

Microsoft® Shared Computer Toolkit for Windows® XP

The right way to share Windows



Bob McCoy
Microsoft Services

www.microsoft.com/sharedaccess

Disclaimer

This information relates to a pre-release software product, which may be substantially modified before its first commercial release.

Accordingly, the information may not accurately describe or reflect the software product when first commercially released.

This information is provided for informational purposes only, and Microsoft makes no warranties, express or implied, with respect to this document or the information contained in it.

Agenda

- Shared Computer Defined
- Shared Computer Challenges
- Toolkit at a Glance
- Ideal Customers
- System Requirements and Recommendations
- Security Threats and Attack Vectors
- The Tools
- The Handbook
- Benefits Summary
- Call To Action

Shared Computer Defined

- Any computer that is primarily intended to be used by more than one person

Sometimes referred to as public or community access



Our Focus

Non-focus

Untrusted, often unknown users

At work

At home

At school

Around town

On the road

- Universities
- Community colleges
- K-12 Schools

- Public libraries
- Internet Cafes
- Rural kiosks
- Community centers

- Airports
- Hotels
- Business Conferences

Shared Computer Challenges

For Users

- Personal privacy
- Safety and security
- Windows is optimized for personal use:
 - Remembers passwords
 - Tracks Internet History and Favorites
 - Auto-fills frequently used fields
 - Remembers recently used docs
- One user can easily compromise the experience of another by:
 - Changing computer settings
 - Infecting a computer with spyware or viruses
 - Viewing or stealing personal information

For Operators

- Protecting shared computers from untrustworthy users and malware:
 - Changing computer settings
 - Spyware and viruses
 - Unauthorized software
- Troubleshooting broken shared computers
- Finding inexpensive and easy-to-use software management tools
- Managing frequent software updates
- Finding time to learn how to properly manage shared computers

The Microsoft Shared Computer Toolkit for Windows XP - At a Glance

Windows Disk Protection

- Prevent unapproved changes to the Windows partition
- Allow critical updates and antivirus updates

Windows Restrictions

- Restrict untrusted users from files and settings
- Lock user profiles for protection and privacy

User Profiles

- Create “persistent” user profiles on unprotected partitions
- Delete locked user profiles

Accessibility

- Accessibility settings & utilities when restricted
- Quick access for repeat use

Getting Started

- Use and learn about the Toolkit
- Quick access toolbar

Tools are scriptable. Additional command-line tools included.
Comprehensive Help and Handbook with supplemental security guidance.

Ideal Customers

Organizations

- K-12 schools
- Colleges and universities
- Libraries
- Community technology centers
- Internet and gaming cafes
- Owners of Internet kiosks

Not Ideal

- “Enterprise” customers, employee computers, servers
- Consumers looking for parental controls
- Special purpose kiosks

People / Roles

Depending on the size of the org.:

- Technology Coordinators
- Teachers and Librarians
- Volunteers
- IT Managers
- Network or System Engineers

Environments

- Workgroup or standalone computers
 - All tools
- Domain-joined computers
 - Some tools

System Requirements

- Windows XP SP2: Home, Professional, and Tablet Editions
- Hard disk must have unallocated disk space for Windows Disk Protection (1024 MB or greater)
 - Two options for creating unallocated space
 - Resize existing partition using 3rd party tool
 - Reinstall Windows and size disk appropriately
- Optional: a second partition (D: drive) for persistent data and settings

Software Recommendations

- Computer must be “trustworthy”
 - Latest Microsoft Updates
 - Antivirus updates
 - Antispyware updates
 - Software required by your customers should be pre-installed
 - Uninstall unnecessary Windows components, applications, shareware, tools, etc.
 - They may introduce “attack vectors”

