing the Printers and Faxes window through the icon on the Start menu.
- **Remove Search icon.** Prevents users from using the Search tool through the icon on the Start menu to locate folders, files, and network resources to which they should not have access.
- **Remove Run icon.** Prevents users from using the Run dialog box to issue commands or start programs.
- **Remove Frequently Used Programs list.** Prevents the Start menu from displaying frequently-used programs.



Important

Many of the Start Menu Restrictions remove the icon for a folder or program from the Start menu, but do not otherwise prevent access to the folder or program. For this reason, it is important that you use all recommended restrictions in the User Restrictions tool to provide the best possible combination of restrictions.

- **Remove Shut Down button.** Prevents users from turning off or restarting the computer through the icon on the Start menu.

General Windows XP Restrictions

The following list describes the General Windows XP Restrictions:

- **Prevent right-click in Windows Explorer.** Disables the shortcut menu that appears when a user right-clicks an object in the Windows environment.
- **Prevent AutoPlay on CD, DVD, and USB drives.** Prevents Windows from automatically displaying options (or taking particular action) when a user inserts removable media. Digital entertainment media such as songs and movies will still auto play with this setting enabled.
- **Remove the Recycle Bin (to help ensure privacy between users).** Helps to ensure that when a user deletes a file, subsequent users cannot access the file.
- **Prevent access to some Windows Explorer features (such as Search).** Disables searching and prevents the user from customizing toolbars and Folder Options. In addition, the My Documents folder is hidden from the left pane.
- **Prevent access to the taskbar.** Prevents access to the Windows taskbar.
- **Prevent access to the command prompt.** Prevents users from accessing folders, files, and programs from the Windows command prompt.
- **Prevent access to the Registry Editor.** Prevents users from accessing the built-in tools that allow them to modify the Registry.
- **Prevent access to Task Manager.** Prevents users from accessing Task Manager, a utility that you can use to stop and start programs and processes, and shut down or restart the computer.
- **Prevent access to Microsoft Management Console utilities.** Prevents users from using the MMC console to load snap-ins that can be used to alter the Windows environment.
- **Prevent users from adding or removing printers.** Prevents users from adding or removing printers to preserve system configuration.
- **Prevent users from locking the computer.** Prevents users from being able to lock the computer to deny access to other users.
- **Prevent password changes (also requires Control Panel to be removed).** Prevents users from changing the password associated with the user account with which they are logged on.

Internet Explorer Restrictions

The following list describes the Internet Explorer Restrictions:

- **Prevent right-click in Internet Explorer.** Prevents users from being able to perform advanced activities on Web content in Internet Explorer by right-clicking items. Some types of content can still be right-clicked, such as Macromedia Flash objects.
- **Prevent access to some Internet Explorer menu choices (such as Internet Options).** Prevents users from accessing certain Internet Explorer menu commands, such as Internet Options, that can be used to modify Internet Explorer configuration.

- **Prevent access to some Internet Explorer toolbar buttons (such as Search).** Prevents users from accessing certain toolbar buttons, such as History, Search, and News. This prevents users from bypassing access controls.

Microsoft Office Restrictions

You can use the User Restrictions tool to set restrictions that apply to Microsoft Office XP, and 2003. Some of these restrictions also apply to Microsoft Office 2000. The following list describes the Microsoft Office Restrictions:

- **Prevent use of Visual Basic for Applications (VBA) in Office XP/2003.** Prevents users from accessing VBA tools in Office XP and Office 2003 programs. (Does not work on Office 2000.)
- **Disable macro shortcut keys.** Prevents users from running macros using shortcut keys in Office programs.
- **Disable Tools | Macro menu items.** Prevents users from accessing macro commands in Office programs.
- **Disable Tools | Add-ins menu items.** Prevents users from enabling and disabling add-in programs in Office programs.
- **Disable the Web toolbar.** Prevents users from enabling the Web toolbar in Office programs and being able to view files and folders on restricted drives.
- **Disable Detect and Repair from Help menu.** Prevents users from running the Detect and Repair command in Office programs.
- **Prevent changes to Clip Organizer contents in Office XP/2003.** Prevents users from importing or deleting clips in the Clip Organizer in Office XP and Office 2003 programs. (Does not work on Office 2000.)



Important

Some games (such as Microsoft Halo® and Activision Call of Duty) and other programs that use copy protection do not work properly when Software Restrictions are selected. If you use these games, you cannot also use Software Restrictions. Keep in mind that turning off Software Restrictions significantly weakens the security of your computer.

Software Restrictions

Software Restrictions provide important security settings that can help you restrict system tools and downloaded software from running. For increased security, ensure that both of these restrictions are selected. If these restrictions are not selected, users may find ways to bypass other restrictions set using the Toolkit. For example, a limited user can download programs that ignore restrictions; enabling them to edit the registry, access restricted drives, and even the use the command prompt even when restricted from doing so.

The following list describes the restrictions within the Software Restrictions list:

- **Only allow software in the Program Files and Windows folders to run.** Prevents users from being able to run programs that are not in the Program Files folder or the Windows path, such as downloaded programs or programs on USB Drives. Shortcuts from any location will work if they point to software in the Program Files and Windows folders. Executables cannot be placed on a restricted Start menu or desktop; only shortcuts to allowed software will work from these locations.
- **Prevent System Tools and some management tools from running.** Blocks system tools such as Disk Defragmenter from running.

Optional Restrictions

The following list describes the restrictions within the Optional Restrictions list:



Note

Preventing All Users menu items from displaying will block any icons placed in All Users, either by the Toolkit or by other Windows programs, from displaying on limited users' Start menus. Ensure icons users will need are copied from the All Users Start menu folder to the Start menu folder for the restricted user.

Additional Start Menu Restrictions

- **Prevent programs from the All Users folder from appearing on the Start menu.** This setting prevents any icons located in the All Users Start menu folder from displaying in the user's Start menu.
- **Remove Help and Support icon.** Prevents users from accessing the Help and Support window through the icon on the Start menu. Many help pages provide shortcut access to system tools and locations.

Additional General Windows XP Restrictions

- **Remove Shared Documents from My Computer.** This setting prevents unauthorized sharing of documents between users and protects user privacy.
- **Remove CD and DVD burning features.** Prevents users from using the built-in features of Windows XP to copy information to a writable CD or DVD.
- **Disable keyboard shortcuts that use the Windows logo key.** Prevents users from using shortcuts to access unauthorized menus or programs (such as Windows logo key + E to start Windows Explorer).

Additional Internet Explorer Restrictions

- **Prevent Internet access from Internet Explorer.** This setting prevents the user from accessing the Internet with any programs that use the Internet Explorer proxy settings. When you enable this restriction, the Proxy setting is automatically configured as *NoInternetAccess*.
- **Prevent printing from Internet Explorer.** This setting prevents users from printing from Internet Explorer.

Additional Software Restrictions

- **Prevent Windows Messenger and MSN Messenger from running.** This setting prevents the user from being able to use Windows Messenger or MSN Messenger. Note that this setting prevents users from running Windows Messenger directly from its icon, but does not prevent users from running Messenger from a Web-based interface like MSN Web Messenger. To prevent access to a Web based service, you will need to add the URL of the service to the blocked URL list in Internet Explorer.
- **Restrict Notepad and WordPad (recommended for Restricted Administrators).** This setting restricts the two major text-editing tools used by administrators to edit batch files and scripts in Windows XP. This setting can be used to help prevent a restricted administrator account from modifying scripts, including those provided with the Shared Computer Toolkit.
- **Prevent Microsoft Office programs from running.** This setting prevents the user from running any Microsoft Office programs. For this setting to work properly, Microsoft Office must be installed in the default (%ProgramFiles%) location, such as C:\Program Files\Microsoft Office.



Chapter 5: A Restricted User Experience

Although the tools in the Microsoft® Shared Computer Toolkit for Windows® XP are primarily used by shared computer operators, the main purpose of the tools is to enhance and simplify the user experience.

This chapter covers the following topics:

- A typical restricted desktop
- How to test restricted user profiles
- Online resources for using public computers
- The Accessibility tool

A Typical Restricted Desktop

If you create, configure, and restrict user profiles, you can provide a controlled, consistent experience for users. The following figure shows the Start menu for a user profile that has been restricted to show only selected program shortcuts.

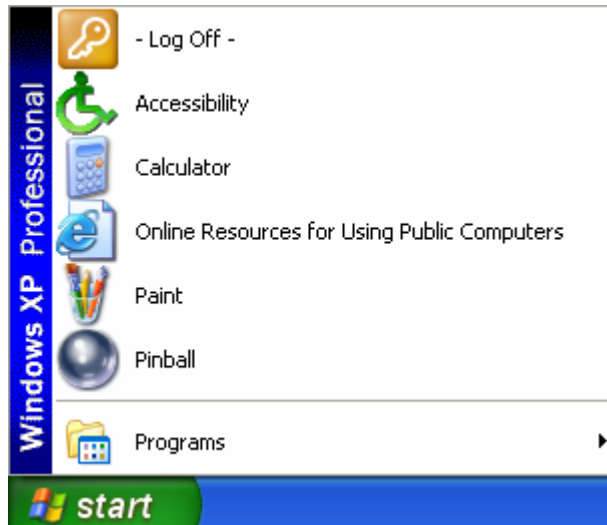


Figure 5.1 A restricted Start menu

How to Test Restricted User Profiles

Before you turn on Windows Disk Protection, you should take the time to test each user account and profile to make sure that the configurations and restrictions work properly. To test a user account, log on to the computer with the user account and verify that:

- Start menus appear correctly.
- Shortcuts on the Start menu and Desktop work correctly.
- No license agreements or other first-time setup screens are offered.

- Programs to which users should not have access do not appear on the Start menu.
- User restrictions that you have configured for the desktop, Start menu, and Internet Explorer work properly.
- Any session timers that you have applied work properly.
- The Accessibility tool is located directly on the Start menu so that it is available to users who may need it.
- The Online Resources for Using Public Computers link is located directly on the Start menu so that it is available to all users.
- Ensure that no script-blocking or similar third party security warnings appear.

The problems that you discover when you test a user account can usually be resolved with one of the following approaches:

- Select additional restrictions in the User Restrictions tool to prevent unintended access to system resources. This can be performed by the Toolkit administrator on a user profile that is restricted and locked.
- Clear restrictions in the User Restrictions tool if some programs cannot run because of the restrictions. This can be performed by the Toolkit administrator on a user profile that is restricted and locked.
- Add or delete program icons from the user's Start menu and the All Users Start menu if the user's Start menu icons are incorrect. This can be performed using Windows Explorer from an administrative account, even if the profile is restricted and locked.
- Change the settings of a user profile while you are logged on as the user. This can only be performed on a user profile that is unrestricted and unlocked.

Some settings can only be configured when you are logged on as the user. The following procedure describes how to modify these settings after a user profile has been restricted and locked.

To change user profile settings that require you to log on as the user

1. Log on as the *Toolkit administrator*, the administrative account with which you installed the Toolkit.
2. Start the User Restrictions tool. Choose the user profile that you want to change.
3. Make a note of the restrictions so that you can re-apply them later.
4. Click the **Select Drives to Restrict** button. In the **Select Drives to Restrict** dialog box, ensure that all drives appear in the **Listed** column and that the **Restricted** column is empty.
5. Clear the **Lock this profile** check box, the **Restart at Logoff** check box, and the **Recommended Restrictions for Shared Accounts** check box.
6. Click **OK** to apply these changes and close the User Restrictions tool.
7. Log off and then log on as the user account. Make the required configuration settings.
8. Log off and then log on again using the Toolkit administrator account.
9. Start the User Restrictions tool to lock the user profile (if it was locked before) and configure the same restrictions that you had before.
10. Log off and then log on again as the user and test the profile again.
11. Repeat steps 1 to 6 as required until you correct the issue.

12. If Windows Disk Protection has been on previously (this should not be the case yet if this is your first time using the tools), open it and select the option to **Save changes with next restart**, click **OK**, then click **Yes** to restart the computer.

After you test each user account to ensure it works correctly with the restrictions configured, you are ready to turn on Windows Disk Protection by following the steps in the next chapter.

Online Resources for Using Public Computers



Note

A shortcut to the Online Resources for Using Public Computers page is installed into the Start menu folder in the All Users profile.

For users who are new to computers or to Windows XP, or new to using computers in public places, the Online Resources for Using Public Computers Web page provides a list of online resources with information about how to use Windows and to increase security and privacy. The page also features resources specifically for teenagers and young children.

To access this page, users can click the **Online Resources for Using Public Computers** shortcut on their Start menu.

The Accessibility Tool

Windows XP provides a number of Accessibility options and utilities for users who have special needs—options that make the desktop easier to see and that make such input devices as the keyboard and mouse easier to use.

The Toolkit provides easy access to certain Accessibility options so that users of a restricted account can still customize their Windows environment. When a user logs on, the user can simply click **Start**, and then click **Accessibility** to access the Accessibility window shown in the following figure. If a profile is not locked, settings made in the Accessibility window are saved to the user's profile so that the user will have the same experience when they next use the computer.

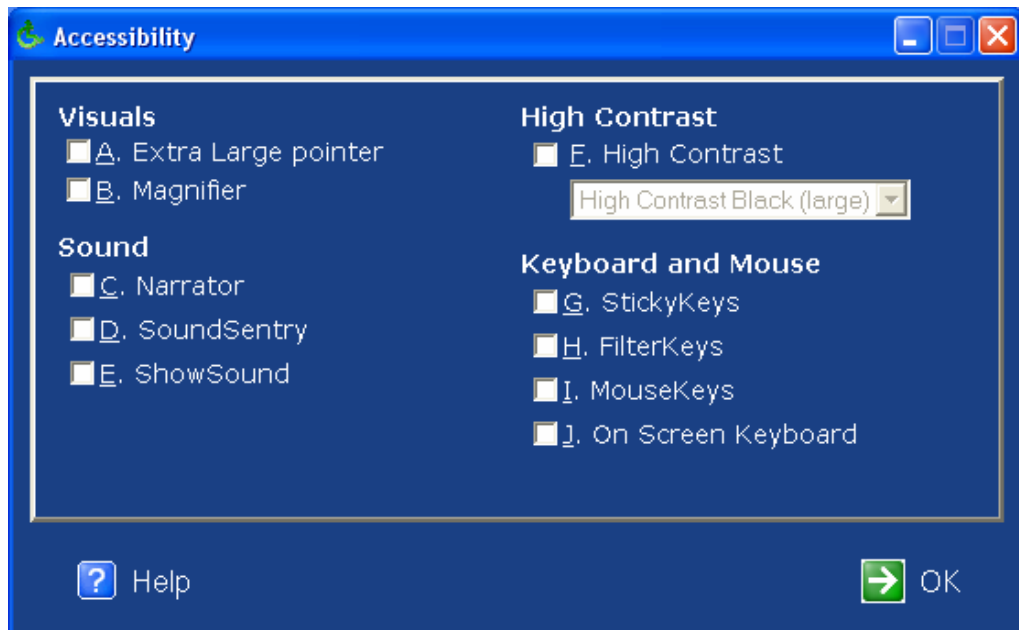


Figure 5.2 *The main screen of the Accessibility tool*

Users can configure the following options in the Accessibility window:

- **Visuals.** The options in this section include the following:
 - **Extra Large Pointer** increases the size of the Windows pointer.
 - **Magnifier** reserves the top of the screen to provide a magnified view of the area surrounding the Windows pointer.
- **Sound.** The options in this section include the following:
 - **Narrator** works with some programs by using a synthesized voice to read aloud text from the screen.
 - **SoundSentry** causes Windows to generate visual warnings when the system makes a sound, which is useful for users who are deaf or hard of hearing. You can have Windows flash the caption bar at the top of a window or dialog box, flash the active window itself, or flash the entire desktop.
 - **ShowSound** causes Windows to display an icon or a text note to indicate the particular sound that Windows makes.
- **High Contrast.** A selection of contrast options make high contrast desktop color schemes available, which improve readability for people who have impaired vision.
- **Keyboard and Mouse.** The options in this section include the following:
 - **StickyKeys** allows a user to use key combinations (such as CTRL+ESC) by pressing one key at a time instead of having to press the keys simultaneously. StickyKeys works for the CTRL, ALT, and DEL keys, in addition to the Windows logo key. When a user presses one of these keys, Windows registers the key as “pressed” until the user completes the key combination.
 - **FilterKeys** causes Windows to ignore repeated keystrokes, which is useful for people who have involuntary hand movements that cause them to press keys in rapid succession or hold a key longer than they intend to.
 - **MouseKeys** allows a user to use the numeric keypad on the keyboard to control pointer movements instead of (or in addition to) using a mouse.
 - **On-Screen Keyboard** opens a software-based keyboard in an on-screen window. Users can press the keys on the keyboard by clicking them with their mouse or other pointing device.

To use the Accessibility tool

1. Click **Start** and then click **Accessibility**.
2. In the **Accessibility** tool, either select a check box or press ALT plus the underlined letter key that corresponds to each option you want.
3. Select as many options as you want to apply and then click **OK**.



Chapter 6: Windows Disk Protection



malware

Malicious software, which includes viruses, worms, and Trojan horses, that is designed to harm a computer operating system.



spyware

Potentially unwanted software that may collect personal information and is inappropriate for shared computers.



Important

Before you turn on Windows Disk Protection, be sure that you have correctly prepared the disk and created, customized, and restricted the required user profiles as discussed in the previous chapters.



Note

For best disk performance, defragment your Windows partition prior to turning on Windows Disk Protection. Do not defragment the disk when Windows Disk Protection is on.

The Windows Disk Protection tool protects the Windows operating system and program files from being permanently changed on a Windows partition. During a session, a user can make changes as necessary within the bounds of any restrictions placed on the user. When the computer restarts, Windows Disk Protection returns the Windows partition to its original condition, discarding any changes made during the user session.

This tool helps protect computers from users who might attempt to damage the operating system, and it also prevents malware and spyware from tampering with the computer.

Each time the computer restarts, Windows Disk Protection returns the partition that holds the Windows and program files (called the *Windows partition*) to its original state. This provides the next user with a standard and reliable experience.

This chapter covers how to:

- Turn on Windows Disk Protection
- Save changes when Windows Disk Protection is on
- Retain changes when Windows Disk Protection is on
- Retain changes indefinitely when Windows Disk Protection is on
- Improve the performance of Windows Disk Protection
- Manage the protection partition

Turn On Windows Disk Protection

The default behavior of Windows Disk Protection is to clear disk changes made to the Windows partition with each computer restart, thereby protecting the disk from unwanted changes. Operators can at any time choose to save changes made to the disk. Operators can also schedule Windows Disk Protection to download, install, and save critical updates to disk automatically while the computer is not in use.