Security Threats and Attack Vectors

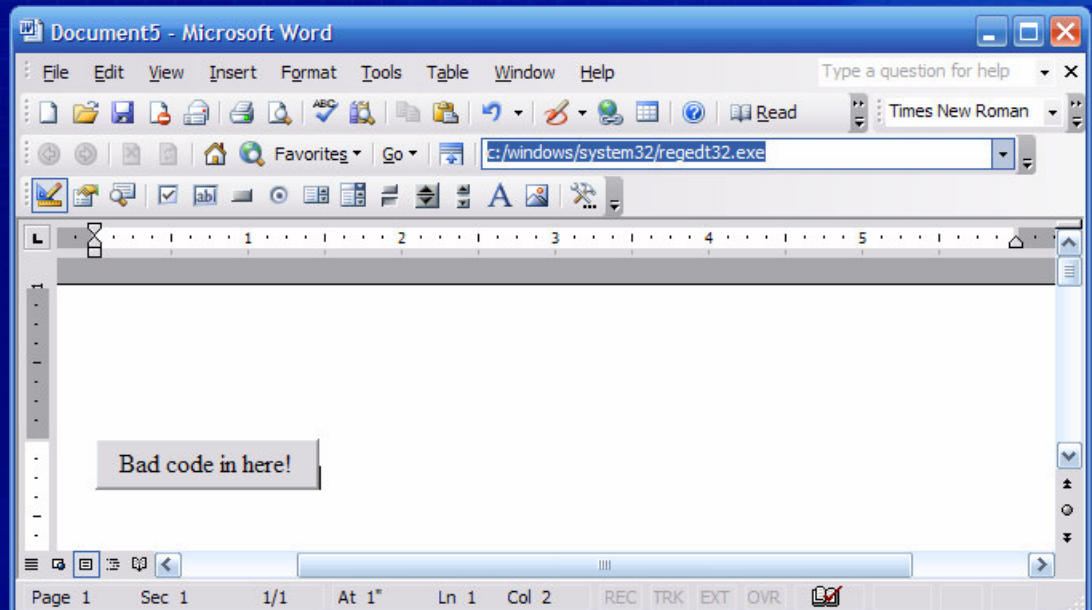
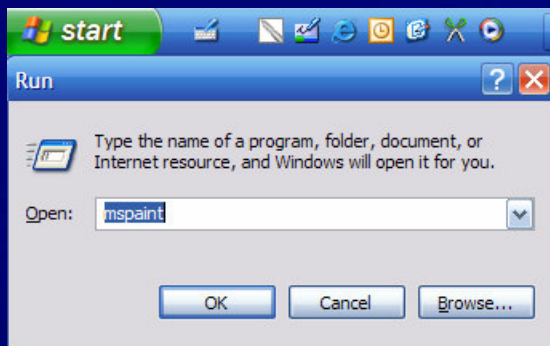
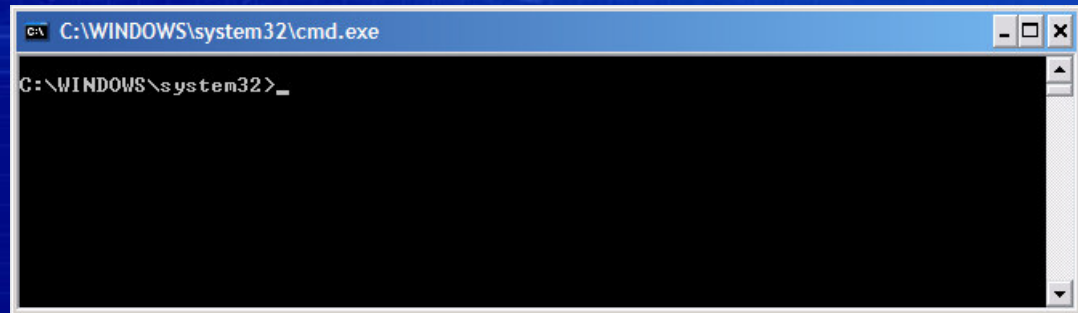
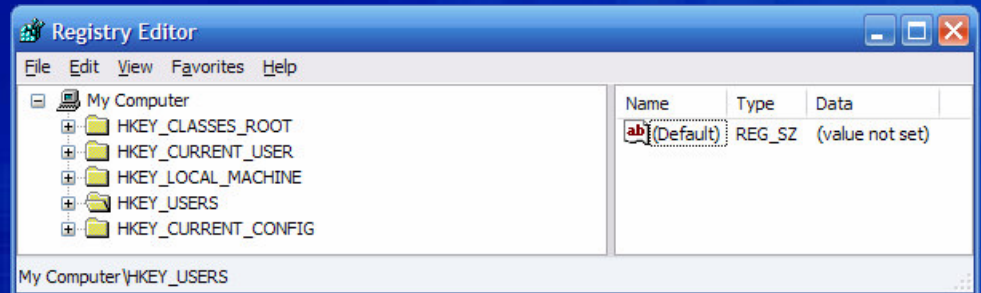
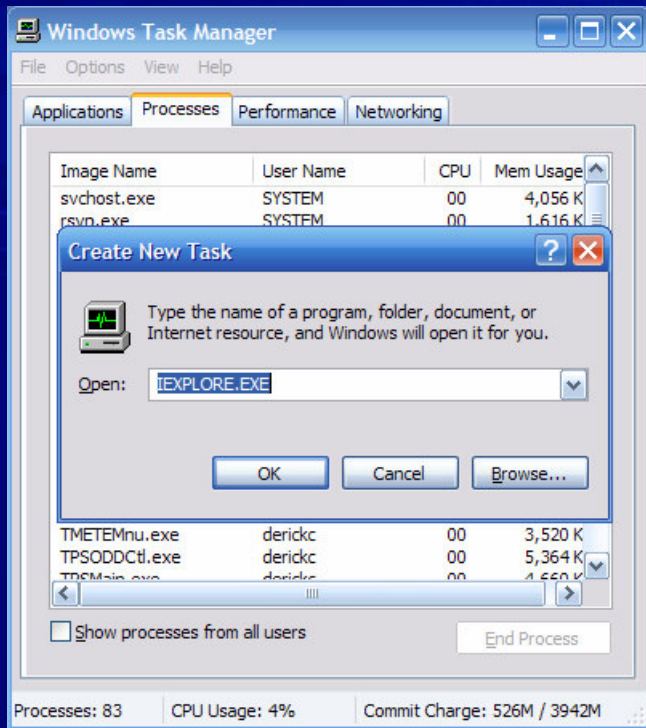
Threats

- Accidents
- “Just for fun” hackers
- Malware and spyware
- Rootkits
- Vandals
- Stalkers, predators, and spies

Attack Vectors


- Windows is flexible
 - Too flexible for the shared computer environment
- Command-line access
- Scripts and macros
- Starting & stopping processes
- Editing the registry
- Privilege escalation
- Every application offers new possibilities

Attack Vectors



Getting Started


Getting Started

Show Getting Started at Startup  Print This Page (recommended)

Getting Started with the Shared Computer Toolkit

Welcome to the Microsoft Shared Computer Toolkit for Windows XP. Getting Started provides a quick and easy way to use the Toolkit and learn about its basic functionality.

Quick access to useful utilities, tools, and resources:



Expand All Steps

- Step 1. Prepare the Disk for Windows Disk Protection ↓
- Step 2. Select Computer Security Settings ↓
- Step 3. Create a Public Account for Shared Access ↓
- Step 4. Configure the Public User Profile ↓
- Step 5. Restrict and Lock the Public User Profile ↓
- Step 6. Test the Public User Profile ↓
- Step 7. Turn on Windows Disk Protection ↓
- Step 8. You're Done! Learn More About the Toolkit ↓

Preparing the Disk

Step 1. Prepare the Disk for Windows Disk Protection

Important: The prerequisites for Windows Disk Protection have not been completed.