To turn on Windows Disk Protection and schedule critical updates

1. Click **Start**, point to **All Programs**, point to **Microsoft Shared Computer Toolkit**, and then click **Windows Disk Protection**. Restart the computer if requested and then start Windows Disk Protection again.
2. In the **Restart Action** section, click **Keep On**. If this is the first time you have used the Shared Computer Toolkit, Windows Disk Protection creates the protection partition. The computer requires a restart to complete the initialization process.
3. After the restart, return to Windows Disk Protection to complete the configuration.
4. If Windows Disk Protection identifies antivirus software it knows how to update, it displays a dialog box to this effect. If you see this dialog box, click **OK**.
5. If Windows Disk Protection did not detect your antivirus software, click **Set** to specify an antivirus script you have created. You can configure other update scripts as needed to manage updates for third-party programs.
6. In the **Critical Updates** section, configure the day and time at which Windows Disk Protection should download and install critical updates.

7. For Microsoft Updates, Click **Enabled** to enable critical Microsoft updates.
8. Click **OK**.
9. Windows Disk Protection displays a message that states that the computer must be restarted for the changes to take effect. Click **Yes** to restart the computer.



Important

Do not attempt to change any partition after Windows Disk Protection is turned on because it tracks physical disk and partition numbers and they must not change. If you must change partitions, turn off Windows Disk Protection and delete the protection partition before making any partition changes.

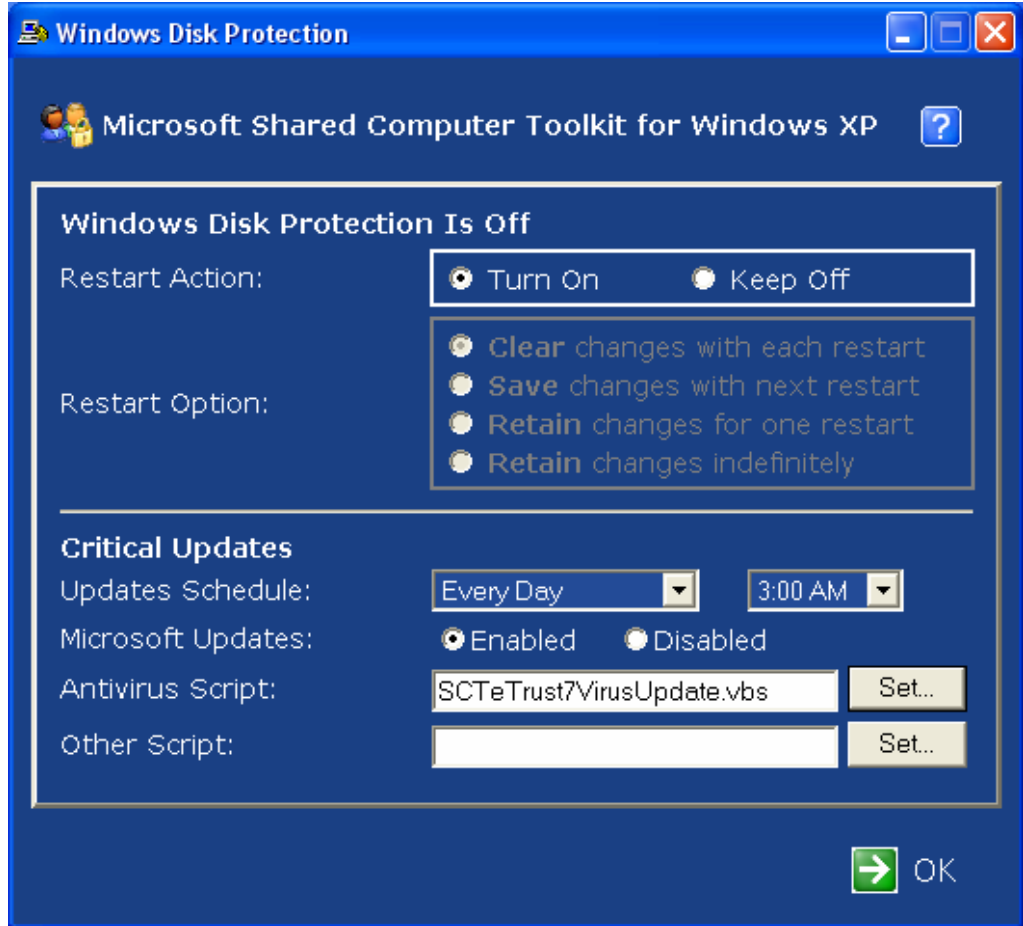


Figure 6.1 The main screen of the Windows Disk Protection tool



Note

Services, such as event logging, that usually write to the Windows partition will not be able to permanently record log entries because new entries will be lost when changes are cleared. To keep event logs, consider moving them to a persistent volume. This process is covered in the “Improve the Performance of Windows Disk Protection” section later in this chapter.

The default setting for Windows Disk Protection is to **Clear changes with each restart**. This option ensures that untrusted users and malware cannot save any disk changes to the Windows partition of the computer. When the computer restarts, all disk changes that were made are removed, and the computer returns to its previous state.

The **Restart Option** will not become available to change until after the computer has been restarted with Windows Disk Protection turned on. This ensures that Windows Disk Protection is started with the default settings.

Hibernation and Windows Disk Protection

If hibernation is enabled on your system when you turn on Windows Disk Protection, you will receive a message that indicates that hibernation does not work with Windows Disk Protection.

When a system hibernates, it writes the contents of the system RAM to a file on the disk. Because modifications to the Windows partition are cleared when Windows Disk Protection is on and set to **Clear changes with each restart**, hibernation will fail.

To disable hibernation, open Control Panel, double-click **Power Options**, click the **Hibernate** tab, and then clear the **Enable hibernation** check box.

Windows Disk Protection Status

When Windows Disk Protection is on and Getting Started is not configured to run automatically, a popup called **Disk Protection Is On** will appear when you log on as the Toolkit administrator. This popup provides a convenient way to open Windows Disk Protection when you have to save changes to disk.



Figure 6.2 The Disk Protection Is On popup

If you want to stop this popup from appearing, delete the **Check Windows Disk Protection** shortcut from the Toolkit administrator's Startup folder.

Critical Updates

When you turn on Windows Disk Protection, it will continue to install Microsoft critical updates using the Automatic Updates schedule you may have configured previously. It will use [Microsoft Update](#), [Windows Update](#), or [Windows Server Update Services](#), depending on which of these is currently used by Windows. (Software Update Services is not supported.) You can enable or disable Microsoft Updates and set the schedule to suit your needs when you turn on Windows Disk Protection.

When Windows Disk Protection downloads and installs critical updates, it will log off the active user, restart the computer to clear disk changes, and temporarily disable local user accounts to prevent unapproved disk changes from being saved at the same time. After downloading and installing the updates, it will set Windows Disk Protection to **Save changes with next restart** and then restart the computer.

In addition to being able to save Microsoft critical updates automatically, Windows Disk Protection allows a script you select to save antivirus updates and updates for other programs.

Alternatively, you can schedule antivirus updates through the graphical interface your antivirus product provides. Schedule the updates to occur at the exact same hour and day(s) as the schedule you select for critical updates in the Windows Disk Protection tool. The Windows Disk Protection critical updates process will wait at least 10 minutes for other updates to be completed concurrently before it restarts the computer to save disk changes.

Windows Disk Protection will offer to perform antivirus updates automatically as part of the critical updates process if it detects an antivirus product it knows how to update. The Toolkit currently detects and includes scripts for updating the following antivirus products:

- [Computer Associates Etrust 7.0](#)
- [McAfee VirusScan 2005](#)
- [McAfee VirusScan Enterprise 8.0](#)



Note

For more information about the Windows Disk Protection critical updates process, see Appendix A, "Technical Primer."

If you have another antivirus product, you might want to prepare a signature update script for it as described in your antivirus software manual. Look for sections that describe the command-line tools that perform signature updates.

Check the Microsoft Windows Shared Access newsgroup to see if anyone else has already created a signature update script for the antivirus software you have.

Other Updates from Microsoft

Windows Disk Protection only automates critical updates from Microsoft—it does not automatically install recommended updates, optional updates, driver updates, or special updates that may have their own license agreements. Review the updates available on [Microsoft Update](#) periodically, download and install the ones you want, and then use the Windows Disk Protection tool to save changes to disk.

Save Changes When Windows Disk Protection Is On



Important

Restart the computer once before you change the Windows Disk Protection restart option to clear all past changes that you might not want to keep.

When Windows Disk Protection is on, you must take special actions to make permanent changes to the disk. Such changes include installing a program, modifying the registry, adding a user account, or configuring system settings for users.

To install a program when Windows Disk Protection is off, log on to the computer as the Toolkit administrator, install the program, and then make sure that the program shortcut appears on the appropriate Start menus. When Windows Disk Protection is on, these disk changes must be saved within the Windows Disk Protection tool.

Sometimes, you need to make a permanent disk change. Although you could accomplish this by turning off Windows Disk Protection long enough to install the program, this action requires that you remember to turn on Windows Disk Protection after you finish installing the program. A faster approach is to use **Save changes with next restart**, as described in the following process.

To make changes when Windows Disk Protection is on

1. Restart the shared computer to ensure recent disk changes are cleared.
2. Log on as the Toolkit administrator.
3. Click **Start**, point to **All Programs**, point to **Microsoft Shared Computer Toolkit**, and then click **Windows Disk Protection**. Alternatively, you can click the **Open Windows Disk Protection** link in Step 7 of Getting Started. A shortcut is also included in the **Quick access** section near the top of the Getting Started window.
4. Click **Save changes with next restart**, and then click **OK**. A restart will not occur at this time.
5. Make the required changes (such as installing software or changing a user profile) to the shared computer and then restart the computer.
6. When the computer restarts, Windows saves your changes to the Windows partition and automatically returns to **Clear changes with each restart**.

**Important**

The **Retain changes for one restart** option remains in effect for only one restart. When the computer completes the restart, the tool will return to the default restart option: **Clear changes with each restart**.

Retain Changes When Windows Disk Protection Is On

In some situations, users might need to install a program or make system changes that you want to test or do not want to keep on the computer permanently—yet a restart is required.

To retain changes temporarily when Windows Disk Protection is on

1. Restart the shared computer to clear past disk changes.
2. Log on as the Toolkit administrator.
3. Click **Start**, point to **All Programs**, point to **Microsoft Shared Computer Toolkit**, and then click **Windows Disk Protection**.
4. Click **Retain changes for one restart** and then click **OK** to exit the tool.
5. Make the changes that you want, and then restart the computer.
6. Allow the user to log on and use the computer.
7. After the user session, you can restart the computer again to undo changes to the Windows partition and automatically return to **Clear changes with each restart**. Alternatively, you can choose to **Save Changes with next restart**.

The above approach can also be used to perform a CHKDSK of the Windows partition, which requires a restart of the computer.

**Important**

If you plan to use the **Retain changes indefinitely** option for extended periods of time, Windows Disk Protection will require more unallocated disk space. The protection partition should match the size of your Windows partition to run this way indefinitely.

Retain Changes Indefinitely When Windows Disk Protection Is On

This option allows operators to accomplish tasks that can involve installing and testing several new programs. After you click **Retain changes indefinitely**, changes will continue to accumulate on the computer until you click **Save changes with next restart** or **Clear changes with each restart**.

The **Retain changes indefinitely** option can be particularly useful if you need to install several new programs. For example, after this option is enabled, you can install a new program, test it for potential compatibility issues with the other programs on the computer, and then move on to installing other programs before clearing or saving all disk changes.

Improve the Performance of Windows Disk Protection

Ways to improve the performance of Windows Disk Protection include defragmenting the disk when Windows Disk Protection is turned off and eliminating unnecessary disk writes by moving the virtual memory paging file and event logs to a persistent partition.

These activities are entirely optional and are intended for operators with a high level of expertise managing Windows XP.

Defragment the Windows Partition

You can optimize disk performance on the Windows partition if you defragment the partition before you turn on Windows Disk Protection. You should not need to defragment the Windows partition often after this. Although the installation of critical updates and program fixes will add a negligible amount of fragmentation, the disk should not require a subsequent defragmentation pass.

Do not defragment the Windows partition when Windows Disk Protection is on. Turn off Windows Disk Protection to defragment the disk.

To defragment the Windows partition

1. Turn off Windows Disk Protection.
2. Restart the computer to complete the deactivation of Windows Disk Protection.
3. Use the Windows Disk Defragmenter or a third-party tool to defragment the Windows partition.
4. Turn on Windows Disk Protection and then restart the computer.

Move the Virtual Memory Paging File

The virtual memory paging file is the file that holds parts of programs and data files that do not fit in memory. Windows XP stores this paging file in the Windows partition by default. Writing data to a paging file located on the Windows partition can dramatically reduce system performance.

By moving the paging file off the Windows partition to a persistent disk, you allow the system to optimize its use of the protection partition.

To move the paging file to a persistent disk

1. Configure Windows Disk Protection to **Save changes with next restart**.
2. Click **Start**, right-click **My Computer**, and then click **Properties**. The **System Properties** dialog box opens.
3. On the **Advanced** tab, under **Performance**, click the **Settings** button.
4. In the **Performance Options** dialog box, click the **Advanced** tab.
5. In the **Virtual memory** section, click **Change**.
6. In the **Virtual Memory** dialog box (as shown in the following figure), in the **Drive** list, click the disk that holds the Windows partition and then click **No paging file** to remove the paging file from that disk.
7. Click **Set** to apply these settings.
8. In the **Drive** list, click a disk on a persistent partition, and then click **System managed size** to configure Windows to allocate space on that disk for a paging file.
9. Click **Set** to apply these settings.
10. Click **OK** to save the paging file settings. You will receive a message that settings will not be changed until the computer restarts. Click **OK** to close the dialog box and then click **OK** to close both the **Performance Options** dialog box and the **System Properties** dialog box.
11. Click **Yes** when prompted to restart the computer and save the settings change.

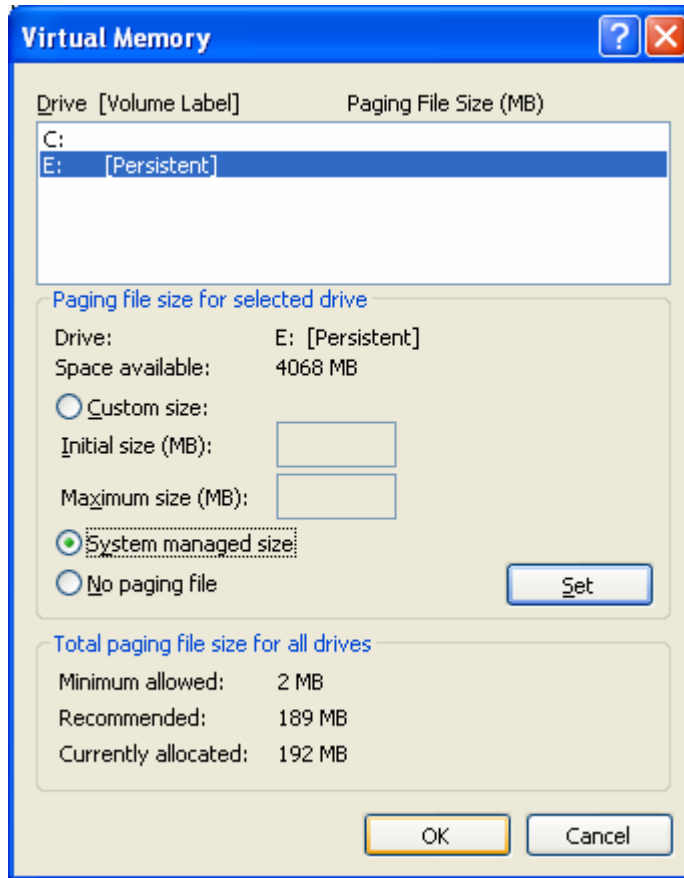


Figure 6.3 Placing the paging file on a persistent partition can optimize performance

Placing Event Logs on a Persistent Partition

Entries made to system and application event logs stored on the Windows partition will be lost each time the system restarts when Windows Disk Protection is on. For this reason, it may be worthwhile in your environment to move the event logs to a persistent partition. You can accomplish this by making a registry modification as described in the following procedure.

To move the location where event logs are stored

1. Restart your computer to clear any pending changes to the Windows partition.
2. Open the Windows Disk Protection tool and configure Windows Disk Protection to **Save changes with next restart**.
3. Open the Registry Editor and modify the paths saved in the following registry keys:
 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\
 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security\
 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\
4. Change the paths listed in the **File** key to a location on a persistent partition on your computer.
5. Close the Registry Editor and restart your computer to save the configuration changes.

Manage the Protection Partition

Windows Disk Protection functions very well for its intended purpose when configured according to the instructions in Chapter 2, "Prepare the Disk for Windows Disk Protection." Occasionally, however, it may become necessary to control the configuration of Windows Disk Protection more closely. This section describes how to use a second disk to contain the protection partition—a useful option on computers that have a nearly filled primary disk—and describes a procedure for managing the size of the protection partition.

These activities are entirely optional and are intended for operators with a high level of expertise managing Windows XP.

Place the Protection Partition on a Different Disk

The Windows Disk Protection preparation process described in earlier chapters assumes the use of a single disk drive. At times it is not feasible to use an existing disk drive, either for space considerations (the drive is nearly full) or because some other prerequisite is not met. In this case, you can use a second disk drive to store the protection partition so that Windows Disk Protection can still be used.

The following prerequisites must be satisfied for Windows Disk Protection to create the protection partition on the second disk:

- The first disk does not have enough space to support a protection partition.
- The second disk has a primary partition.
- The second disk has sufficient unallocated disk space after the primary partition to contain the protection partition.

The process of placing a protection partition on a second disk involves installing a second disk, formatting a primary partition (remember that the protection partition must follow a primary partition), and configuring the Windows Registry to allow use of the second disk as the protection partition.



Note

The second disk used in this scenario must meet the other prerequisites for Windows Disk Protection. It must not have more than three primary partitions or must have sufficient free space available in an extended partition.

To use a second physical disk with Windows Disk Protection

1. Install a second physical disk into your computer.
2. In Disk Management, create a primary partition at the beginning of the new disk.
3. Start the Registry Editor. Locate the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Computer Toolkit
4. Change the value of **SCTForceOverlay** to a size in bytes that is smaller than the unallocated disk space on the second disk.

For example, to create a 3-GB partition, use 3145728 for the value of **SCTForceOverlay** ($3 * 1024 * 1024 = 3145728$).
5. Open the Windows Disk Protection tool. Windows Disk Protection will discover the available space on the second disk and configure the protection partition when it is turned on.

If you want to change the protection partition location afterwards, uninstall and reinstall the Toolkit and repeat the protection partition creation process.

Specify the Size of the Protection Partition

You can create a protection partition of a specified size by using the **SCTForceOverlay** registry setting mentioned in the previous procedure. This works for either the first disk or the second disk. It is useful when you want to control the size of the protection partition.

The following two prerequisites must be satisfied for Windows Disk Protection to create the fixed-size protection partition on the disk:

- The disk has a primary partition.
- The disk has sufficient unallocated disk space to contain the fixed-size protection partition.

To create a fixed-size protection partition

1. Start the Registry Editor. Locate the following key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Computer Toolkit
2. Change the value of **SCTForceOverlay** to the size you want to use for the protection partition.

For example, to create a 2-GB partition, use 2097152 for the value of **SCTForceOverlay** ($2 * 1024 * 1024 = 2097152$).
3. Open the Windows Disk Protection tool. Windows Disk Protection will discover the available space on the disk and automatically configure the protection partition.

If the disk is ever reverted to an unprotected state, you can reverse these settings by changing the **SCTForceOverlay** value to **0** or by uninstalling and reinstalling the Toolkit.



Chapter 7: Security Checklist

Computer and online security is a growing concern for all computer users, and is especially important if you provide public access to shared computers. Security issues often seem complicated and overwhelming, but fortunately there are some relatively simple steps that you can take to improve the security of your shared computer environment.

Setup Checklist

Perform the following checks and steps during configuration and installation of the Microsoft® Shared Computer Toolkit for Windows® XP to ensure the best possible security for your systems:

- Set a strong administrative password or passphrase.
- Visually differentiate the administrator accounts from limited user accounts.
- Remove the Toolkit administrator account from the Welcome screen.
- Physically secure computers by keeping them in view, locking the cases, and physically marking them.
- Lock down the system BIOS
- Download and install all critical updates
- Audit physical network security
- Use a firewall
- Install antivirus software
- Install antispymware
- Install and configure Web filtering software

Maintenance Checklist (Monthly)

Check the following items monthly to ensure continued security:

- Change administrator passwords
- Visually inspect computers for signs of tampering
- Audit physical network security
- Check for updates to Windows and other installed software
- Maintain antivirus updates (if not automated)
- Maintain antispymware updates (if not automated)

The following sections describe in more detail each of these checklist items.

Toolkit Administrator Security

- **Use a strong password.** Any administrative account on a shared computer, including the Toolkit administrator account, should have a strong password. Avoid practices such as using a common dictionary word, basing a password on your name, or using a common password such as “password” or “letmein”. Also avoid using a blank password for the Toolkit administrator account. A strong password is:
 - **Long.** Passwords should be at least eight characters long, and longer is better. For the Toolkit administrator password, consider using a password that is at least 15 characters long for enhanced password security.
 - **Complex.** Passwords should use a combination of lower-case and upper-case letters, numbers, and symbols (for example, ` ~ ! @ # \$ % ^ & * () _ + - = { } | [] \ : " ; ' < > ? , . / or a space character).
- **Use a passphrase instead of a password.** In Windows XP, you can use a passphrase instead of a password. Passphrases can be long, complex, and easy to remember. Just make sure that you still use the same strong password rules mentioned previously. An example of a passphrase is “I taught my 3 old dogs 6 new tricks!”
- **Change the password regularly.** Change passwords regularly and make them different from previous passwords. Just adding a number to the end of your regular password is not different enough. You should change administrative passwords quarterly, if not more frequently.
- **Visually differentiate the Toolkit administrator account from other accounts.** Make it easy to determine at a glance if a user is logged on with the Toolkit administrator account. Use a different desktop background and even a different color scheme for menus and windows. If your shared user accounts use the Classic Start menu (as is recommended), you could have the Toolkit administrator account use the Windows XP Start menu.
- **Remove the Toolkit administrator account from the Welcome screen.** Use Getting Started or the Welcome.wsf tool to remove the Toolkit administrator account from the Windows Welcome screen. At the Welcome screen, press CTRL+ALT+DEL to access the traditional logon dialog box, in which you can type the account name and password.

Physical Network Security

- **Audit physical network security.** Make sure no unidentified computers or devices are attached to your network or can be easily attached to your network. Packet sniffers and rogue servers can be used to penetrate your network, compromising your computers and your data.

Physical Security

- **Keep computers visible.** If the shared computers are intended for public access, make sure that you can see what users are doing. Although it is usually inappropriate to look over a user’s shoulder during a session, you should at least be able to see whether the user is trying to open the computer case.

- **Lock computers.** Use locks on computer cases to ensure that users cannot open them. This prevents users from being able to open the case to add or remove components, or install monitoring devices. Use locks to keep computers and other devices attached to their tables or desks. Use an optical mouse so that users cannot take the mouse ball. Also, if you provide headphones to users, secure the headphone cable to the computer case to help prevent theft or vandalism.
- **Perform regular inspections.** After a user finishes using a computer, inspect the computer and peripherals for any signs of tampering. Some monitoring devices attach to a parallel port, USB port, or inline with a keyboard cable.
- **Mark computers.** Consider using an etching tool to mark the inside of computer cases with information that identifies the computer and your organization. Also record the model and serial numbers of computers and peripherals.

BIOS Protection

- **Update the BIOS.** Ensure that your shared computer is running the latest BIOS version available from the manufacturer of the computer before you install Windows XP.
- **Password protect the BIOS configuration.** This protection requires that a user enter a valid password to access the computer's BIOS setup screens.
- **Prevent startup from removable media.** In the BIOS setup screens, disable the options that allow the computer to start from a CD-ROM, floppy disk, or removable USB drive. This will help ensure that users cannot start the computer with an alternate operating system and make changes to the computer.
- **Use startup passwords if available.** On some computers, the BIOS offers the ability to password protect starting of the computer from certain drives (most BIOS refer to this as a "boot" password). For example, you might be able to require a password for someone to start the computer using the floppy drive, CD-ROM drive, or even the hard drive. If you do not want to disable starting from removable devices, consider using a startup password. If a user can start using their own disk, they can usually circumvent any security measures you have in place.



Important

If an untrusted user can start your computer from removable media, the computer can be modified by anyone and become untrustworthy. BIOS protections are critical security measures.

Software Updates

- **Enable critical updates in Windows Disk Protection.** Use the Windows Disk Protection tool to enable critical updates and schedule regular updates. For more information, see the "Critical Updates" section in Chapter 6, "Windows Disk Protection."
- **Check for updates with EULAs.** Routinely (at least once a month) check for critical updates that require users to accept a EULA. Accept the EULA manually, and then save the changes to disk using Windows Disk Protection.
- **Check for recommended updates.** Visit the [Microsoft Update](#) Web site monthly to check for recommended updates to Microsoft software.
- **Update other software.** Manually check for updates to third-party software. You should perform this check at least monthly.

Firewalls

- **Use a perimeter firewall.** Perimeter firewalls protect an entire network, blocking all traffic that isn't explicitly allowed between the Internet and a local network. Firewalls can also hide the addresses of the computers behind your firewall, making individual computers on a local network invisible to the outside. A perimeter firewall might be a piece of hardware that you plug into your network or a program like Microsoft Internet Security and Acceleration (ISA) Server.
- **Use a local firewall.** A local firewall is a program that you install on a computer to block unsolicited traffic coming into (and sometimes going out of) that computer. Windows XP with Service Pack 2 (SP2) comes with a local firewall called *Windows Firewall* that is enabled by default when you install SP2.

Antivirus Software

- **Install reputable antivirus software.** Antivirus software scans the contents of incoming e-mail messages, downloads, and files already on your computer, to detect virus signatures. If the software finds a virus, the software deletes or quarantines it.
- **Update the antivirus software regularly.** Because hundreds of viruses are released each month, antivirus software must be updated regularly with the latest signature definitions and scanners so that the software can catch the latest viruses. If you use Windows Disk Protection, you can use a script to download and install updates to antivirus software and save those changes to disk automatically as part of the critical updates process.

Antispyware

- **Install reputable antispyware software.** Antispyware software regularly scans the shared computer for spyware that has been installed. Some antispyware software has components that run in the background to help detect spyware before it is installed or makes changes to the computer.
- **Update the antispyware software regularly.** As with antivirus software, you must keep antispyware updated so that it can detect the latest spyware threats. Although the Toolkit does not include scripts that you can use to update antispyware software, you can use the techniques discussed in Chapter 6, "Windows Disk Protection," to update antispyware software and save the updates to disk.



Note

Some antispyware programs will warn about the operation of certain aspects of the Shared Computer Toolkit. These messages are expected and are discussed in Chapter 8, "Troubleshooting."

Web Filtering

- **Consider installing Web-filtering software.** Many companies offer products that filter Internet use based on a variety of criteria. Typically, these services are much more robust than the built-in Content Advisor in Internet Explorer. You can learn more about software vendors by browsing the [Content Filtering](#) category at the Windows Marketplace.



Chapter 8: Troubleshooting

If you have problems installing the Toolkit or using any of its tools, the following tips and troubleshooting instructions can help. This chapter covers the following topics:

- Install and uninstall
- Script-blocking security software
- Profile management
- User Restrictions
- Windows Disk Protection
- General errors

Install and Uninstall

The following are suggested solutions for possible problems that you might encounter when you install and uninstall the Toolkit.

Windows requires that I validate my copy of Windows when I try to open a tool in the Toolkit.

The Shared Computer Toolkit requires a validated copy of Windows XP. Windows checks for validation before it allows access to any of the tools in the Toolkit. After validation, you will no longer see this message.

I tried to validate Windows by going to the Windows Genuine Advantage Web site, but was unsuccessful.

You can learn more about genuine Microsoft software and find information about the validation process (including troubleshooting information) on the [About Genuine Microsoft Software](#) Web site.

I cannot validate my copy of Windows because I do not have Internet access on the shared computer.

WGA requires Internet access to validate your copy of Windows—there is no workaround. Internet access is only required temporarily for validation—you can remove it again after validation has completed.

The installer fails because UPHClean is not installed or running, but it is installed.

The installer checks that the User Profile Hive Cleanup (UPHClean) service is both installed and running. Use the Services tool from the Administrative Tools folder to ensure that the UPHClean service is actually running. If it cannot be started, uninstall and reinstall UPHClean using the Windows Installer (MSI) package.

I installed the Toolkit, but I do not see shortcuts for any of the tools on the Start menu—only shortcuts for the Accessibility tool and the Online Resources for Using Public Computers page.

The Start menu icons for the Toolkit are only installed for Toolkit administrator—the administrative account under that you used to install the Toolkit. You must log on as the user who installed the Toolkit to use the tools.

After I uninstalled the toolkit, Windows displays Script Not Found errors for some users.

Many functions of the Toolkit, such as session timers, require that the Toolkit be installed. To avoid this problem, remove restrictions and turn off Windows Disk Protection before you uninstall the Toolkit. To resolve this problem, reinstall the Toolkit, remove restrictions and turn off Windows Disk Protection, and then uninstall the Toolkit. See Chapter 1, “Installation,” for more information.

After I uninstalled the Toolkit, Windows Disk Protection no longer protects my disk from changes.

Many functions of the Toolkit, including Windows Disk Protection, require that the Toolkit be installed.

After I uninstalled the Toolkit, AutoRestart no longer works.

Many functions of the Toolkit, including AutoRestart, require that the Toolkit be installed.

Script-Blocking Security Software

The following are suggested solutions for possible problems that you might encounter if you run script-blocking software.

My security software displays an error during installation of the Toolkit that states that it has blocked a suspicious or malicious script.

Some security programs report the execution of Toolkit scripts. If you see these warnings during installation and your security software supports it, you should allow the script to run.

I cannot permanently allow or authorize scripts to run with my antispyware or security software.

Toolkit scripts must be permanently authorized to run, or the Toolkit will not work. Turn off the script blocking functionality of your antivirus or security software.

Script-blocking software displays pop-up messages that state that a malicious script has been detected when I run many of the tools in the Toolkit.

Because many of the tools in the Toolkit are scripted, script-blocking software detects when the tools are used and warns about the possibility of malicious scripts. The Toolkit scripts are not malicious. There are two ways to handle this problem:

- Disable script-blocking in your security software while you use the tools in the Toolkit.
- If your script-blocking software supports it, tell the software to authorize the script and not to ask about the script again. If you do this, you should only see the pop-up messages appear the first time you use each script.
- If possible, authorize these scripts in advance. Browse to the Shared Computer Toolkit installation folder and run each script individually one time to authorize it in your antispyware program. A list of these scripts is included in Chapter 3, “Set Up Local User Profiles.”

My antispyware program asks for approval before allowing “GetStarted.hta” to be added to Windows startup.

In order for Getting Started to run on startup, you must allow your antispyware program to add GetStarted.hta to your Run key in the registry.

Profile Management

The following are suggested solutions to possible problems that you might encounter when you configure user accounts and profiles.

Windows automatically logs on as a particular user, even though I have not configured it to do so.

If there is only one account listed on the Welcome screen and that account is configured with a blank password, Windows automatically logs on as that account. This is a feature of Windows, not of the Toolkit.

Log off the account to log on as another account not listed in the Welcome screen. To prevent **Restart at Logoff** from occurring, press down and hold the SHIFT key while you click **Log Off** and then **OK** to log off the restricted account.

To prevent the Welcome screen from logging on automatically, assign a password to the account or create another account. For more information, see [The "Welcome" Logon Screen Does Not Appear](#) and [How to automatically log on to a user account in Windows XP](#) knowledge base articles.

Alternatively, you can deselect **Use the Welcome screen to simplify the log on process for users** and **Prevent account names from being saved in the CTRL-ALT-DEL logon dialog** in Getting Started, Step 2.

The Welcome screen appears and I cannot press CTRL+ALT+DEL twice to log on as the Toolkit administrator.

This happens when you are logged on as a Toolkit administrator in an idle mode for too long, and the Toolkit administrator has been removed from the Welcome screen.

See the [Welcome Screen Appears After Your Computer Has Been Idle](#) knowledge base article for more information.

A user does not appear in the User Accounts tool.

This happens when the account has been disabled using the Accounts.wsf command-line tool. Enable the account and it will appear in the User Accounts tool.

See the [A User Account Does Not Appear in the User Accounts Tool](#) knowledge base article for more information.

All or some of the user pictures on the Welcome screen are the same.

See the [How To Add or Change a User's Picture in Windows XP](#) knowledge base article for more information.

Users of the shared computer report that every time they run a program, they have to accept a licensing agreement—even if they have already done so in a previous session.

There are two possible causes for this problem. The profile is locked or Windows Disk Protection clears the changes made by the user when the computer restarts.

- To prevent this, run programs the first time for each user account before you lock profiles or turn on Windows Disk Protection.
- To solve this problem if it occurs, restart the computer, select **Save changes with next restart** in Windows Disk Protection, clear the **Lock this profile** check box, log on as the user, run the program, and then restart the computer.

Users report the following error: “This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.”

This error message occurs because User Restrictions is configured to block access to the C: drive and the user’s profile is stored on the C: drive. The error appears when Windows Explorer attempts to access special folders (such as My Documents and My Music) that are located on that drive. To resolve this problem, remove the Windows Explorer shortcut from the Start menu and replace it with a shortcut to My Computer.

The Create Profile button does not display in the Profile Manager tool.

The user profile already exists. Delete the user profile if you want to create a new one.

The Delete Profile button does not display in the Profile Manager tool.

The user profile does not exist and must be created first.

Icons that do not exist in the Start menu folder of a user’s profile display on the user’s Start menu.

Windows XP builds a user’s Start menu by combining icons in the Start menu folders of the All Users profile and the individual user’s profile. The icons on the user’s Start menu likely exist in the All Users Start menu folder.

I installed a new program and, during installation, I selected the option to make the program available to all users. The shortcut appears on some user’s Start menus, but not on others.

Installation programs typically install shortcuts to the Start menu folder for the All Users profile. The accounts on which the shortcuts do not appear are likely restricted by the **Prevent programs from the All Users folder from appearing on the Start menu** check box in User Restrictions.

When I create a new user profile, the profile disappears after I restart the computer.

Windows Disk Protection clears changes made to the hard disk when the computer restarts. You must use Windows Disk Protection and select the **Save changes with next restart** option.

The shared computer has some programs that cannot be run by a limited user account because they require an administrative account.

Although not a recommended scenario, it is possible to restrict an administrative account so that users can run such programs. For more information, see the “Restrict a Shared Administrative Account” section in Chapter 9, “Advanced Scenarios.”

User Restrictions

The following are suggested solutions for possible problems that you might encounter when you use the User Restrictions tool.

I used the User Restrictions tool to change settings, but after I restart the computer, those changes are not there.

Windows Disk Protection clears changes made to the hard disk when the computer restarts. You must either use Windows Disk Protection to select the **Save changes with next restart** option or create the user profile on a persistent partition.

After setting user restrictions, I cannot see the Accessibility tool and some program icons on the Start menu.

Icons that are placed in the All Users Start menu folder are blocked from a restricted user's Start menu when you select the **Prevent programs from the All Users folder from appearing on the Start menu** setting. You can copy these icons into the user's Start menu folder to make them available to the user.

After setting user restrictions, I cannot run some shortcuts.

If the **Only allow software in the Program Files and Windows folders to run** software restriction setting is selected, users will not be allowed to run shortcuts to programs that do not exist in either the Program Files folder or the Windows folder. Move the program to one of these folders to allow it to run.

Users report that they are not able to change settings in Windows even though Windows Disk Protection is off.

You have likely used the User Restrictions tool to lock the user profile.

I set the restriction to prevent Microsoft Office programs from running, but users can still run Microsoft Office programs.

Most likely, Microsoft Office is not installed in the default location. This restriction works by preventing programs in C:\Program Files\Microsoft Office folder from running. If Microsoft Office is installed in another folder, the restriction will not work.

Some games (such as Microsoft Halo® or Activision Call of Duty) and other programs that use copy protection do not work properly when software restrictions are in place.

Software Restrictions can prevent some copy-protected games from running. To use those games, clear the **Software Restrictions** check box. Keep in mind that turning off software restrictions significantly weakens the security of a shared computer.

Users do not see the Web page I set within Active Desktop for a restricted account.

The recommended restrictions prevent Active Desktop from working. This is intentional.

To display a Web page containing information for all users to see upon logon, add Internet Explorer to the user's Startup folder and have it point to the Web page.

With my antispyware installed, I cannot change the Internet Explorer home page for a locked user profile without having the user receive a message from antispyware regarding the changed home page.