Review Chapter 2: "Prepare the Disk for Windows Disk Protection" in the Handbook, which describes how to use [Norton PartitionMagic 8.0](#) to create unallocated disk space for use by Windows Disk Protection.

Alternatively, you could use another disk partitioning product such as [TeraByte Unlimited BootIt Next Generation](#), which is available as a fully-working trial download with instructions on the TeraByte Unlimited Web site.

Note: In this step you need to reduce the size of the Windows partition to leave at least 1024 MB or 10% of the disk (whichever is greater) as unallocated disk space *after* the Windows partition.

If you cannot prepare the disk as described, you can still use the other tools in the Toolkit.



Open the Handbook

Use the Disk Management utility in Windows XP to view the current disk configuration and compare it to the recommended configuration described in the Handbook.



Open Disk Management

Example Disk Partitioning

The screenshot shows the Windows Disk Management console. At the top, a table lists the available volumes:

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
Windows Partition (...)	Partition	Basic	NTFS	Healthy (S...)	36.00 GB	28.43 GB	64 %

Below the table, the details for **Disk 0** are shown. It is a Basic disk with a total capacity of 40.00 GB and is Online. The disk layout consists of a single partition: **Windows Partition (C:)**, which is 36.00 GB in size, uses the NTFS file system, and is Healthy (System). The remaining 4.00 GB of the disk is Unallocated. A legend at the bottom indicates that black represents Unallocated space and blue represents a Primary partition.

The screenshot shows the Windows Disk Management console with a different disk configuration. The table at the top lists the volumes:

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
Data (D:)	Partition	Basic	NTFS	Healthy	23.00 GB	18.58 GB	80 %	No	0%
Windows XP (C:)	Partition	Basic	NTFS	Healthy (System)	30.00 GB	21.94 GB	73 %	No	0%

The details for **Disk 0** show a Basic disk with a total capacity of 55.88 GB and Online status. The disk layout includes three partitions: **Windows XP (C:)** (30.00 GB NTFS, Healthy System), **Data (D:)** (23.00 GB NTFS, Healthy), and a 2.89 GB Unallocated space. A legend at the bottom indicates that black represents Unallocated space and blue represents a Primary partition.

Computer Security Settings

Step 2. Select Computer Security Settings

The Windows Restrictions tool applies restrictions on a per-user basis. The following security settings, on the other hand, are applied to everyone who uses this computer. It is highly recommended that you check all of these computer security settings on shared computers:

- Prevent account names from being saved in the CTRL+ALT+DEL logon dialog.
- Prevent Windows from caching Passport or domain credentials within user profiles.
- Prevent logon to locked (or roaming) user profiles that can not be found to improve security.
- Remove cached copies of locked (or roaming) user profiles to improve privacy and save disk space.
- Remove the **Shut Down** and **Turn Off Computer** logon options.
- Use the Welcome screen.
- Remove **Admin** from the Welcome screen. **Important:** Press CTRL+ALT+DEL twice to log on to accounts not listed in the Welcome screen.

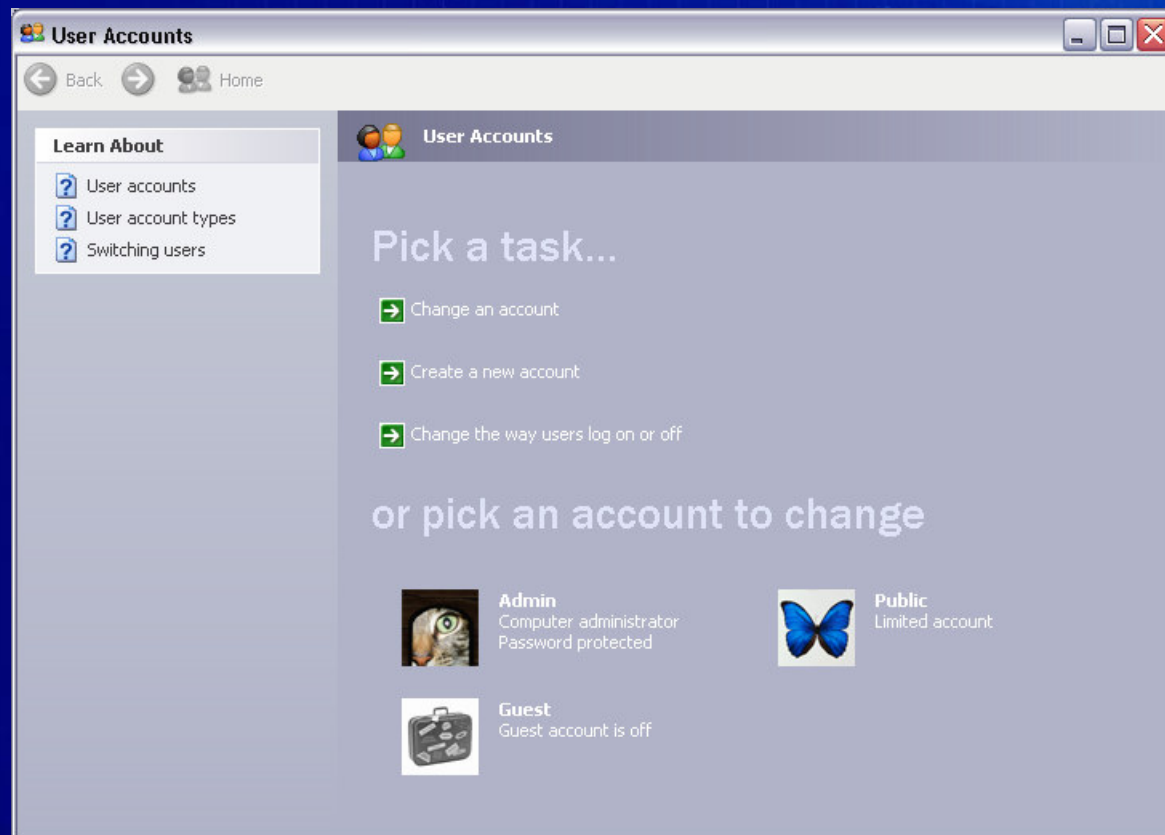
Note: Many of these check boxes take effect immediately, while some require a restart to take effect.

Create a Public Account

Step 3. Create a Public Account for Shared Access

Click **Open User Accounts**, create a local limited user account called **Public** (or a name you prefer), and then close User Accounts.

 **Open User Accounts**



Configure the Public User Profile

Step 4. Configure the Public User Profile

Click **Log off now** and log on as the Public account to do the following:

- Set the desktop wallpaper and other Windows preferences.
- Add and configure one or more printers.
- Configure first time settings and accept license agreements for programs such as Windows Media Player and Microsoft Office.

Important: If this last step is not performed, each user will be asked to complete the same initial steps each time they log on (after you use the Windows Restrictions tool to lock the profile).



Log off now

When finished, log on as the Toolkit administrator and then return here (**Getting Started**) to complete the remaining steps.

User Accounts vs. User Profiles

User Accounts

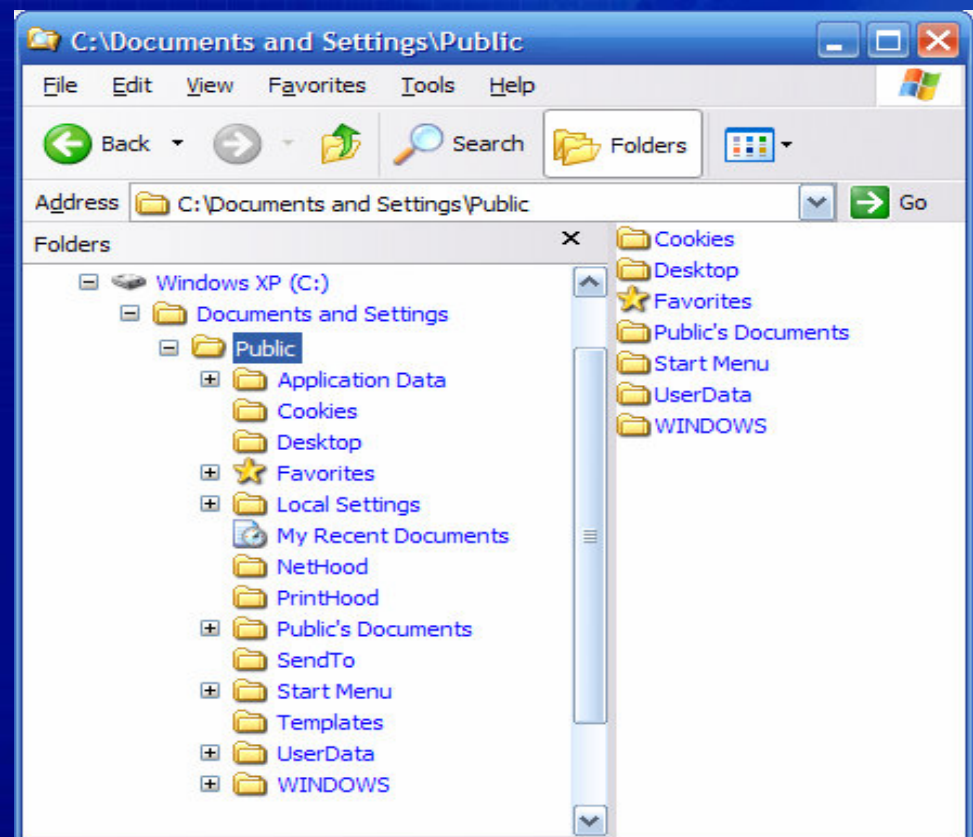
- Local directory
 - User names + passwords
- Accessed by Control Panel
- Used by logon process

Tips

- Accounts and Profiles are distinct, yet related
- User Profile is created with first logon