This warning occurs with some security software when the User Restrictions tool changes the Internet Explorer home page.

To prevent this error, change the home page within Internet Explorer before you lock the profile.

Windows Disk Protection

The following are suggested solutions to possible problems that you might encounter when you use Windows Disk Protection.

I cannot turn on Windows Disk Protection.

Make sure that the computer is prepared to use Windows Disk Protection. For more information, see Chapter 2, "Prepare the Disk for Windows Disk Protection."

I am using a dynamic disk for my Windows volume. Windows Disk Protection reports the error, “This computer does not currently support Windows Disk Protection...”

Windows Disk Protection is designed to support basic disks only. Computers that use dynamic disks for the Windows volume cannot use Windows Disk Protection. You will have to reinstall Windows using a basic disk for the Windows partition.

Windows displays a message that states “Enhanced Write Filter is committing changes to disk.”

This message is expected and appears when you use Windows Disk Protection to **Save changes with next restart**.

Windows displays a warning message on startup that it has finished installing new devices. This continues to happen through successive restarts.

This problem can occur when Windows makes changes to the system after you turn on Windows Disk Protection. You should open Windows Disk Protection, select **Save changes with next restart**, and then restart the computer.

Windows does not start and a black screen appears instead.

This problem can occur if a third-party disk partitioning utility causes corruption in the Master boot record, Partition tables, Boot sector, or NTLDR file. See the [Computer stops responding with a black screen when you start Windows XP](#) knowledge base article for more information.

When I log on to the shared computer, Windows displays a message that a critical update requires that I accept a licensing agreement. Even when I accept it, I see the same message the next time I restart the computer and log on.

Windows Disk Protection clears changes made to the hard disk when the computer restarts, including the installation of the update. The scheduled update feature of Windows Disk Protection cannot automatically accept a licensing agreement. You should restart the computer, log on as an administrator, configure Windows Disk Protection to **Save changes with next restart**, install the update, and then restart Windows.

When I run Windows Disk Protection, Windows prompts me to restart the computer.

Windows Disk Protection requires that the computer be restarted once after installation before you can turn on the tool. This is by design.

I changed or resized the partitions or added a new hard drive to the computer. Now Windows Disk Protection is not working.

Windows Disk Protection keeps track of the physical location of the disk and Windows partition. If this changes, Windows Disk Protection will no longer work. Turn off Windows Disk Protection, delete the protection partition, and turn on Windows Disk Protection again.

Windows Disk Protection seems to protect the files in the Windows directory just fine, but doesn't protect my system partition. The boot partition and system partition are separate partitions on the shared computer.

Most computers running Windows XP use a single disk partition to hold the system and boot partitions for the computer. In this circumstance, Windows Disk Protection protects the system and boot partitions. If the system and boot partitions are on separate disk partitions, Windows Disk Protection protects only the boot partition, which holds the %Windir% directory.

When I turn on Windows Disk Protection, I receive a warning message that hibernation will not work with Windows Disk Protection.

Windows Disk Protection allows files to be written or modified in the Windows partition, making them appear to be modified. When your system hibernates, the Hiberfil.sys file that stores the contents of the system RAM during hibernation is not written to the Windows partition. When you restart the computer, the system will not detect a hibernation file and will start as usual.

I receive a Delayed-write failure when Windows Disk Protection is on.

These write failures are caused by your protection partition filling up. This can happen when you burn a CD or DVD because a complete image of the CD or DVD is made on your computer prior to writing it to disk.

If your customers will need to burn CDs or DVDs or perform other disk-intensive activities, turn Windows Disk Protection off, delete the protection partition, increase the amount unallocated disk space, and then turn Windows Disk Protection back on. You need to ensure that there is sufficient disk space for their disk activities.

If you need to burn a CD or DVD, you can also simply turn off Windows Disk Protection, burn the disk, and then turn Windows Disk Protection back on.

Another time you might receive a Delayed write failure is if you are using the **Retain changes indefinitely** option. If the problem prevents you from logging on or accessing Windows Disk Protection, press F8 before Windows startup to access the **Advanced Startup Options** screen. Select the **Enhanced Write Filter Restore Mode (restores one level)** option to tell Windows Disk Protection to clear the retained disk changes.

I added a user profile for a new user, but after restarting the computer, the profile is missing.

In its default configuration, Windows Disk Protection discards all changes made to the system disk each time the computer restarts. To retain the user profile, configure Windows Disk Protection to **Save changes with next restart**. This setting will write the user profile to the disk, making it available after the restart.

I installed a new software program on my computer. When I restarted the computer, my icons were still there, but the new program was missing.

If a user profile is stored on a persistent partition it will retain icons from installed programs, even if the programs have been deleted by the **Clear Changes with each restart** option in Windows Disk Protection. To prevent this, select the **Save changes with next restart** option before you restart the computer.

I used a disk partitioning tool to make space for the protection partition, but now my system will not start.

Unfortunately, Microsoft is not able to provide support for third-party disk partitioning tools. Please contact the vendor of your partitioning tool for assistance with this issue.

When I attempt to run Getting Started or Windows Disk Protection, I get a message saying WDP.CMD is blocked by my script blocking software.

If script-blocking software blocks WDP.CMD, the Toolkit displays a warning message asking you to allow it to run. Authorize or allow WDP.CMD to run in your script-blocking program to ensure that accurate information is provided by Windows Disk Protection.

When I attempt to manage partitions using Norton PartitionMagic, the program returns an error.

Do not attempt to change any partitions when Windows Disk Protection is on. Turn off Windows Disk Protection, restart the computer, delete the protection partition (called

a Healthy Unknown partition) using Disk Management in Windows, and then use PartitionMagic to change your partitions. If you plan to use Windows Disk Protection again, make sure you keep enough unallocated space on the disk for the creation of a protection partition.

I receive an error message in the System event log stating that configuration of the page file for a crash dump has failed (Event 49).

This is expected behavior and does not affect the normal use of the computer. The system reports this error because it cannot commit changes to a page file on the Windows partition and cannot start its memory dump routines. If you want to fix this problem, move your page file to a persistent disk. For more information, see the "Improve the Performance of Windows Disk Protection" section in Chapter 6, "Windows Disk Protection."

The Disk Protection Is On popup does not start.

This popup will only start if Windows Disk Protection is on and Getting Started is not configured to open automatically. Clear the **Show Getting Started at Startup** check box in Getting Started, and ensure that Windows Disk Protection is on.

General Errors

The following are suggested solutions to other errors or concerns that you might encounter when using the Shared Computer Toolkit.

Automatic scrolling is sometimes very slow in the window for the Getting Started tool.

It is likely that there is a problem with the video driver for the graphics adapter on the shared computer. Ensure that you are using the latest driver available for your device.

When I try to run any tool in the Toolkit, I receive an error message from Microsoft HTML Application Host regarding LegitCheckControl.DLL.

LegitCheckControl.DLL has become corrupt and cannot validate that your copy of Windows is genuine, so it will not let any tools run. To fix this, delete LegitCheckControl.DLL from the Windows\System32 folder. Delete the Windows Genuine Advantage Validation tool from the Windows\Downloaded Program Files folder. Run the tool again and perform the required Windows validation steps to reactivate the Toolkit.

One of the graphical tools in the Toolkit will not start.

This can happen if a tool is forced to close while processing. Use Task Manager to end the process called mshta.exe.

The Getting Started tool displays an error that suggests that software restrictions on this computer do not apply to administrative accounts.

This warning appears only on computers on which software restriction policies have previously been configured so as not to apply to administrators. The **PolicyScope** key defines whether software restrictions apply to everyone (administrators included) or just users. If this key has previously been set to "just users," the Toolkit installation does not apply software restrictions to administrators. This helps to ensure that past software restrictions are not inadvertently applied to administrative accounts.

For more information, see [Using Software Restriction Policies to Protect Against Unauthorized Software](#).



Chapter 9: Advanced Scenarios

This section of the Handbook focuses on advanced scenarios that might fit your needs when you manage a shared computer environment. These techniques are intended for operators who have a high level of expertise managing Windows XP. Specifically, this section contains information about how to:

- Store persistent user data
- Quickly install software for a limited user
- Configure a User Start menu to not use the All Users profile
- Restrict a shared administrative account
- Block Microsoft® ActiveX® controls in Internet Explorer
- Use simple site filtering to control Internet access
- Use a central script for common client updates
- Restrict children on a family computer
- Automate User Restrictions using Restrict.wsf
- Create a mandatory profile for multiple users
- Image or clone a Toolkit-secured computer

Store Persistent User Data

On some shared computers, you may want users to be able to customize their user profile or store data, and have these changes not be discarded by Windows Disk Protection when the computer restarts. There are two ways to store persistent user data:

- Create a partition that is separate from the Windows partition that Windows Disk Protection protects. Use this separate partition to store user profiles and other user data. The advantage of using this method is that you can create persistent user profiles while still protecting the shared computer with Windows Disk Protection.
- Use a USB drive or network location to allow the storage of persistent user data. This method allows users to save data they create, but does not provide a good way to store persistent profiles.

Storing Persistent User Data on a Separate Partition

You can create a new partition to hold persistent data by using the Disk Management tool in Windows XP. To create a new partition in this manner requires that you have enough unallocated disk space with which to create the partition, and that the new partition not take away from the unallocated space required to use the Windows Disk Protection tool. After you create a new partition, you can use the Profile Manager tool to create user profiles on the new partition instead of in the default location on the Windows partition.

Create a New Partition with the Disk Management Tool

You can use the Disk Management tool in Windows XP to create a new partition from unallocated space.

**Note**

The persistent partition can be placed on the same physical disk as the protection partition or on another disk.

To use the Disk Management tool to create a new partition

1. In the Disk Management window, right-click the unallocated space on the disk on which you want to create a partition, and then click **New Partition**.
2. On the Welcome page of the New Partition Wizard, click **Next**.
3. On the Select Partition Type page of the wizard, accept the default option for **Primary partition**, and then click **Next**.
4. On the Specify Partition Size page of the wizard, determine the amount of unallocated space that you want to use to create the new volume. Make sure that you leave enough unallocated space to meet the minimum requirements for Windows Disk Protection (at least 10 percent of the size of the Windows partition or 1 GB—whichever is greater).
5. On the Assign Drive Letter or Path page of the wizard, accept the default recommendation for assigning a drive letter, and then click **Next**.
6. On the Format Partition page of the wizard, accept the default settings to create the new partition, click **Next**, and then, on the final page of the wizard, click **Finish**.

Create Persistent Profiles with the Profile Manager Tool

The Profile Manager tool lets you create and delete user profiles for existing user accounts. You can also create the profiles on alternative partitions.

To use the Profile Manager tool to create or delete persistent user profiles

1. Log on as the Toolkit administrator.
2. Click **Start**, point to **All Programs**, point to **Microsoft Shared Computer Toolkit**, and then click **Profile Manager**.
3. In Profile Manager (shown in the following figure), click **Select an Account**.
4. In the **Select an Account to Manage** dialog box, click the user account you want to manage.
5. In the **User Password** box, type the password for the user account.
6. Perform one of the following options:
 - ◆ To create a profile for the user account, select the drive on which you created the persistent partition from the **Profile Location** drop-down menu, and then click **Create Profile**. If you do not see this button, a user profile already exists for the user account.
 - ◆ To delete a user profile for the account, click **Delete Profile**. If you do not see this button, a user profile does not yet exist for the user account.
 - ◆ To open the User Accounts window to create and manage local user accounts, click **Manage Users**.
7. After you finish, click **Close**.

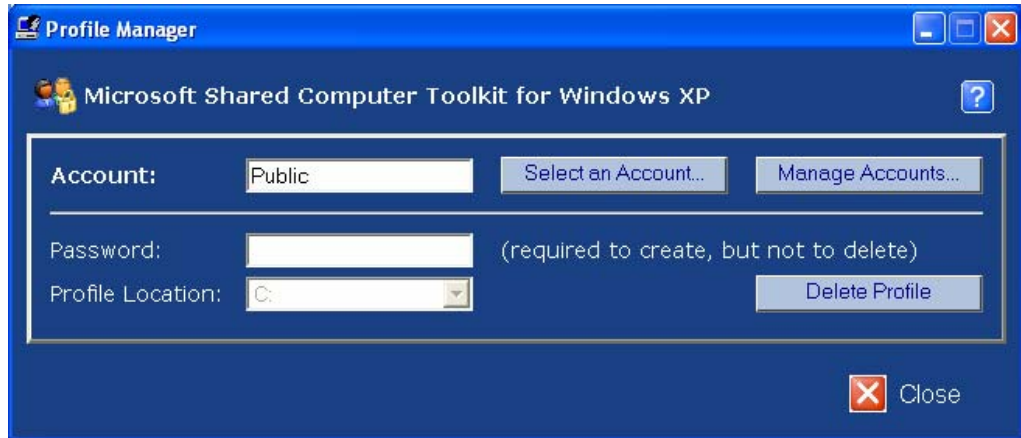


Figure 9.1 Use the Profile Manager tool to create and delete user profiles



Note

If users share a USB drive or network location, there is no way to keep documents private. Users of the same shared account will be able to view each others files.

Using Removable USB Drives or Network Locations

Windows XP provides the ability to redirect the My Documents folder (typically stored within a user's profile) to a different location. If you use Windows Disk Protection, but still want to provide users with the ability to save documents, you can redirect the My Documents folders to a persistent partition, a removable drive such as a USB drive, or to a network location.

To redirect a user's My Documents folder to a USB drive

1. Restart the computer to clear recent disk changes.
2. Log on as the Toolkit administrator.
3. If Windows Disk Protection is turned on, start the Windows Disk Protection tool, click **Save changes with next restart** and then click **OK**.
4. Start the **User Restrictions** tool.
5. Disable restrictions for the user account for which you want to redirect the My Documents folder. This step is necessary if restrictions prevent the user from right-clicking.
6. Log off and then log on using the user account for which you want to redirect the My Documents folder.
7. Insert a USB drive and wait for Windows to recognize it.
8. Click **Start**, right-click **My Documents**, and then click **Properties**.
9. In the **My Documents Properties** dialog box, click **Move**.
10. In the **Select a Destination** dialog box, click the USB drive or network location and then click **OK**.
11. In the **My Documents Properties** dialog box, click **OK**.
12. Windows displays a **Move Documents** dialog box. Click **Yes** to move the documents or **No** to leave the existing documents in the old location.
13. Log off and then log on as the Toolkit administrator. If you disabled any restrictions in Step 1, re-enable those restrictions now.
14. Restart the computer to allow Windows Disk Protection to save changes and revert to the default **Clear changes with each restart** option.

15. Log on as the user and test the My Documents folder and any restrictions placed on the user.

Quickly Install Software for a Restricted User

Often it is necessary to install software for a user temporarily. This software might only be used for a single session, or might be something you plan to add permanently, but need to add quickly and with minimal inconvenience to your client.

Fast user switching can be used to switch quickly to the Toolkit administrator account to install a program. You can then switch back to the restricted user's session without logging the user off.



Note

If you selected the **Disable keyboard shortcuts that use the Windows logo key** setting in User Restrictions, the Windows logo key + L keystroke combination will not work.

To use fast user switching to install software temporarily for a limited user

1. Press Windows logo key + L to switch to the Windows Welcome screen.
2. Log on as the Toolkit administrator.
3. Install and configure the new software. Ensure that an icon is placed on the user's Start menu or in the All Users Start menu.
4. If the software requires a restart, use Windows Disk Protection and set the Restart Option to **Retain changes for one restart** and restart the computer.
5. Log off the Toolkit administrator and log on as the limited user to resume the initial session.

Unless the software requires a restart to complete installation, the software should be available for the limited user's session.

Configure a User Start Menu to Not Use the All Users Profile

One of the optional restrictions available in the User Restrictions tool allows you to prevent Windows from displaying shortcuts from the Start menu for the All Users profile in the Start menu for individual user profiles. This restriction provides optimal control over what appears on Start menus, but also requires a bit more work to configure properly. In particular, you will need to address two added concerns:

- When you set up a user profile that will use this restriction, no shortcuts appear by default in the user's Start menu. You must use Windows Explorer to copy the shortcuts that you want from the Start menu of the All Users profile. Steps for accessing these folders in Windows Explorer are covered in Chapter 3, "Profile Management."
- When you install new programs on the shared computer, the installation program will create shortcuts in the Start menu of the All Users profile. To make the shortcuts appear on the Start menus for individual users, you must copy the shortcuts from the All Users Start menu to the user's Start menu. In addition, if Windows Disk Protection is turned on, you will need to configure it to retain changes when you copy the shortcuts. For more information, see Chapter 6, "Windows Disk Protection."

**Note**

You can find a list of third-party programs that do not work with limited user accounts in the [Certain Programs Do Not Work Correctly If You Log On Using a Limited User Account](#) article in the Microsoft Knowledge Base.

**Important**

Although the Toolkit can help restrict an administrative account, it cannot remove all security risks associated with allowing the use of such an account.

Restrict a Shared Administrative Account

Microsoft strongly recommends that you only allow users of the shared computer to log on with limited user accounts. This helps to ensure limited access to computer resources and provide the most secure environment. When using a limited user account, users will not have access to any administrative tools and privileges through which they could introduce unwanted changes to the operating system and programs.

However, there are some third-party programs that have not been designed to run properly using a limited user account and do not meet Windows XP logo requirements. Instead, a user must log on with a shared administrative account to run the programs. Although it is better to avoid such programs and use only limited user accounts, this is not always possible and you may need to allow users to log on with administrative accounts. This scenario occurs most frequently in locations such as Internet gaming cafés because many Internet-based and network-based multiplayer games require an administrative account to run. Some older educational programs experience similar problems.

If you have software with this administrative account limitation, take the following steps:

- Investigate if the software can be upgraded to a version that runs correctly with limited user account privileges on Windows XP.
- Investigate if the software can be replaced with another product that runs correctly with limited user account privileges on Windows XP.
- Investigate if the software can be removed from your environment with a limited impact on your business needs.

If you cannot accomplish all of these steps, you might find it necessary to allow some users to use a shared administrative account to use certain programs.

If your environment requires shared administrative accounts, you can use the User Restrictions tool and the Windows Disk Protection tool together to help restrict the activities of these accounts and increase the security of the computer. However no solution will provide 100 percent protection from administrative account misuse.