User Profiles

- User files and settings
- Stored on disk



Restrict & Lock the Public User Profile

Step 5. Restrict and Lock the Public User Profile

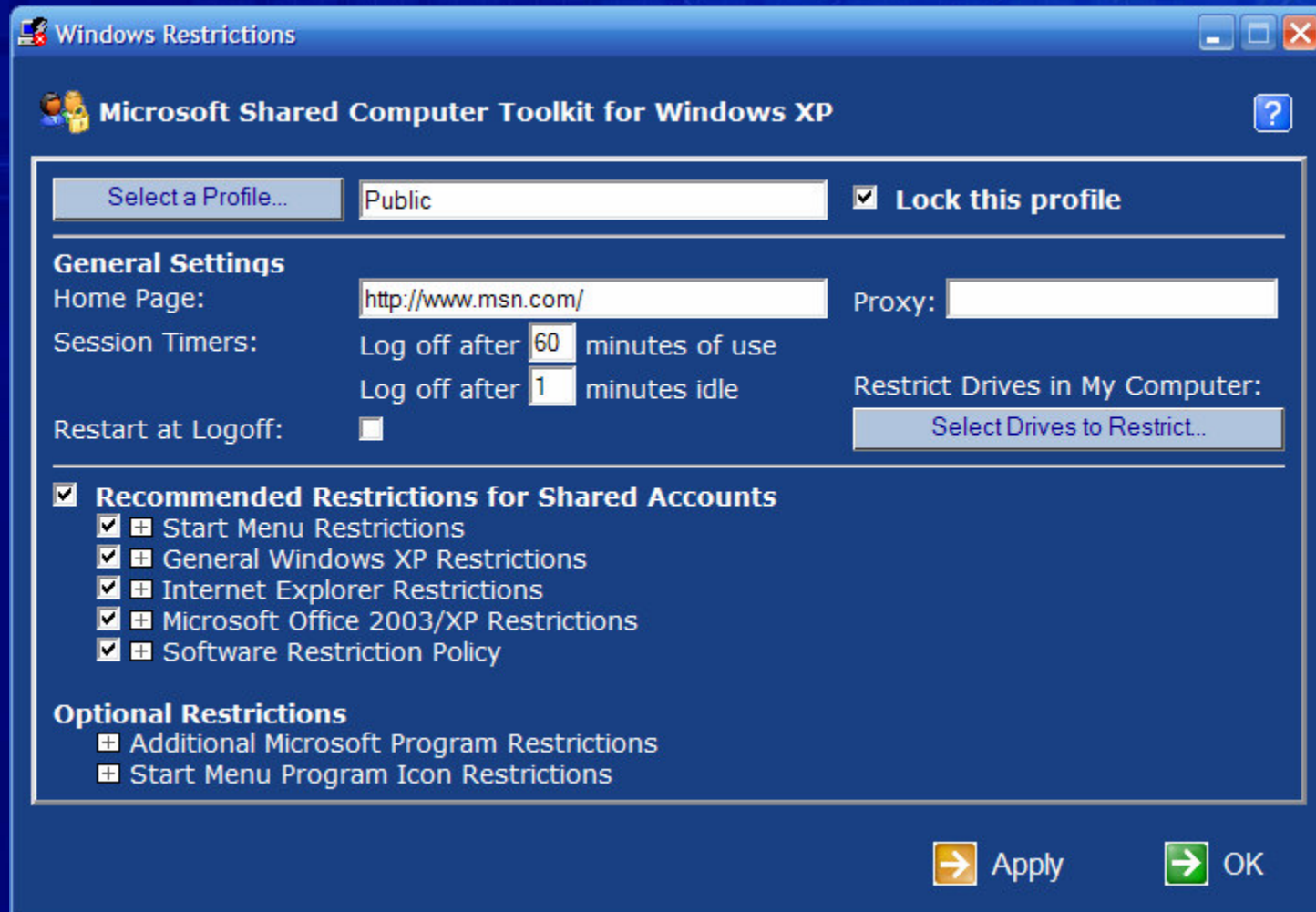
Click **Open Windows Restrictions**, select the Public user profile and:

- Select the **Lock this profile** check box to prevent user changes and Internet history from being saved.
- Select the **Recommended Restrictions for Shared Accounts** check box to make the account more secure for shared access.
- Configure the **General Settings** as you feel appropriate.
- Click **OK** to apply the restrictions and close the tool.