To restrict a shared administrative account

1. Log on as the Toolkit administrator.
2. Click **Start**, point to **All Programs**, point to **Microsoft Shared Computer Toolkit**, and then click **User Restrictions**.
3. In the **User Restrictions** window, click **Select a Profile**.
4. In the **Select a Profile to Restrict** window, click the shared administrator account you want to restrict.
5. Select the **Lock this profile** check box.
6. In the **User Restrictions** window, in the **General Settings** section, click **Select Drives to Restrict**.
7. In the **Select Drives to Restrict** window, click **Restrict All**. Click **OK**.
8. In the **User Restrictions** window, select the **Recommended Restrictions for Shared Accounts** check box. Be sure to leave all of the restrictions selected; clearing any of the restrictions creates an opening that could be abused by a malicious person who uses the administrative account.
9. Under Additional Start Menu Restrictions, select the **Prevent Programs from the All Users menu from appearing on the Start menu** check box and the **Remove Help and Support icon** check box.

10. Under Additional Software Restrictions, select the **Restrict Notepad and WordPad** check box and the **Prevent Microsoft Office Programs from running** check box. This will prevent the restricted administrator from modifying critical scripts and batch files to bypass security.
11. Click **OK** to apply the restrictions and close the User Restrictions tool.

Block ActiveX Controls in Internet Explorer

Internet Explorer provides a method of controlling security based on security zones, including being able to block ActiveX controls. Security zones contain lists of Web sites deemed to have similar security settings requirements. The four zones provided are as follows:

- **Internet.** Contains all Web sites that you have not placed in other zones.
- **Local Intranet.** Contains all Web sites that are on the local network. By default, this zone includes all sites that bypass the proxy server (if a proxy server is in use) and all local network paths.
- **Trusted Sites.** Contains Web sites that are believed to be safe. There are no sites in this zone by default.
- **Restricted Sites.** Contains Web sites that could potentially be harmful. There are no sites in this zone by default.



Important

If you block ActiveX controls it will cause problems with some Web pages.

Although it is generally a good idea to leave each security zone set to its defaults, you can customize the security level for each site if the default settings are not adequate for a user. By default, the Internet security zone prevents the downloading and installation of unsigned ActiveX controls. To increase this security, you can customize the Internet security zone.

To block ActiveX controls in Internet Explorer

1. Log on as the Toolkit administrator.
2. If necessary, remove restrictions from the user account for which you want to block ActiveX controls and configure Windows Disk Protection to **Save changes with next restart**.
3. Log on as the user for which you want to block ActiveX controls.
4. Start Internet Explorer.
5. In Internet Explorer, on the **Tools** menu, click **Internet Options**.
6. In the **Internet Options** dialog box, click the **Security** tab.
7. Click the Internet security zone, and then click **Custom Level**.
8. In the **Security Settings** dialog box, disable each of the settings in the **ActiveX controls and plug-ins** section of the list.
9. Log on as the Toolkit administrator again, enable restrictions for the user, and then restart the computer.

Use Simple Site Filtering to Control Internet Access

The User Restrictions tool provides a way to disable Internet access. Although it might be necessary on some shared computers to enable Internet access, you can limit the sites to which a user can connect.

Use the following procedure to limit Internet access to a few selected sites. This procedure only works in environments that do not use a proxy server.

To use simple site filtering in Internet Explorer

1. Log on as the Toolkit administrator.
2. Open the User Restrictions tool and select the user profile you want to limit.
3. Under **Optional Restrictions**, expand **Additional Internet Explorer Restrictions**, and then select the **Prevent Internet access from Internet Explorer** check box.
4. The Proxy setting will change to NoInternetAccess, which will disable access for all sites except for those listed in the **Proxy Exceptions** box.
5. In the **Proxy Exceptions** box, list any sites that you will allow this user to browse. Within the allowed sites list, you can use wildcard characters such as *.microsoft.com. Use a semicolon (;) as a delimiter between sites.
6. Click **OK**.
7. Log on as the restricted user and use Internet Explorer to confirm that the chosen sites are the only ones available.
8. Log on as the Toolkit administrator.
9. Configure Windows Disk Protection to **Save changes with next restart** and then restart the computer to save changes.

If more advanced site or content filtering services are required, search the [Windows Marketplace](#) for a third-party product that meets your requirements.

Use a Central Script for Common Client Updates

If you have several shared computers on a network, there may be times when you need to apply an update or perform an installation on all of those shared computers even though Windows Disk Protection is turned on. To address this issue, you can use the **Other Script** option in Windows Disk Protection to call a common script from a network location.

For example, you could keep a script named Sharedupdate.bat in a shared folder on the network. Generally, you would keep this script empty—a blank document. Each day during the regular update process, shared computers would execute this empty script to no effect. When you want the shared computers to run a script (for example, to install a new program), you could simply add the proper script to the Sharedupdate.bat file. After the regular update cycle, when all of the shared computers have run the script, you could return the Sharedupdate.bat file to its empty state.

Restrict Children on a Family Computer

Although not the intended purpose of the Toolkit, one exciting possibility the Toolkit offers is the ability to restrict the actions of other kinds of users in other environments. One such environment is a home computer used by children.

On a home computer, the User Restrictions tool makes it easy to control the Windows features and programs to which a child has access. For example, you could restrict a child in the following ways:

- Prevent the child from using Internet Explorer or Windows Messenger.
- Prevent the child from changing the profile used to log on to Windows.
- Apply time restrictions to the child's computer use.
- Restrict access to Windows features that would enable the child to modify configurations or run inappropriate programs.
- Restrict the features and programs that are available on the Start menu.

You could use the Windows Disk Protection tool to ensure children can't make permanent changes to Windows. Be careful using Windows Disk Protection on computers on which you want to save data permanently. Without careful planning, you might inadvertently clear documents, pictures, and other important files that you and your family want to keep.



Important

The examples provided here are not intended as prescriptions for keeping your child safe, but as examples of how you could use the Toolkit to help implement a security and privacy plan for your child. The Online Resources for Using Public Computers Web page provides links to a number of resources that you can use to learn more about children and computers.

Example 1: Restrict a Young Child

For a young child, particularly one who is first learning to use a computer, a parent's goal is both to protect the child from the dangers associated with online activity and to protect the computer from the fearless explorations of the child.

You could use the Toolkit to restrict a young child's activities in the following ways:

- User Restrictions
 - Lock the user profile so that no permanent configuration changes are allowed. If you lock the user profile, you can redirect the My Documents folder for the user profile to a folder on a persistent partition so that the child can still save documents. You could also store the user profile on the Windows partition and turn on Windows Disk Protection for additional protection.
 - Configure the Start menu so that only local games are available—not Internet-based games. You could also make games that have inappropriate content unavailable to young children.
 - Disable Internet access. Experts suggest that young children only be allowed Internet access when parents or teachers can help them, or at least only be allowed to use the Internet on a computer that is in a public family area.
 - Disable Windows Messenger. Most experts agree that instant messaging programs are not appropriate for young children.
 - Prevent disk access to all disks except the disk on which the child is allowed to store documents.
 - Set time restrictions that enforce the limits you have chosen for your family.
 - Configure User Restrictions to prevent access to areas of the operating system the child should not be involved with.
 - Configure Start menu restrictions to prevent access to operating system features and programs.

- Windows Disk Protection
 - Turn on Windows Disk Protection so that changes a child makes are not saved. This is especially important if you allow the child to access the Internet, e-mail, Windows Messenger, or have access to configuration tools.

Example 2: Restrict a Teenager

For a teenager, you will probably want to set fewer restrictions than for a young child. In particular, teenagers will often need access to the Internet, e-mail, and Windows Messenger. They will also find it more important to be able to configure their desktop, and might even enjoy having access to other configuration tools so that they can learn more about the operating system.

You could use the Toolkit to restrict a teenager's activities in the following ways:

- User Restrictions
 - Do not lock the user profile. Teenagers will want to be able to configure their environment. Redirect the My Documents folder for the user profile to a folder on a persistent partition and also store the user profile on a persistent partition, such as a D: drive.
 - You may want to configure the Start menu so that some Internet games are available to your teenager. If not, you should configure the Start menu so that only local games are available.
 - Enable Internet access and Windows Messenger. You might want to use the privacy options in Internet Explorer or configure additional parental controls for Internet use.
 - Set time restrictions that enforce the limits you have chosen for your family.
 - Set restrictions to prevent access to some areas of the operating system.
 - Configure Start menu restrictions to prevent access to operating system features and programs.
- Windows Disk Protection
 - Turn on Windows Disk Protection so that changes made to the Windows partition are not saved.

Automate User Restrictions Using Restrict.wsf

The command-line tool Restrict.wsf allows you to configure restrictions for a user profile by using restrictions stored in an XML file. Examples of ways that you can use this tool with an XML file include the following:

- Use a preconfigured XML file to apply restrictions to users. The Toolkit includes several sample XML files in the XML folder inside the program's folder (C:\Program Files\Microsoft Shared Computer Toolkit\xml). For example, the file Restrict.Office.XML can be used to restrict Microsoft programs and can also be customized to restrict third-party programs.
- Use Restrict.wsf to create an XML file for a user. You could then customize the XML file to add restrictions for the user or for additional users.
- Use Restrict.wsf to apply an XML file to a user.
- Use Restrict.wsf to lock or unlock a profile.

The syntax for Restrict.wsf is as follows:

Restrict.wsf [/User:username] [/Create] [/Apply] [/Accounts] [/XML:filename.xml] [/Lock] [/Unlock]

- **/User** Specifies which user to configure with this tool.
- **/Create** Tells the tool to create an XML file using the specified user's settings.
- **/Apply** Applies settings from an XML file to the specified user.
- **/Accounts** Lists user accounts that the tool can be used to configure.
- **/XML** Specifies the file name to be used to store or apply settings for the specified user.
- **/Lock** Locks the specified user's profile.
- **/Unlock** Unlocks the specified user's profile.

If you were using Restrict.wsf to copy restrictions from user Jane to file Cafe.xml, you would issue the following command:

Restrict.wsf /User:Jane /Create /XML:Cafe.xml

To use Restrict.wsf to apply restrictions to user Joe from file Cafe.xml and also lock Joe's profile, you would issue the following command:

Restrict.wsf /User:Joe /Apply /XML:Cafe.xml /Lock

In addition to saving and applying settings for a single user, Restrict.wsf can be used to automate the application of settings to many users.

Create a Mandatory Profile for Multiple Users

Mandatory user profiles are essentially roaming profiles to which users cannot make permanent changes. Mandatory user profiles are available in Windows XP Professional, but not in Windows XP Home Edition. Mandatory user profiles are stored on a network server and are downloaded and applied each time a user logs on. The profile is not updated when the user logs off.

The advantage of using a mandatory profile is that you can make changes only to the master mandatory profile and have that profile used on any shared computer. The potential disadvantage of mandatory profiles is that the shared computer must have network access for a user to log on. If a mandatory user profile is unavailable, the user cannot log on.

To create a mandatory profile for multiple users:

1. Create a shared folder on a network server that will hold profiles.
2. Create a subfolder in that shared folder for each mandatory profile you want to use.
3. On each shared computer, start the Computer Management tool. (Right-click **My Computer**, and then click **Manage**.)
4. In the Computer Management tool, under **Local Users and Groups**, expand the **Users** folder.
5. For each user account that will use the mandatory profile, right-click the account and then click **Properties**.

6. In the **Properties** dialog box, on the **Profile** tab, in the **Profile Path** box, type the network path to the share where the profile is saved (for example, `\\server1\profiles\user1`).
7. Create, configure, and restrict a user profile and then copy that user profile to the appropriate network share.
8. In the network share, in the profile folder, rename the `Ntuser.dat` file to `Ntuser.man`. This changes the profile from a simple roaming profile to a mandatory profile.

For more information about how to create and use mandatory user profiles, consult the following resources:

- For general information about roaming and mandatory profiles, see the [User Profiles Overview](#) topic in the Windows XP Professional Product Documentation.
- For steps on how to assign a mandatory profile to a user account in Windows XP, see the [How To Assign a Mandatory User Profile in Windows XP](#) article in the Microsoft Knowledge Base.

Image or Clone a Toolkit-Secured Computer

When you install Windows XP Professional on several computers that have identical hardware configurations, the most efficient installation method to use is disk imaging—a process that is also referred to as *cloning*. This method involves the following actions:

- **Configure a reference computer.** This is a computer that is prepared in accordance with the instructions found in Chapters 1–5 in this Handbook.
- **Use the System Preparation Tool (Sysprep.exe) to prepare the computer for imaging (optional).** You can find Sysprep.exe on the Windows XP operating system CD. For more information about the use of Sysprep.exe, see the [Sysprep](#) section of the Windows XP Resource Kit.
- **Create an exact image of the reference computer's hard disk and transfer that image to the hard disks of other computers.** You can accomplish this through the use of a disk imaging program such as Symantec Norton Ghost or Acronis True Image.
- **Perform some final tasks on the cloned computer.** After imaging, the cloned computer will start a mini-setup program that validates and activates Windows XP for use on the new system.

Configure a Reference Computer

You must first configure a reference computer that will be cloned. Configuring a reference computer involves the following tasks:

- **Install the operating system.** Install either Windows XP Professional with SP2 or Windows XP Home Edition with SP2.
- **Prepare the hard disk for Windows Disk Protection.** For more information, see Chapter 2, “Prepare the Disk for Windows Disk Protection.”
- **Install the Microsoft Shared Computer Toolkit for Windows XP.** For more information, see Chapter 1, “Installation.”
- **Create local limited user accounts.** For the reference computer, create a superset of all the user accounts you will need on all the shared computers. You can always remove accounts you won't need from specific computers.

**Important**

Do not turn on Windows Disk Protection before cloning a computer. This can result in difficulty obtaining a clean disk image and problems on the destination computers.

- **Create and customize the user profiles for each account.** For more information, see Chapter 3, “Profile Management.”
- **Configure user restrictions on the computer.** For more information, see Chapter 4, “User Restrictions.”

Use the System Preparation Tool

After you configure the reference computer, your next step is to prepare the computer for imaging. Many settings on a Windows XP Professional computer must be unique, such as the Computer Name and the Security Identifier (SID), which is a number used to track an object through the Windows security subsystem. To address this need, Windows XP Professional provides a utility called the System Preparation Tool (Sysprep.exe) that removes the SID and all other user-specific and computer-specific information from the computer, and then shuts down the computer so that you can use a disk duplication utility to create a disk image. The disk image is simply a compressed file that contains the contents of the entire hard disk on which the operating system is installed.

Typically, when a client computer starts Windows XP Professional for the first time after loading a disk image that has been prepared with Sysprep, Windows automatically generates a unique SID, initiates Plug and Play detection, and starts the Mini Setup Wizard. The Mini Setup Wizard prompts for user-specific and computer-specific information, such as the End-User License Agreement (EULA), regional options, user name and company, product key, and so on.

You can further automate the imaging process by including with your master image a special answer file named Sysprep.inf. Sysprep.inf is an answer file that is used to automate the Mini Setup process. It uses the same INI file syntax and key names (for supported keys) as Unattend.txt. Place the Sysprep.inf file in the %systemdrive%\Sysprep folder or on a floppy disk. If you use a floppy disk, insert it into the floppy disk drive after the Windows startup screen appears. Note that if you do not include Sysprep.inf when running Sysprep, the Mini Setup Wizard requires user input at each customization screen.

To learn more about how to use the System Preparation Tool, consult the following resources:

- For an overview of the process of imaging clients, including the use of Sysprep to prepare a system for imaging, see the TechNet [Imaging](#) Web site.
- For information about how to customize Sysprep installations, see [Customizing Sysprep Installations](#) section in the Windows XP Professional Resource Kit.

Create and Transfer a Hard Disk Image

After you run the System Preparation Tool to prepare the reference computer for imaging, the tool shuts down the reference computer. At this point, you can use a third-party imaging tool to create an image of the computer’s hard disk. You can find recommendations for imaging tools by searching for drive copying utilities at the [Windows Marketplace](#).

Popular imaging utilities include:

- [Symantec Norton Ghost 9.0](#)
- [Acronis True Image 8.0](#)

**Note**

When you create a disk image, all the hardware settings of the reference computer become part of the image. Thus, the reference computer should have the same (or similar) hardware configuration as the destination computers.

**Note**

Volume-licensed Windows XP computers will not require activation or validation after cloning if the original image was activated and validated. This is one of the advantages of the Volume Licensing program.

Post-Imaging Activities

After you transfer an image to a new computer and start the computer, Windows generates a unique SID, initiates Plug and Play detection, and starts the Mini Setup Wizard. After installation finalizes, there are several tasks you must complete. These include:

- **Activate Windows.** For more information about this step, see [Description of Microsoft Product Activation](#) article in the Microsoft Knowledge Base.
- **Validate Windows XP.** You can validate Windows through the [Windows Genuine Advantage](#) Web site. If you used Sysprep to prepare the computer for imaging, you will be required to validate Windows again before using the Toolkit tools.
- **Turn on Windows Disk Protection.** You can turn on Windows Disk Protection by using tool directly, or you can use the **DiskProtect** command-line tool.



Chapter 10: The Shared Computer Toolkit in Domain Environments

This chapter of the Handbook focuses on using the Shared Computer Toolkit on computers in a domain environment, and handling other enterprise-level requirements. Specifically, this chapter covers:

- The Shared Computer Toolkit and Active Directory
- Windows Disk Protection on domain-joined computers
- Create a persistent local user profile for a domain account
- Group Policy restrictions for domain accounts
- User restrictions for unrestricted domain accounts
- User profiles in other languages

The Shared Computer Toolkit and Active Directory

The Active Directory® directory service offers significant benefits for shared computers on a network. Active Directory gives network users controlled access to resources anywhere on the network using a single set of credentials. It also provides network administrators with an intuitive, hierarchical view of the network, and a single point of administration for all network objects.

Active Directory provides a better environment for centrally managing user accounts that require access to network resources or need to log on with the same credentials on multiple computers, as many educational institutions require. For these reasons, the Shared Computer Toolkit has been designed to work as favorably in domain environments as it does for workgroup computers.

Windows Disk Protection works well out-of-the-box on domain-joined computers, greatly easing the administrative burden of securing and maintaining Internet kiosks, employee self service systems, and public access computers in a domain.

Most of the settings and restrictions available in the User Restrictions tool are available through the Group Policy template (SCTSettings.adm) provided with the Toolkit. Group Policy is more effective than the User Restrictions tool for restricting multiple user accounts across numerous computers at one time.



Note

The Toolkit provides a Group Policy template (SCTSettings.adm) that includes most of the settings found in the User Restrictions tool. You can use this template to configure users in a Group Policy object.

**Note**

Windows Disk Protection disables the automatic client initiation of machine account password changes in the domain. To remedy this, Windows Disk Protection updates the password automatically every time disk changes are saved. At a minimum, this happens during the scheduled critical updates process.

**Important**

Domain-joined clients running Windows Disk Protection must not run for 30 days with either **Retain changes** restart option, otherwise they will become unjoined from the domain due to a stale machine account password.

Windows Disk Protection on Domain-Joined Computers

When a computer running Windows XP Professional is joined to an Active Directory domain, the computer uses a machine account password to authenticate with the domain and gain access to domain resources. By default, the domain-joined computer initiates a change to the machine account password automatically within every 30-day period. A domain controller accepts the password change and allows the domain-joined computer to continue to authenticate. The new password is stored locally on the domain-joined computer and can be confirmed by Active Directory. If a password change fails, or if a domain-joined computer attempts to use an incorrect password, the computer will not be able to access the domain.

Machine Account Passwords in a Domain Environment

When Windows Disk Protection is turned on, the tool disables the automatic client-initiated machine account password updates on the computer. Windows Disk Protection then automatically initiates a password change every time disk changes are saved. This happens one time when Windows Disk Protection is turned on. Thereafter, the update occurs at each restart where disk changes are saved. At a minimum, this happens during the scheduled critical update process.

The reason for this change in functionality is that if a shared computer with Windows Disk Protection turned on were to initiate a machine account password change, a new password would be created in Active Directory. Upon restarting the computer, Windows Disk Protection would revert to the previous password. This would result in an inability to access all domain resources.

If you turn on either of the **Retain changes** options in Windows Disk Protection, no changes to the Windows partition are saved. If a machine account password change is made while one of these options is turned on and changes are not saved within the maximum number of days allowed for a password change by the domain (30 days, by default), the machine account passwords will become out of sync. Therefore, you should not run with either **Retain changes** restart option for 30 days or longer.

One other issue to be aware of is the result of changing the **Restart Option**. If you configure Windows Disk Protection to **Save changes with next restart**, it changes the domain password immediately in anticipation of being restarted. If you then configure Windows Disk Protection to **Clear changes with next restart**, the computer discards the new password and can no longer log on to the domain.

Central Software Management and Windows Disk Protection

When Windows Disk Protection is on, software updates to the computer are ideally performed through the critical updates process offered by Windows Disk Protection. Windows Disk Protection keeps the computer trustworthy by first performing a regularly scheduled restart to clear all disk changes, and then downloading and installing the required updates on top of this trusted base. This model is a little less flexible than some central software management models in which updates can be initiated centrally and scheduled to occur at any time.

A centrally managed software distribution system, such as Microsoft Systems Management Server, can provide the flexibility to schedule software updates to occur at any time, but this flexibility cannot be easily matched by Windows Disk Protection.

If your organization has a strong need to regularly change the schedule for software updates, rather than following a fixed schedule you set within Windows Disk Protection, you might want to consider whether Windows Disk Protection is right for your environment.

In contrast, if you can integrate your centrally managed software update process into the client-driven Windows Disk Protection update process, you might find a happy medium in which central software distribution and Windows Disk Protection can co-exist.

Mobile Computers and Windows Disk Protection

It is important to note that the software management model used by Windows Disk Protection might not be appropriate for environments with portable computers such as notebooks and tablets that are routinely disconnected or turned off at the time when the Windows Disk Protection critical updates process is scheduled to occur.

Managing Windows Disk Protection Using DiskProtect.wsf

To automate the configuration of Windows Disk Protection on multiple computers, you can use the DiskProtect.wsf command-line tool included with the Shared Computer Toolkit. This tool can be used in batch files and scripts to configure Windows Disk Protection.

The syntax for this tool is:

```
DiskProtect.wsf [/Status] [/On] [/Off] [/Save] [/Clear] [/Retain] [/Once] [/Restart] [/MU]
[/NoMU] [/AV] [/Other] [/Time] [/Day]
```

The following example would turn on Windows Disk Protection, enable Microsoft Updates, and install McAfee Antivirus updates—all at 2:00 A.M.:

```
DiskProtect.wsf /On /MU /AV:"C:\Program Files\Microsoft Shared Computer
Toolkit\scripts\update\SCTMcAfeeVirusUpdate.vbs" /Time:2
```

DiskProtect.wsf can be called from batch files, logon scripts, and software installation scripts. One use would be to set Windows Disk Protection to **Save changes with next restart** to allow the scripted installation of a program. Upon restart, the program would be saved to the Windows partition.



Note

Running the DiskProtect.wsf tool with the `/?` option will give a description of each command-line option.

Create a Persistent Local User Profile for a Domain Account

For some domain accounts that log on to shared computers, you may find it necessary to create a persistent local user profile that is not affected by the default restart behavior of Windows Disk Protection when it clears all disk changes made to the Windows partition. This might be necessary, for example, to allow a teacher to save her documents and Windows settings on a computer protected by Windows Disk Protection.

To create persistent local user profiles for domain accounts, use the ProfileMgr.wsf command-line tool located in the **Scripts** subfolder of the Toolkit installation. To create a user profile, use the following command syntax:

```
ProfileMgr.wsf /create username password /domain:<domain name>
/drive:<drive letter>
```

For example, to create a profile on drive D for a user named User1 in the Contoso domain with the password UserPass5, you would use the following command:

```
ProfileMgr.wsf /create User1 UserPass5 /domain:Contoso /drive:D:
```

Create Persistent Local User Profiles for all Accounts

If you want to ensure that all of the local user profiles created for any accounts, including domain accounts, are placed on a persistent partition where they are not affected by



Note

When you use ProfileMgr.wsf to create a profile on a persistent partition, it creates a Documents and Settings folder to contain the new profile (if one does not already exist).

Windows Disk Protection, you will need to customize the computer installation so that the default location for user profiles is not on the Windows partition.

It is possible to change the default location where user profiles are installed, but the only supported way to make this change is during Windows XP installation, and you must make the change by automating the installation of Windows with a special answer file. This method changes the location where *all* user profiles are stored, including the Default and All Users profiles. This allows you to have Windows automatically create profiles on a persistent partition instead of having to use the Profile Manager tool to specify the location of profiles as they are created.

Answer files are text files that contain responses to some, or all, of the questions that Setup asks during the installation process. After creating an answer file, called unattend.txt, you can apply it to as many computers as necessary.

The easiest way to create an answer file for an unattended installation of Windows XP is to use Windows Setup Manager, a deployment tool that provides a wizard-based interface for creating the answer file. For more information about using Setup Manager to automate installations, see the [Automating and Customizing Installations](#) chapter in the Windows XP Resource Kit. The answer file you create using Setup Manager can include other information, such as the time zone, network settings, and so on.

After you create an answer file, you can change the default location where user profiles are stored by adding the following entry:

```
[GuiUNattended]
ProfilesDir = drive:\foldername
```

Group Policy Restrictions for Domain Accounts

The Toolkit includes a Group Policy template called SCTSettings.adm in the bin folder of the install. This template reproduces most of the settings included in the User Restrictions tool and can be used to deploy these restrictions to users that are members of an Active Directory domain.

Group Policy for a domain can be configured either with the Group Policy Management Console, an add-on tool available for download from Microsoft, or by using the Group Policy Editor built into Active Directory Users and Computers. By adding the SCTSettings.adm template into these tools, you gain access to account restrictions and settings that are appropriate for shared accounts.

The SCTSettings.adm Group Policy template included with the Shared Computer Toolkit also includes the ability to set idle and mandatory logoff timers, if the Toolkit is installed on your computers.

It is important that you only apply these settings to specific user accounts, so as not to restrict legitimate administrative activities on any computers.

**Note**

Microsoft recommends that you create an OU that stores the shared user accounts in your environment, and that you apply the SCTSettings.adm template to the User Configuration portion of a Group Policy Object linked to this dedicated OU.

**Important**

The SCTSettings.adm template was designed to be applied only to the User Configuration of a Group Policy Object. Do not apply the SCTSettings.adm template to the Computer Configuration because this will restrict all users of computers affected by the policy.

To use Active Directory Users and Computers to manage Toolkit restrictions

1. To start Active Directory Users and Computers on a Windows Server 2003 computer, browse to Administrative Tools, which is located on the Start menu or in Control Panel.
2. In the Active Directory Users and Computers console, right-click the organizational unit (OU) for which you want to configure policy, and then click **Properties**.
3. On the **Group Policy** tab, click the policy you want to modify, and then click **Edit**.
4. Expand **User Configuration**, right-click the **Administrative Templates** folder, and then click **Add/Remove Templates**.
5. In the **Add/Remove Templates** dialog box, click **Add** and then browse to the location of the SCTSettings.adm template (usually the Program Files\Microsoft Shared Computer Toolkit\bin folder.)
6. Browse the settings in the **All Shared Computer Toolkit Restrictions** folder and note their similarity to the settings in User Restrictions. Note also the explanations given for each setting.
7. Make any restrictions changes that you want and then exit the Group Policy Editor.

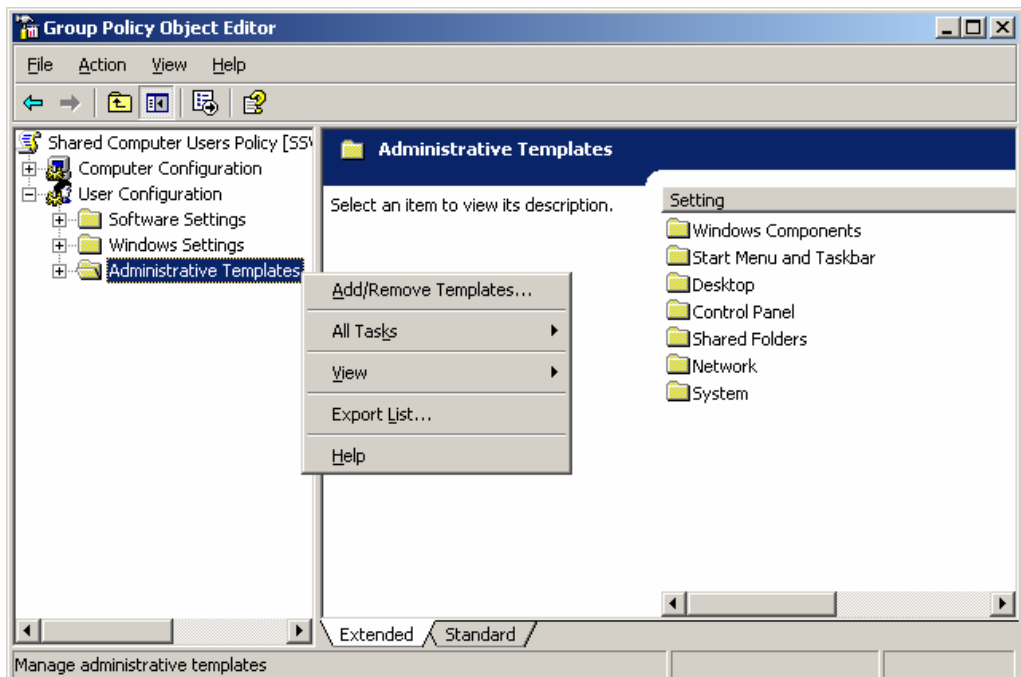


Figure 10.1 Configuring Group Policy templates in the Group Policy Editor

**Note**

Software restrictions can be tailored to individual users or groups of users by creating more than one policy and controlling which policy is applied to each user through security settings.

Using Group Policy to Configure Software Restriction Policies

Software Restriction Policies provide control over which programs are allowed to run on a computer. The Shared Computer Toolkit provides some Software Restrictions in the User Restrictions tool. This tool works well for a few computers, but becomes unwieldy to manage when the number of computers or locations increases. Configuring Software Restriction Policies in Group Policy is the best way to centrally manage software restrictions across many computers or users.

Software restrictions that are identical to those applied by the User Restrictions tool can be configured in Active Directory using Software Restriction Policies, which are located in Group Policy under Security Settings.

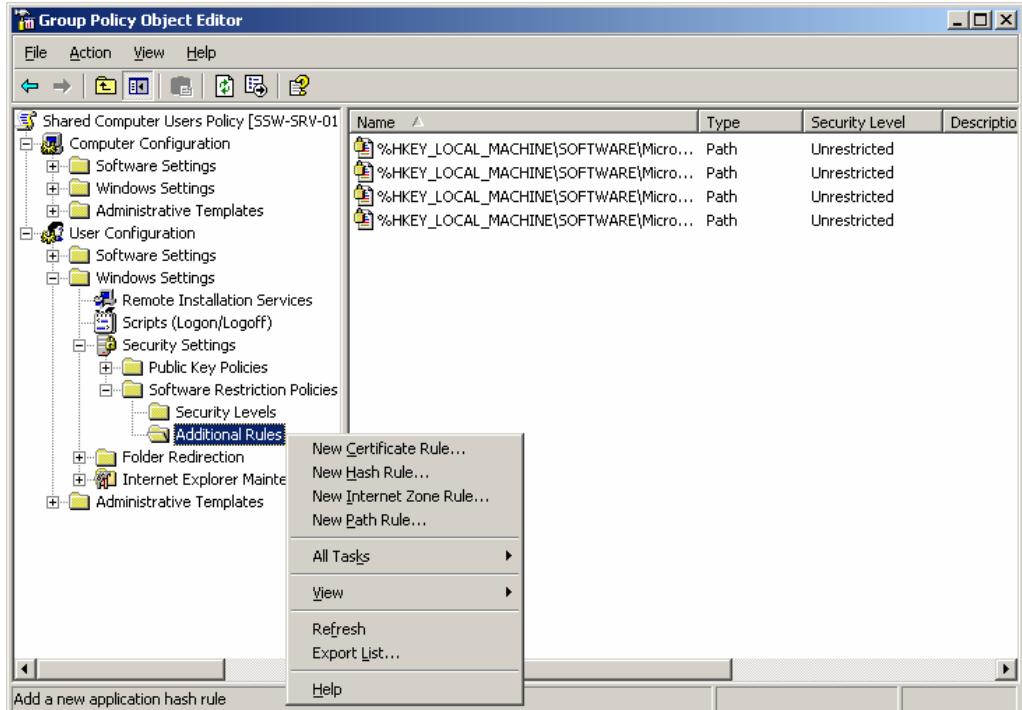


Figure 10.2 Use path rules to restrict software based on its name or location

✓ **Note**

Software restrictions may also be applied Computer Configuration—use caution and ensure that legitimate administrators are not restricted by setting Enforcement to All users except local administrators.

✓ **Note**

For more information about software restrictions, see the [Using Software Restriction Policies to Protect Against Unauthorized Software](#) article on TechNet.

To configure Windows XP software restrictions using Group Policy

1. To start Active Directory Users and Computers on a Windows Server 2003 computer, browse to Administrative Tools, which is located on the Start menu or in Control Panel.
2. In the Active Directory Users and Computers console, right-click the Active Directory domain or an organizational unit for which you want to configure policy, and then click **Properties**.
3. On the **Group Policy** tab, click the policy that you want to modify, and then click **Edit**.
4. Expand **User Configuration, Windows Settings, Security Settings**, and then click **Software Restriction Policies**.
5. If Software Restriction Policies have been defined, there will be an **Additional Rules** folder under **Software Restriction Policies** that contains rules.
6. You can edit an existing definition or right-click the **Additional Rules** folder, and then click **New Path Rule** (as shown in the following figure).
7. In the **New Path Rule** dialog box, enter the path and then choose whether the rule will **Disallow** or **Unrestrict** software in the path. The path entry can use environment variables (such as %ProgramFiles%) and wildcard characters (* and ?) to define the path.
8. Click **OK** to save the new path rule.

**Note**

Prevent Windows Messenger and MSN Messenger from running is included in the SCTSettings.adm Group Policy template and does not use a path restriction.

To duplicate the software restrictions put in place by the Users Restrictions tool, create the path rules defined in the two following sections. Optionally, you can also restrict Notepad and WordPad and prevent Microsoft Office programs from running using Software Restriction Policies as described below.

Only allow software in the Program Files and Windows folders to run

To use Software Restriction Policies to duplicate the effect of the **Only allow software in the Program Files and Windows folders to run** check box in the User Restrictions tool, set the Software Restriction Policy Security Level to Disallowed, then create additional rules to unrestrict or allow each of the following paths:

- %ProgramFiles% (this allows programs to run)
- %Windir% (this allows Windows programs to run)
- *.lnk (this allows Start menu and desktop shortcuts to work)

As an added security measure, you should also create an additional path rule that disallows files from running from the Temp folder, because all users have access to write files to this location:

- %WinDir%\Temp

Prevent System Tools and some management tools from running

To use Software Restriction Policies to duplicate the effect of the **Prevent System Tools and some management tools from running** check box in the User Restrictions tool, create an additional path rule to disallow each of the following:

NTBackup.exe, Cleanmgr.exe, Migwiz.exe, MSInfo32.exe, Rstrui.exe, CACLS.exe, MMC.EXE, Diskpart.exe, Net.exe, Reg.exe, Regini.exe, GPEdit.exe, XCopy.exe, Rename.exe, Ren.exe, Control.exe, DiskMgmt.msc, NusrMgr.cpl, ConfigWizards.exe, DDEShare.exe, RegSvcs.exe, RegSvr32.exe, ShrPubw.exe, SPUninst.exe, FSquirt.exe, and DxDiag.exe

If the Shared Computer Toolkit is installed on your computers, create additional path rules to disallow each of the following:

ETPrep.exe, EWFMgr.exe, SrvAny.exe, NetDom.exe, UPHClean.exe, XPePM.exe, SchTasks.exe, CreateProfile.exe, DenyAccess.exe, WindowsUpdates.vbs, Banner.wsf, DiskProtect.hta, GetStarted.hta, CheckWDP.hta, ProfileMgr.hta, and Restrict.hta

Restrict Notepad and Wordpad (recommended for Restricted Administrators)

To use Software Restriction Policies to duplicate the effect of the **Restrict Notepad and Wordpad** optional restriction check box in the User Restrictions tool, create an additional path rule to disallow the following:

- Notepad.exe
- Wordpad.exe

Prevent Microsoft Office programs from running

To use Software Restriction Policies to duplicate the effect of the **Prevent Microsoft Office programs from running** optional restriction check box in the User Restrictions tool, create an additional path rule to disallow the following:

- %ProgramFiles%/Microsoft Office

Restart at Logoff Using a Logoff Script

When a Windows XP-based computer is joined to a domain, it can become more difficult to ensure changes are cleared between user logons. Because the User Restrictions tool will

**Note**

You might want to research the paths of additional programs that you want to restrict. You can restrict other programs in addition to those listed here.

not be used in a domain scenario, it becomes necessary to reproduce the **Restart at Logoff** function usually provided by this tool.