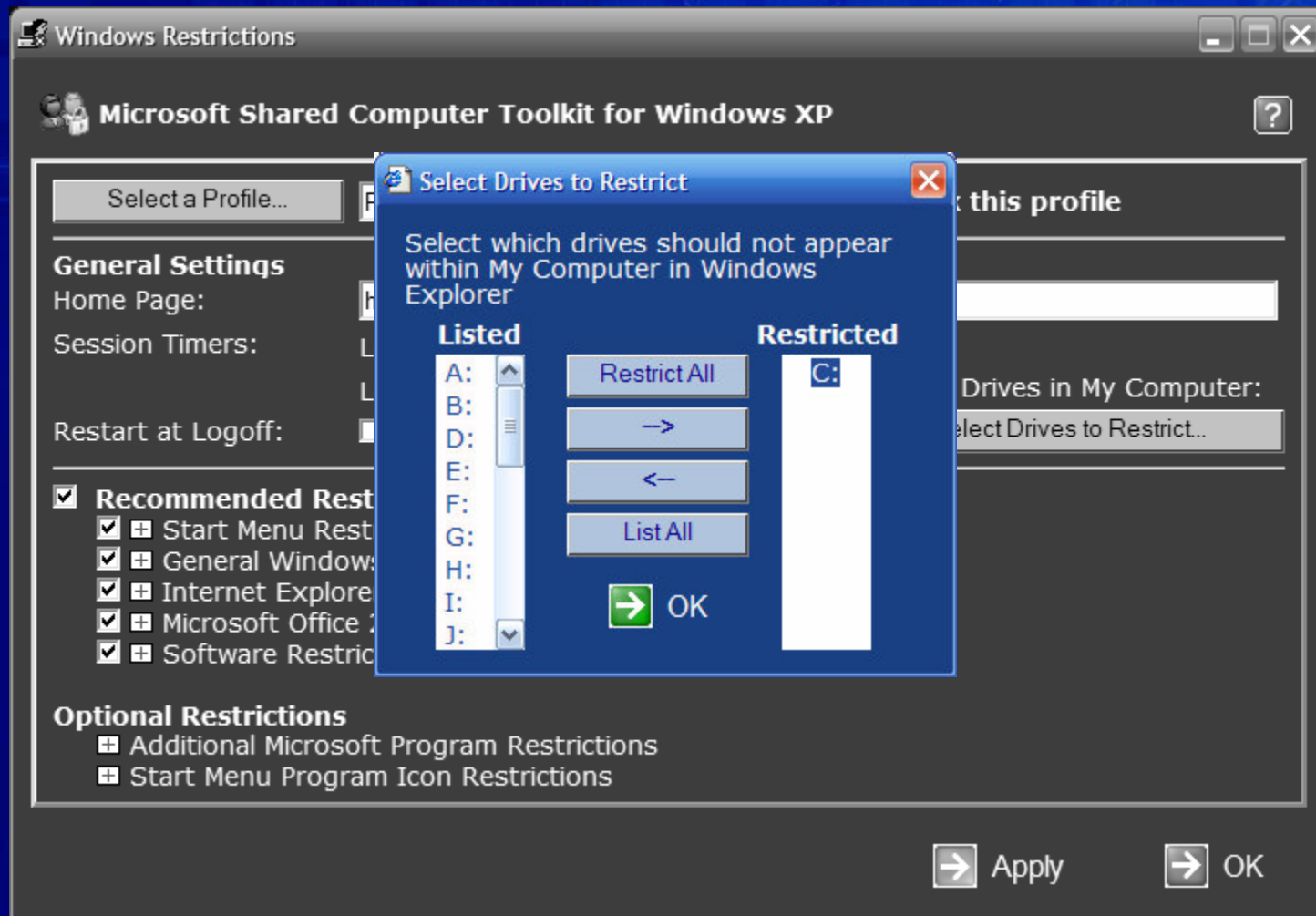


Open Windows Restrictions

The Windows Restrictions Tool



The Windows Restrictions Tool



Test the Public User Profile

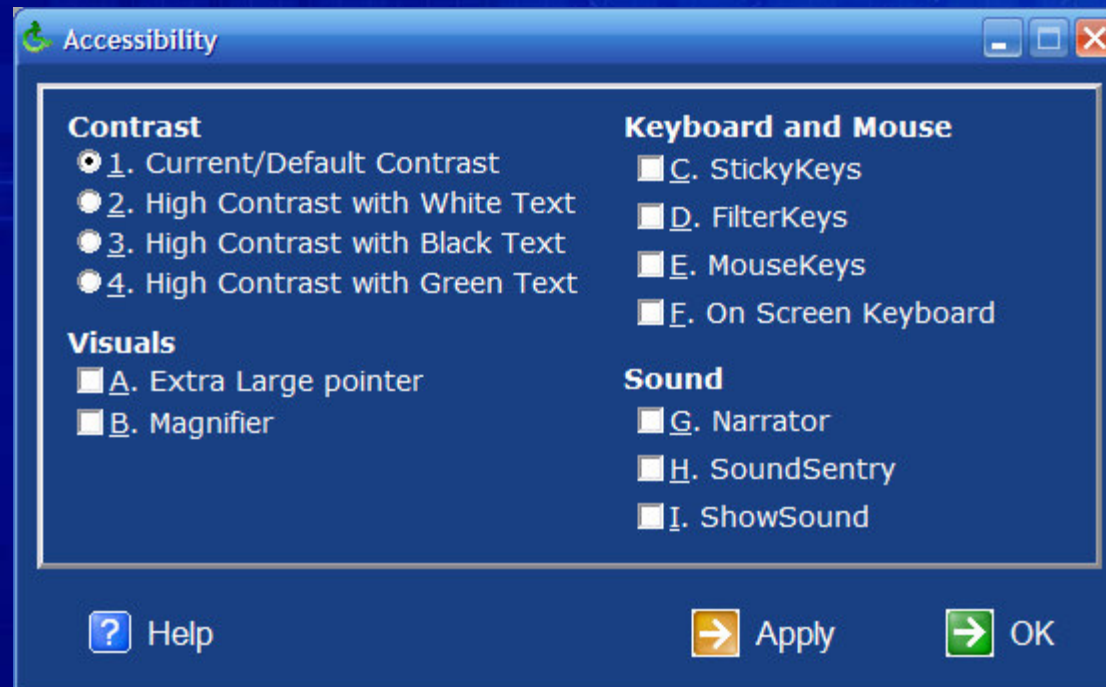
Step 6. Test the Public User Profile

Click **Log off now** and log on as Public to test the restricted user profile, confirm that the necessary programs are available and working, and that the restrictions are appropriate.

 **Log off now**

Log on as the Toolkit administrator and then return here (**Getting Started**) to complete the remaining steps.

The Accessibility Tool



Turn on Windows Disk Protection

Step 7. Turn on Windows Disk Protection

Click **Open Windows Disk Protection**, select **Turn On**, and then:

- If prompted, click **Yes** to the antivirus update script suggestion.
- Ensure that **Critical Updates** are enabled and scheduled to occur every day while the computer is not in use.
- Click **OK** to finish and then click **Yes** when asked to restart the computer.