Note

You can use the **shutdown** command in a batch file to restart the computer. At the command line, issue the command **shutdown -r -t 00**

The **shutdown** command is restricted when you restrict access to the command prompt. You can also use the **ForceLogoff.exe** tool included with the Toolkit to restart the computer.

To use Group Policy to force the computer to restart when a user logs off

1. Open the Group Policy object for the domain or organizational unit to which your users belong.
2. Under **User Configuration**, expand **Windows Settings**, and then click **Scripts (Logon/Logoff)**.
3. Open the **Logoff** object and add a logoff script. The logoff script can be a script written in any scripting language supported by Windows that contains a command to restart the computer.

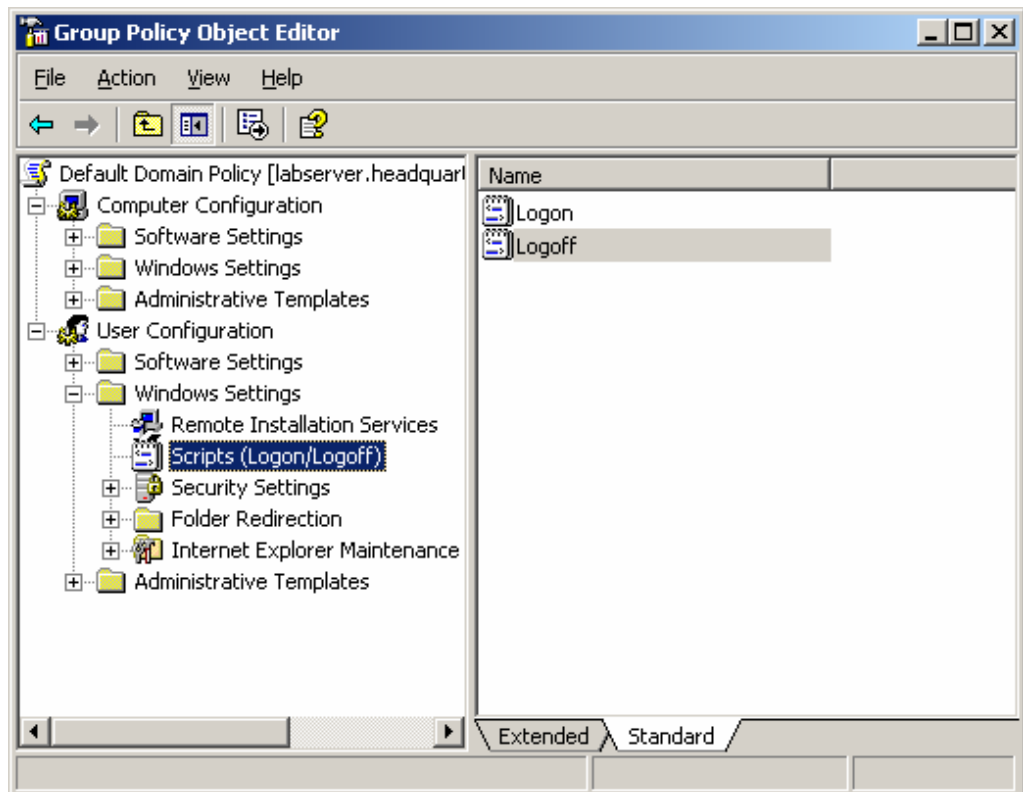


Figure 10.3 Group Policy allows the configuration of Logon and Logoff scripts for users

User Restrictions for Unrestricted Domain Accounts

Some organizations need to restrict domain accounts on specific computers, but these domain accounts are unrestricted by Group Policy. This often happens with shared facilities that are used briefly by domain users, such as media burning labs or other types of dedicated computer kiosks.

Similarly, operators may need to restrict domain accounts on specific computers but do not have the access rights to make the required changes within Group Policy to do so.

Other security conscious environments would like to ensure that default restrictions are applied to domain users even if network issues prevent Group Policy restrictions from being applied at an initial logon (usually caused by tampering, such as the well-timed removal of a network cable).

All of these scenarios can be addressed by using the User Restrictions tool to apply restrictions to the Default User profile on a computer. The Default User profile is used as a template when creating all new user profiles for both domain and local accounts. This particular technique does not work on domain accounts that are configured with roaming user profiles



Important

Before you customize the Default User profile, create a backup of it in case of problems. To do this, make a copy of the Default User folder located in the Documents and Settings folder.



Note

If you copy the Default User folder to the NETLOGON share on a domain controller, all domain users will receive the settings and restrictions of this profile the first time they log on.

The folder will be replicated to all other domain controllers providing a Default User profile for all new domain accounts.

To create a custom Default User profile

1. Log on as the Toolkit administrator.
2. Create a new limited local user account.
3. Log off and then log on as the local user account that you just created.
4. Customize the profile. For example, you could:
 - ◆ Customize the Start menu.
 - ◆ Customize the desktop and taskbar.
 - ◆ Install and configure printers.
5. Log off and then log on as the Toolkit administrator.
6. Use the User Restrictions tool to configure and apply restrictions for the newly created profile.
7. Click **Start**, and then click **My Computer**.
8. Click the **Tools** menu, and then click **Folder Options**.
9. In the **Folder Options** dialog box, on the **View** tab, under **Advanced settings**, click **Show hidden files and folders**, and then click **OK**. Several of the files in the new profile are hidden by default, so hidden files must be shown to be copied to the new custom Default User profile.
10. Click **Start**, right-click **My Computer**, and then click **Properties**.
11. In the **System Properties** dialog box, on the **Advanced** tab, under **User Profiles**, click **Settings**.
12. In the **User Profiles** dialog box, click the user profile that you just created and customized, and then click **Copy To**.
13. In the **Copy To** dialog box, under **Copy profile to**, click **Browse**, click the C:\Documents and Settings\Default User folder, and then click **OK**.
14. Under **Permitted to use**, click **Change**, click **Everyone**, and then click **OK**. If **Everyone** is not available, click **Advanced**, click **Find Now**, click **Everyone**, and then click **OK**. Windows XP will now assign the custom Default User profile along with its restrictions to any new user who logs on to the computer.

This technique cannot be used to lock new user profiles as they are created. However, you can use this technique in conjunction with Windows Disk Protection to clear the new user profiles that are created on the Windows partition with each restart of the computer.

User Profiles in Other Languages

The Multilingual User Interface Pack (MUI) is a set of language-specific resource files that you can add to the English language version of Windows XP Professional. Using MUI, your users can change the interface language of the operating system to any of 33 supported languages. After you install the Toolkit, you can specify the user interface language for your users.

MUI Requirements

MUI will run on computers that run Windows XP Professional, but not on Windows XP Home Edition.

Windows XP MUI is sold only through Volume Licensing programs such as the Microsoft Open License Program (MOLP/Open), Select, and Enterprise agreement. You can request an OEM version of MUI, although MUI is not available through retail channels. This is to ensure that customers have the English version of the operating system running on their computers before they install MUI.

For more information about MUI and its requirements, see the [Windows Server 2003, Windows XP & Windows 2000 MUI](#) page.

How to Install MUI

MUI includes six CDs: one that contains the English version of Windows XP Professional, and the remaining five for the MUI Resource Files. After you use the first CD to install Windows XP Professional, you can run the program MUISetup.exe from any of the five resource CDs to install the User Interface Languages. You can install as many of the languages as necessary. You can also remove languages at any time.

How to Change the Input Language

After you install MUI, you can use the **Regional and Language Options** dialog box in Control Panel to define the standards and formats the computer uses, a user's location, and the input languages used by the user profile.

The input language configured for the computer tells Windows how to react when text is entered using the keyboard. With multiple languages configured, a user can toggle between languages as needed. You can add an input language in a user profile as long as you have installed the appropriate language from MUI.

To add an input language for a user profile

1. Log on as the user for which you want to add an input language.
2. Click **Start**, and then click **Control Panel**.
3. In Control Panel, double-click **Date, Time, Language, and Regional Options**.
4. In the **Date, Time, Language, and Regional Options** window, click **Regional and Language Options**.
5. In the **Regional and Language Options** window, on the **Languages** tab, in the **Text Services and Input Languages** section, click **Details**.
6. In the **Text Services and Input Languages** dialog box, click **Add**.

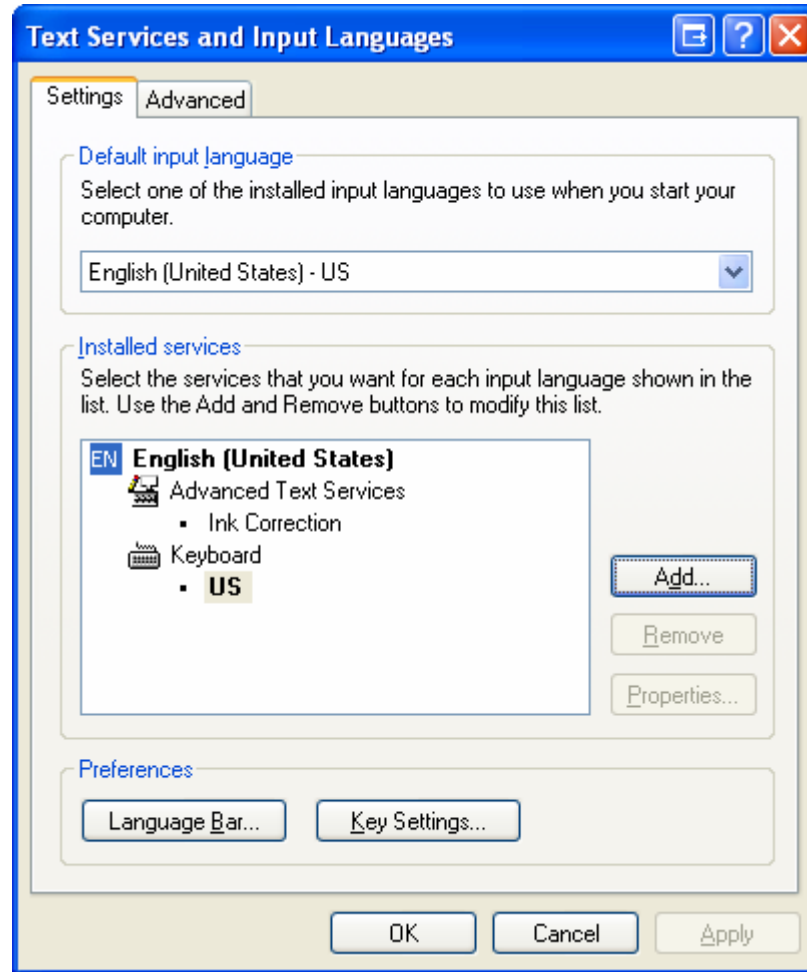


Figure 10.1 Add an input language for a user account

7. In the **Add Input Language** dialog box, click the language you want to add. To choose a specific keyboard layout, select the **Keyboard Layout/IME** check box and choose the appropriate layout. To add a keyboard layout or input method editor (IME), you need to have installed it on your computer first. Click **OK**.
8. In the **Text Services and Input Languages** dialog box, the **Default Input Language** drop-down list, click the language that should be the default language, and then click **OK**.



Appendix A: Technical Primer

To set up the Microsoft® Shared Computer Toolkit for Windows® XP and manage shared computers requires familiarity with a number of technologies and Windows features.

This appendix covers the following topics:

- User accounts and profiles
- How the Profile Manager tool works
- How the User Restrictions tool works
- Disks and partitions
- How the Windows Disk Protection tool works

User Accounts and Profiles

A user account is a collection of information that defines a user. This information includes the user name, password, groups to which the user belongs, basic environment settings that apply to the user, and other details about the user.

A user profile is a group of settings and files that defines the environment that Windows XP loads when a user logs on. The profile includes all the user-specific configuration settings, such as program items, screen colors, network connections, printer connections, mouse settings, and window size and position. A user profile also allows you to specify different programs, languages, and accessibility features for each user account.

A user profile consists of two parts:

- **A set of folders and files stored on the hard disk.** By default, these folders are stored in the Documents and Settings folder on the Windows partition. As the following figure illustrates, Windows creates a folder for each user profile in the Documents and Settings folder. A user folder is a container for programs and other operating system components to populate with subfolders and user-specific settings, such as shortcut links, desktop icons, startup programs, documents, configuration files, and so on. Windows Explorer uses the user profile folders extensively for special folders such as the user's desktop, Start menu and My Documents folder.
- **A registry data file.** The registry is a database used to store computer-specific and user-specific settings on a computer running Windows XP. Portions of the registry can be saved as files. Windows can then reload these files for use as necessary. User profiles take advantage of this feature to provide user profile functionality. The user profile registry file for each user is saved as a file named Ntuser.dat in the profile folder. The information in this file is mapped to the **HKEY_CURRENT_USER** portion of the registry whenever the user logs on. It stores those settings that maintain network connections, Control Panel configurations that are unique to the user (such as the desktop color and mouse settings), and program-specific settings.

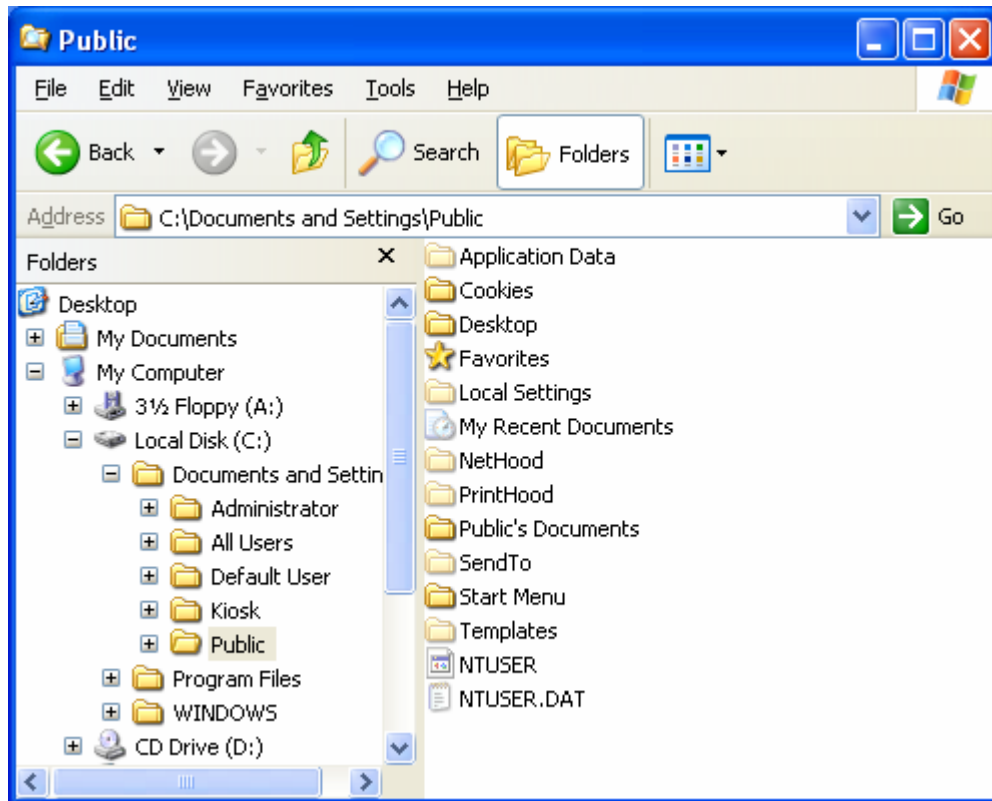


Figure A.1 A user profile is a collection of files and folders

User profiles can be stored on the local hard disk drive, or can be set so that the data roams with the user wherever he or she logs on. The following types of user profiles are available in Windows XP:

- **Local user profile.** Created the first time that a user logs on to a computer, the local user profile is stored on a computer's local hard disk. Any changes made to the local user profile are specific to the computer on which the changes are made.
- **Roaming user profile.** The local profile is copied to (and stored in) a network-accessible location. This profile is downloaded every time that a user logs on to any computer on the network, and any changes made to a roaming user profile are synchronized with the server copy upon logoff.
- **Mandatory user profile.** A type of profile that administrators can use to specify particular settings for users, a mandatory profile is essentially a roaming user profile to which a user cannot make permanent changes. Only system administrators can make changes to mandatory user profiles. Changes made by the user to desktop settings are lost when the user logs off. A mandatory user profile is often referred to as *stateless*, which just means that changes made in the session are not saved in the profile. This is useful on shared user accounts where one user should not be able to change the experience of other users. The **Lock this profile** option in the User Restrictions tool works by turning the user profile into a mandatory user profile (and thus, a roaming profile).
- **Temporary user profile.** A temporary profile is issued any time that an error prevents the user's default profile from being loaded. Temporary profiles are deleted at the end of each session— changes made by the user to desktop settings and files are lost when the user logs off.

How the Profile Manager Tool Works

Typically, a user profile is not created until the first time that a user logs on to the computer with a new user account. When this logon happens, Windows automatically creates a new user profile for that user account. The Profile Manager tool lets you create user profiles without logging on as the user and, more importantly, lets you create profiles on alternative hard disk partitions. You can also delete user profiles for existing user accounts. This includes the ability to delete profiles locked by User Restrictions (which are really mandatory user profiles).

When you create a profile using the Profile Manager tool, the tool simulates logging on with the user account so that it can create the user profile (though this simulation is completely transparent to the user). After creating the profile, if you specified that the profile be created on an alternative partition, the tool moves the profile to that partition.

How the User Restrictions Tool Works

Most of the restrictions available in the User Restrictions tool work by modifying the registry settings related to a user profile. Locking a profile in User Restrictions turns that profile into a mandatory profile that is stored within `/Documents and Settings/<user>.orig`.

You can view the exact list of restrictions applied to `HKEY_CURRENT_USER` for each restricted user profile by viewing the `Restrict.xml` file in the `Xml` subfolder of the Toolkit installation folder.

When the User Restrictions tool restricts a user, a copy of `Restrict.xml` is created called `User.<user>.xml` that contains the exact list of restrictions applied to that user profile. This file can be manually customized (with extreme care) and applied again using the `Restrict.wsf` command-line tool on other local profiles. To help advanced operators with this customization process, this appendix lists all of the registry settings contained in these `.xml` files and describes what they do.

Microsoft cannot support any customizations made to `Restrict.xml`, because it drives much of the user interface in the User Restrictions tool. It is strongly recommended and preferred that you customize a `User.<user>.xml` file and process it using the `Restrict.wsf` command-line tool. However, if you plan to change `Restrict.xml` despite these support implications, be sure to make a backup copy and do not modify the restrictions within the General Settings section, because it is the one section that is closely tied to hard-coded fields in the user interface of the User Restrictions tool (contained in `Restrict.hta`).