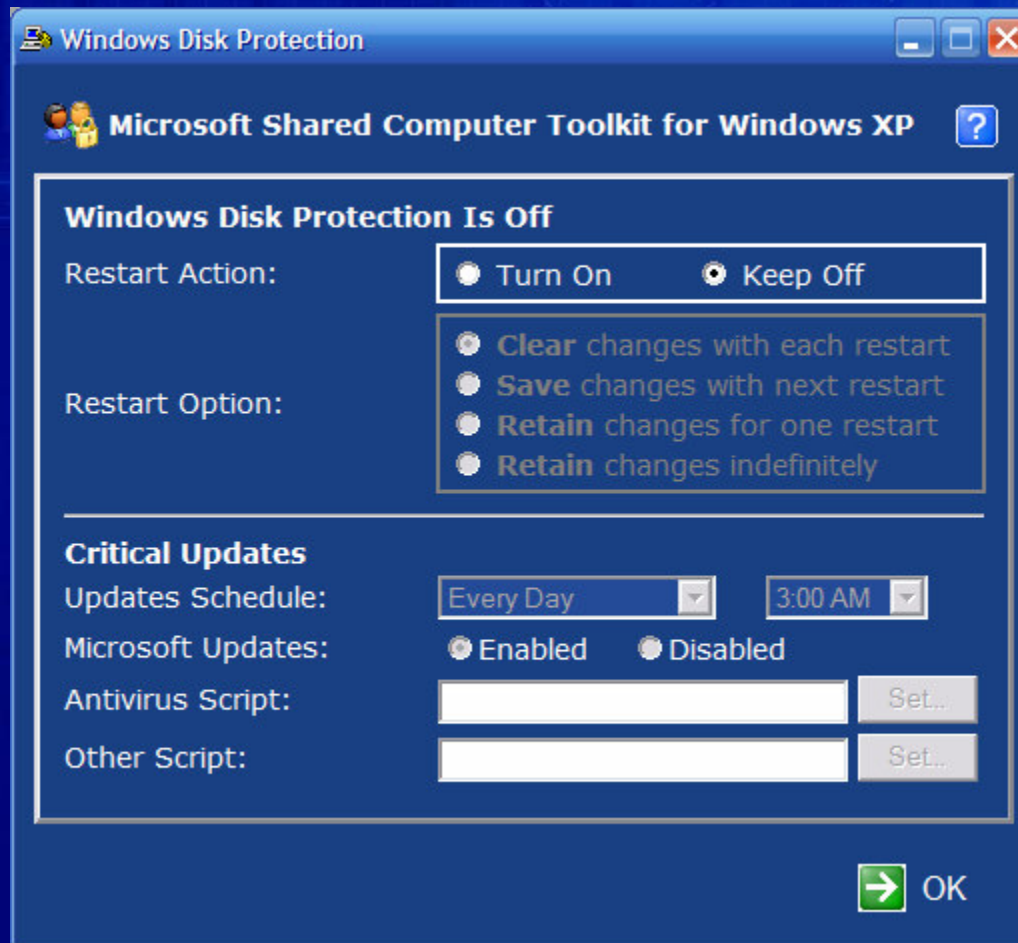
Important: When Windows Disk Protection is on, return to the Windows Disk Protection tool to **Save Changes** of any kind to the Windows partition. For example, **Save Changes** is required when you install new programs or make any Windows configuration changes while Windows Disk Protection is on.

Note: The *Windows partition* is usually the C: drive, which contains Windows and other programs.