Disks and Partitions

A partition is a logical section of a hard disk on which Windows can write data. Every hard disk must be partitioned before it can be used. Often, a hard disk is set up as one big partition, but you can divide a hard disk into multiple partitions. When you partition a hard disk, you decide how much space to allocate to each partition.

For example, assume that your computer has an 80-GB hard disk. If you purchased your computer with Windows XP already installed, or if you installed Windows XP using the default choices during installation, the hard disk likely has a single partition that takes up all of the 80 GB on the disk. However, you could divide that same disk into multiple

partitions—maybe a 40-GB partition to hold Windows and program files, a 20-GB partition to hold your documents, and another 20-GB partition for future use.

When you partition a hard disk, you do not have to use all of the space on the hard disk at once. For example, on the 80-GB hard disk, you could create a single 40-GB partition and leave the rest of the space unpartitioned. Unpartitioned space on a hard disk is called *unallocated space*.

 **unallocated disk space**
Unused space on a hard disk that is not part of any partition.

Windows XP treats each partition on a hard disk as though it were a separate drive, assigning each partition a drive letter. Typically, the first partition (and the one that usually holds the Windows system files) is assigned drive letter C. This Handbook refers to the partition that holds the Windows files as the *Windows partition*. Other partitions are assigned drive letters as they are created, and the exact drive letters assigned depend on when the other partitions are created (during installation or afterward) and on what other drives you have on the computer (such as CD or DVD drives).

 **Windows partition**
The hard disk partition that holds Windows system files and programs.

Windows can recognize up to four *primary partitions*. To get around this limit, Windows allows you to create an *extended partition* (in place of one of the four primary partitions) that acts as a shell in which you can install any number of *logical partitions*. Windows Disk Protection reduces the limit on primary partitions to three, plus the requirement for unallocated space.

Windows XP supports two types of disk storage. The first, called *basic storage*, uses partitions to allocate storage space to Windows. This is the type of storage discussed throughout this Handbook. Another type, called *dynamic storage*, offers more storage flexibility. Dynamic storage breaks the limits of four partitions per disk and allows for more flexible use of disk space. Server versions of Windows can even use dynamic storage volumes to create fault tolerant disk arrays for storage reliability.

Windows Disk Protection is designed to support basic storage only. Computers that use dynamic storage will fail Step 1 in Getting Started, and cannot turn on Windows Disk Protection.

How the Windows Disk Protection Tool Works

The Windows Disk Protection tool is designed to protect the Windows partition by rejecting all changes made to that partition since the last restart. Examples of changes include modifications to Windows configuration settings, installation of programs (including viruses and spyware), or even simple changes to the desktop environment.

 **protection partition**
The partition that Windows Disk Protection uses to safeguard the computer from changes that you have not authorized.

The Protection Partition

To achieve this protection, the Windows Disk Protection tool creates a special partition using unallocated disk space on your hard disk. This special partition is called the *protection partition*. The tool saves changes made during the user session to that special partition, making it appear to the user as though everything is operating ordinarily. Depending on how the Windows Disk Protection tool is configured, the tool can discard changes made within the protection partition when a user session finishes or save those changes to the Windows partition.

The Critical Updates Process

When Windows Disk Protection is turned on, it disables the Automatic Updates client in Windows XP, which is usually accessed through Control Panel. Any schedule set through Automatic Updates will have no effect on the computer while Windows Disk Protection is on. After you turn on Windows Disk Protection, critical updates schedule changes must be made in the **Critical Updates** section of the Windows Disk Protection tool.

If you want to change the schedule for critical updates, set Windows Disk Protection to use the **Save changes with next restart** restart option, make the appropriate changes, and then restart the computer.

After you turn on Windows Disk Protection, you will find three tasks in your system's Scheduled Tasks folder. These tasks, typically named At1, At2, and At3, are set to run one after the other based on the schedule you selected in the Windows Disk Protection tool.

- **At1** displays a banner message at five minutes before the scheduled hour to inform any interactive user that they will be logged off automatically in 60 seconds for maintenance, after which the computer restarts. This restart clears any potentially untrustworthy changes made to the Windows partition through the default behavior of Windows Disk Protection.
- **At2** displays the same message one minute before the scheduled hour. Any interactive user is then logged off and all local user accounts are disabled except the Toolkit administrator and the Windows XP Professional administrator account. Domain accounts are not disabled.
- **At3** occurs at the scheduled hour and runs the actual critical updates script. This script downloads and installs Microsoft critical updates, starts the identified antivirus script and other script if they have been configured through the Windows Disk Protection tool. It then enables the accounts previously disabled, sets the Windows Disk Protection restart option to **Save changes with next restart**, and restarts the computer. After the restart, Windows Disk Protection resets the restart option to the default: **Clear changes with each restart**.

To allow for other updates you might have scheduled to occur at the same time as Windows Disk Protection critical updates, the At3 task described above will wait for a minimum of 10 minutes before restarting the computer. This delay can be increased by changing the number of minutes in the following registry key (set to 10 by default):

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Computer Toolkit\CriticalUpdatesMins

While the Windows Disk Protection critical updates process downloads and installs updates, it is important that neither you nor any domain accounts use the computer— so that unwanted disk changes are not saved along with the critical updates.

For this reason, schedule the critical updates process to occur during the lightest user demand period of the day in the environment that you manage. If you manage computers that operate 24 hours a day, consider staggering the critical updates schedule among the computers so that some computers are always available to users.

Acknowledgements

Microsoft Solutions for Security and Compliance (MSSC) would like to acknowledge and thank the people responsible for the Microsoft Shared Computer Toolkit for Windows XP.

Developers

José Maldonado, MSSC

Gareth Jones, MSSC

Rajendran Ganapathy, Infosys Technologies

Sivaraman Kothandaraman, Infosys
Technologies

Testers

Gaurav Singh Bora, Infosys Technologies

Amol Choudhari, Infosys Technologies

Archita Dash, Infosys Technologies

Arjun Radhakrishanan, Infosys
Technologies

Harsha Sanagaram, Infosys Technologies

Writers and Editors

John Cobb, Volt

Walter Glenn, Studio B

Dave Field, Studio B

Jennifer Kerns, Wadeware

Program and Product Management

Derick Campbell, MSSC

John Eversole, Windows Client Marketing

Links

Shared Computer Toolkit Web Pages

Shared Computer Toolkit Home Page

<http://go.microsoft.com/fwlink/?LinkId=46755>

Shared Computer Toolkit Download

<http://go.microsoft.com/fwlink/?LinkId=47025>

Shared Computer Toolkit Updates Download

<http://go.microsoft.com/fwlink/?LinkId=47035>

Shared Computer Toolkit Frequently Asked Questions

<http://go.microsoft.com/fwlink/?LinkId=47836>

Shared Computer Toolkit Registration

<http://go.microsoft.com/fwlink/?LinkId=40009>

Shared Access Online Resources and Community

<http://go.microsoft.com/fwlink/?LinkId=39998>

Microsoft Web Sites

Windows Server 2003 Active Directory

<http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.aspx>

Windows XP Service Pack 2 (SP2)

<http://www.microsoft.com/windowsxp/sp2/default.aspx>

Windows Genuine Advantage

<http://www.microsoft.com/genuine>

Microsoft User Profile Hive Cleanup Service (UPHClean) download page

<http://go.microsoft.com/fwlink/?LinkId=27031>

Microsoft Protect Your PC Web site

<http://www.microsoft.com/protect>

Windows Update

<http://update.microsoft.com/windowsupdate>

Microsoft Update

<http://update.microsoft.com/microsoftupdate>

Windows Server Update Services

<http://www.microsoft.com/windowsserversystem/updateservices/evaluation/previous/default.aspx>

About Genuine Microsoft Software

<http://www.microsoft.com/genuine/downloads/whyValidate.aspx>

Windows Marketplace (Content Filtering)

<http://www.windowsmarketplace.com/results.aspx?bcatid=331>

Windows Marketplace (Drive Copy)

<http://www.windowsmarketplace.com/results.aspx?bcatid=391>

Online Resources for Using Public Computers

<http://go.microsoft.com/fwlink/?LinkId=39997>

Windows XP Resource Kit (Automating and Customizing Installations)

http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prbc_cai_nmip.asp

Windows XP Resource Kit (Using Sysprep to Deploy Windows XP)

http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prbc_cai_vnve.asp

Multilingual User Interface Pack (MUI)

<http://www.microsoft.com/globaldev/DrIntl/faqs/muifaq.msp>

Using Software Restriction Policies to Protect Against Unauthorized Software

<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.msp>

Third-Party Tools and Resources

Adobe Acrobat Reader

<http://www.adobe.com/products/acrobat/readstep2.html>

Symantec Norton PartitionMagic 8.0

<http://go.microsoft.com/fwlink/?LinkId=47542>

TeraByte BootIt NG

<http://go.microsoft.com/fwlink/?LinkId=46756>

Computer Associates eTrust 7.0

<http://www3.ca.com/Solutions/Product.asp?ID=156>

McAfee

<http://www.mcafee.com>

Symantec Norton Ghost 9.0

http://www.symantec.com/sabu/ghost/ghost_personal/

Acronis TrueImage 8.0

<http://www.acronis.com/enterprise/products/ATICW/>

WebSense

<http://www.websense.com/>

Secure Computing

<http://www.securecomputing.com/>

Faronics

<http://www.faronics.com>

Fortres Grand

<http://www.fortres.com>

Helpful Articles

Microsoft Knowledgebase Article 307881, *How to convert a FAT16 volume or a FAT32 volume to an NTFS file system in Windows XP*

<http://support.microsoft.com/kb/307881>

Windows XP - Advantages of using NTFS

http://www.microsoft.com/resources/documentation/windows/xp/all/reskit/en-us/prkc_fil_duwx.asp

Automating and Customizing Installations

http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prbc_cai_nmip.asp

Certain Programs Do Not Work Correctly If You Log On Using a Limited User Account

<http://support.microsoft.com/kb/307091>

TechNet Imaging Web site

<http://www.microsoft.com/technet/desktopdeployment/imaging/imagingsysprep.mspx>

Customizing Sysprep Installations

http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/prbc_cai_oziz.asp

Description of Microsoft Product Activation

<http://support.microsoft.com/default.aspx?scid=kb;en-us;302806>

User Profiles Overview

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/userprofile_overview.mspx

How To Assign a Mandatory User Profile in Windows XP

<http://support.microsoft.com/KB/307800>

Using Software Restriction Policies to Protect Against Unauthorized Software

<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx>

Index

—A—

access control list (ACL), 18
accessibility, 8, 12, 93
activation, 79
Active Directory, 8, 9, 10, 27, 81, 82, 84, 85, 86, 101
administrative account, 8, 16, 17, 28, 30, 31, 34, 42, 56, 59, 62, 66, 67, 71
administrator, 8, 16, 17, 18, 19, 21, 24, 28, 33, 39, 42, 47, 48, 49, 55, 56, 59, 61, 64, 68, 69, 70, 71, 72, 73, 89, 97
antivirus software, 45, 48, 55, 58
audience, 7
authentication, 8
AutoLogon tool, 8, 20
Automatic Updates, 47, 97
AutoPlay, 37
AutoRestart tool, 8, 19, 29, 60

—B—

BIOS, 55, 57

—C—

CD-ROM, 17, 23, 24, 57
children, 12, 27, 43, 67, 74, 75
classic Start menu, 30, 56
clear changes, 10, 46, 48, 49, 69, 82, 97
command prompt, 23, 37, 38, 88
community, 7, 12
content filtering, 73
Control Panel, 8, 19, 35, 36, 37, 47, 84, 86, 90, 93, 97
critical updates, 8, 16, 17, 19, 45, 47, 48, 50, 55, 57, 58, 64, 82, 83, 97

—D—

desktop, 7, 10, 28, 29, 35, 38, 41, 42, 43, 44, 56, 75, 87, 89, 93, 94, 96
Disk Management utility, 21, 22, 25, 52, 65, 67, 68
domain, 9, 10, 18, 27, 81, 82, 83, 84, 86, 87, 88, 89, 97
Dynamic Link Library (DLL), 66

—E—

extended partition, 21, 52, 96

—F—

FAT32, 15, 103
favorites, 35, 36
firewall, 55, 58

—G—

games, 28, 38, 63, 71, 74, 75
 Call of Duty, 38, 63
 Halo, 38, 63
Getting Started, 8, 9, 16, 17, 19, 20, 21, 22, 28, 33, 47, 48, 56, 60, 65, 66, 96
group, 93
Group Policy, 8, 9, 10, 81, 84, 85, 86, 87, 88
 SCTSettings.adm template, 81, 84, 85, 87

—H—

help, 9, 10, 11, 12, 13, 17, 19, 37, 38, 39, 57, 58, 59, 71, 74, 95
hibernation, 46, 47, 64
home page, 29, 33, 34, 63

—I—

independent software vendor (ISV)
 Acronis, 77, 78, 102
 Adobe, 16, 29, 102
 Computer Associates, 47, 102
 Faronics, 102
 Fortres Grand, 102
 McAfee, 47, 83, 102
 Symantec, 23, 77, 78, 102
 TeraByte Unlimited, 23, 102
installation, 9, 12, 15, 16, 17, 20, 24, 25, 50, 55, 60, 62, 64, 66, 70, 72, 73, 77, 79, 83, 84, 95, 96
Internet Explorer, 18, 29, 33, 34, 37, 38, 39, 42, 58, 63, 67, 72, 73, 74, 75
Internet Information Services (IIS), 16

—L—

limited user account, 19, 27, 28, 55, 62, 71, 77
 lock, 10, 19, 29, 33, 34, 35, 37, 42, 55, 57, 61,
 63, 71, 74, 75, 76, 89, 94
 logon, 61, 88

—M—

malware, 45, 46
 Microsoft Management Console (MMC), 37
 Microsoft Office, 18, 28, 33, 38, 39, 63, 72, 75,
 87
 Microsoft Passport, 18
 Microsoft Update, 16, 30, 46, 47, 48, 57, 83, 101
 MSN Messenger, 29, 39, 87
 Multilingual User Interface (MUI), 89, 90, 102
 My Computer, 22, 29, 31, 34, 35, 39, 50, 61, 76,
 89
 My Documents, 36, 37, 61, 69, 70, 74, 75, 93
 My Pictures, 36

—N—

NTFS, 15, 25, 103

—P—

partition, 10, 11, 21, 22, 23, 24, 25, 45, 46, 50,
 52, 53, 64, 65, 67, 68, 75, 95, 96
 password, 57, 68
 persistent partition, 25, 49, 50, 51, 62, 65, 67,
 68, 69, 74, 75, 83, 84
 physical security, 56
 printer, 19, 29, 36, 37, 89, 93
 profile management, 10, 17, 24, 27, 61, 70, 78
 Profile Manager tool, 8, 10, 20, 28, 61, 62, 67, 68,
 69, 84, 93, 95
 Program Files, 15, 38, 39, 62, 63, 66, 75, 83, 85,
 87
 protection partition, 21, 22, 45, 46, 49, 50, 52,
 53, 64, 65, 67, 96
 proxy, 33, 34, 39, 72, 73

—R—

Recycle Bin, 37
 registration, 16, 17
 registry, 29, 38, 48, 51, 53, 60, 66, 93, 95, 97
 restart, 8, 10, 19, 21, 24, 35, 37, 43, 45, 46, 47,
 48, 49, 50, 51, 61, 62, 63, 64, 65, 69, 70, 72,
 73, 82, 83, 88, 89, 96, 97
 retain changes, 45, 49, 65, 70, 82, 83

—S—

Scripts, 16, 17, 29, 39, 45, 47, 58, 60, 72, 83, 88
 search, 16, 36, 37, 38, 73
 Setup, 24, 55, 78, 79, 84
 software requirements, 15
 Software Restriction Policies, 66, 85, 86, 87, 102,
 103
 software restriction policy, 66, 85, 86, 87, 102,
 103
 Software Update Services (SUS), 47
 spyware, 7, 45, 58, 96
 Start menu, 8, 10, 12, 15, 18, 27, 29, 30, 31, 33,
 34, 35, 36, 37, 38, 39, 41, 42, 43, 48, 56, 59,
 61, 62, 67, 70, 71, 74, 75, 84, 86, 87, 89, 93
 style conventions, 11
 Supported Environments, 9

—T—

Task Manager, 37, 66
 Technical Primer, 11, 21, 28, 47, 93
 teenager, 75
 time restrictions, 35, 74, 75
 troubleshooting, 10, 13, 16, 58, 59

—U—

unallocated disk space, 10, 21, 22, 23, 24, 25,
 49, 52, 53, 64, 65, 67, 68, 96
 USB drive, 33, 37, 38, 57, 67, 69
 user profile, 8, 10, 15, 17, 18, 19, 20, 27, 28, 29,
 30, 31, 33, 34, 35, 41, 42, 45, 48, 59, 60, 61,
 62, 63, 65, 67, 68, 69, 70, 73, 74, 75, 76, 77,
 78, 83, 84, 89, 90, 93, 94, 95, 101, 103
 All Users, 30, 43, 62, 67, 70, 84
 Default User, 89
 local, 8, 27, 28, 33, 81, 83, 94
 mandatory, 76, 77, 94, 95
 persistent, 67, 68
 roaming, 89, 94
 User Profile Hive Cleanup Service (UPHClean), 59,
 87, 101
 User Restrictions tool, 8, 9, 10, 18, 19, 20, 28, 29,
 30, 33, 34, 36, 38, 42, 59, 61, 62, 63, 67, 69,
 70, 71, 72, 73, 74, 75, 78, 81, 84, 85, 87, 88,
 89, 93, 94, 95

—V—

virus, 7, 45, 58, 96

—W—

- Welcome screen, 8, 18, 55, 56, 61, 70
- Windows Disk Protection tool, 8, 9, 10, 17, 19, 20, 21, 22, 23, 24, 25, 35, 41, 43, 45, 46, 47, 48, 49, 50, 51, 52, 53, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 77, 78, 79, 81, 82, 83, 84, 89, 93, 96, 97
- Windows Explorer, 29, 30, 31, 34, 37, 39, 42, 61, 70, 93
- Windows Genuine Advantage (WGA), 9, 12, 15, 16, 17, 59, 66, 79, 101
 - validation, 12, 15, 17, 59, 66, 79
- Windows Messenger, 39, 74, 75, 87
- Windows partition, 8, 15, 21, 22, 23, 24, 34, 45, 46, 48, 49, 50, 51, 63, 64, 65, 67, 68, 74, 75, 82, 83, 84, 89, 93, 96, 97
- Windows Update, 30, 47, 101
- Windows XP Setup, 10, 21, 24, 25
- workgroup, 9, 27, 28, 81