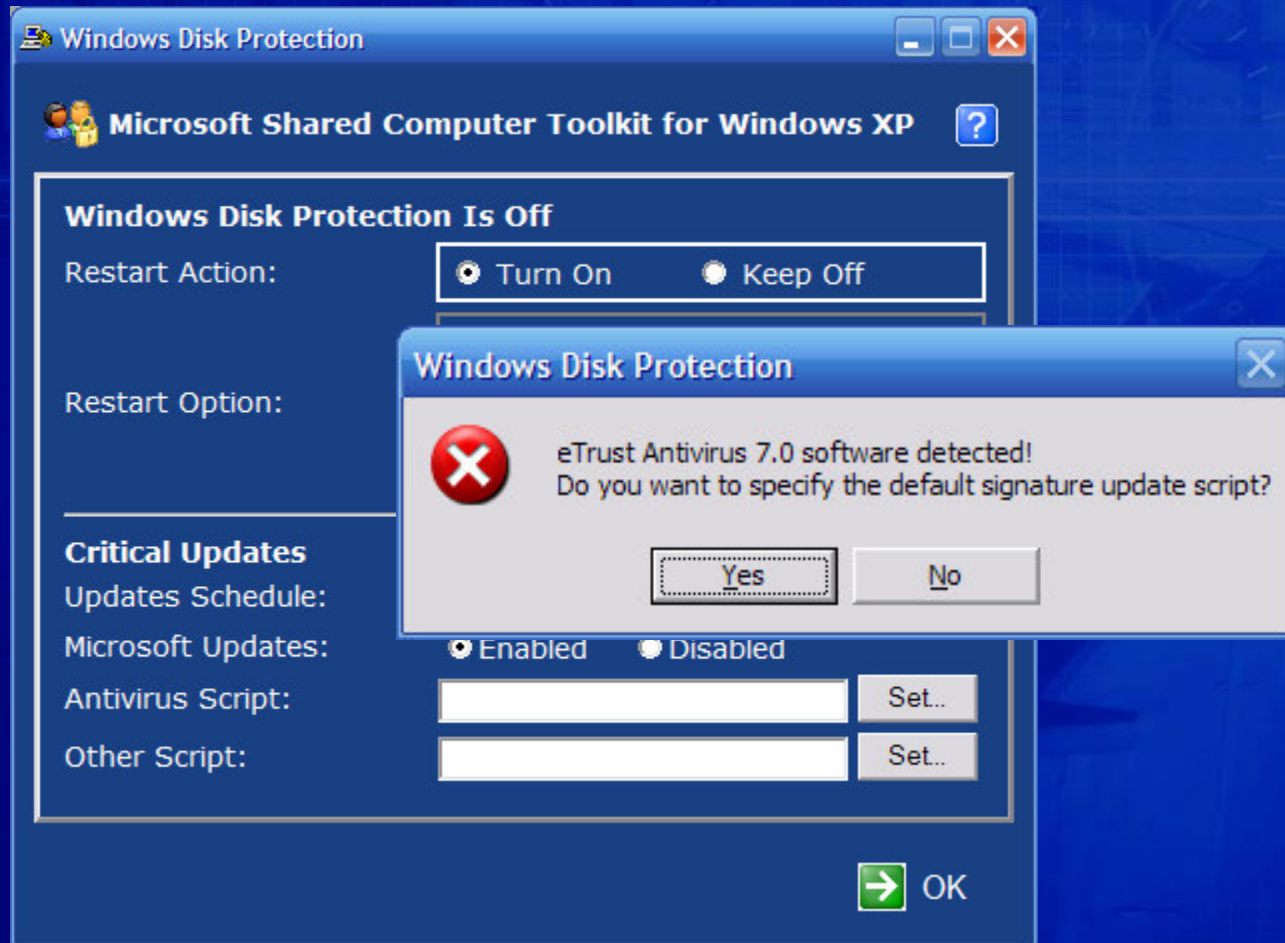


Open Windows Disk Protection

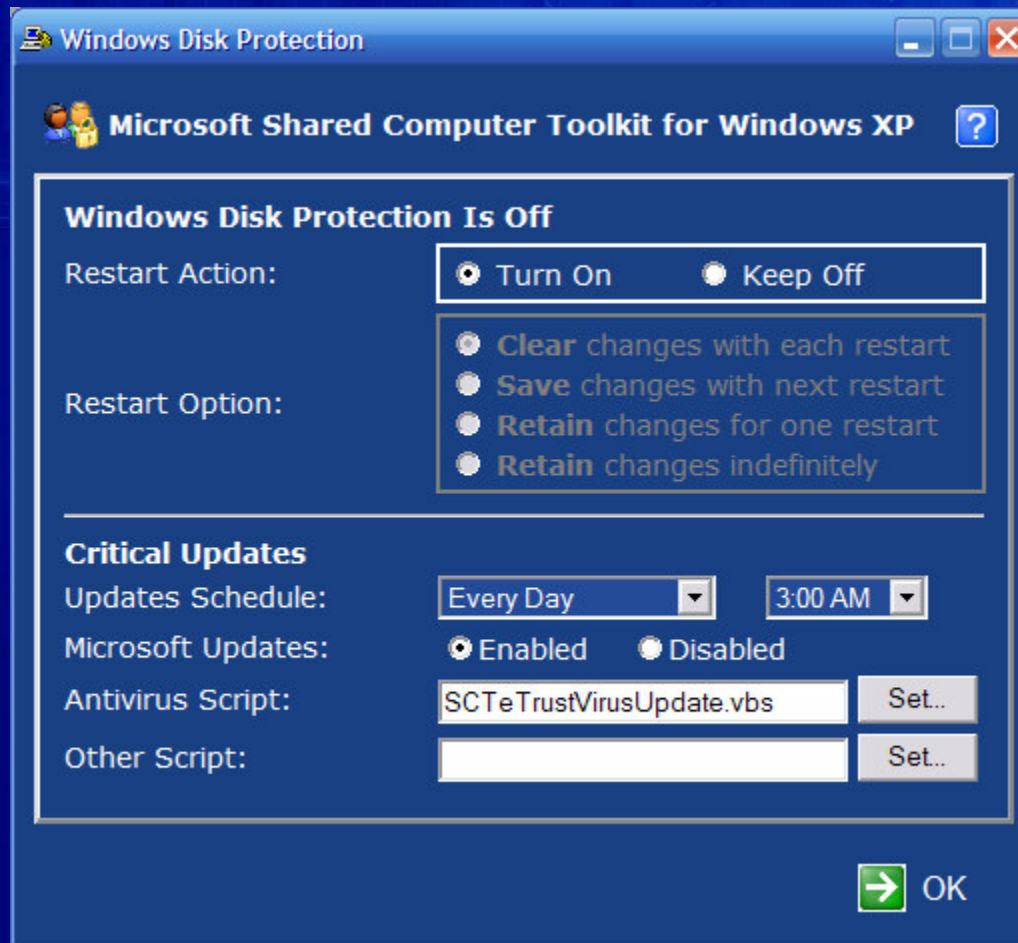
The Windows Disk Protection Tool



The Windows Disk Protection Tool



The Windows Disk Protection Tool



Getting Started - Step 8

Step 8. You're Done! Learn More About the Toolkit

The Handbook includes additional best practices and steps you should consider for improving the security and reliability of your shared computers, as well as several advanced topics.



[Open the Shared Computer Toolkit Handbook](#)

Help describes each tool in more detail, and provides information about several useful command-line tools that may interest you.



[Open the Shared Computer Toolkit Help](#)

Handbook and Help



Microsoft Shared Computer Toolkit for Windows XP Handbook

Microsoft
Your potential. Our passion.™

A screenshot of the Microsoft Shared Computer Toolkit for Windows XP help window. The window title is "Microsoft Shared Computer Toolkit for Windows XP". It has a menu bar with "Hide", "Back", "Print", and "Options". Below the menu bar are tabs for "Contents" and "Index". The "Contents" tab is active, showing a tree view of the help topics. The "Introduction to the Toolkit" topic is selected and expanded, showing sub-topics like "Tools Summary", "Supported Environments", "Installation", "Tools", and "Command Line Tools". The "Introduction to the Toolkit" page is displayed on the right, featuring a welcome message, a globe icon with a question mark, and several paragraphs of text explaining the toolkit's purpose and usage.

Microsoft Shared Computer Toolkit for Windows XP

Hide Back Print Options

Contents Index

- Introduction to the Toolkit
 - Tools Summary
 - Supported Environments
- Installation
 - Prerequisites
 - Install the Toolkit from a Download
 - Install the Toolkit from CD-ROM
 - Set Up the Toolkit (OEM Pre-Installations Only)
 - Uninstall the Toolkit
- Tools
 - Accessibility
 - Getting Started
 - User Profiles
 - Windows Disk Protection
 - Windows Restrictions
- Command Line Tools
 - Accessibility.wsf
 - AutoDemo.wsf
 - AutoLogon.wsf
 - AutoRestart.wsf
 - AutoRunOnce.wsf
 - CriticalUpdates.wsf
 - DiskProtect.wsf
 - Restrict.wsf
 - SCTReport.wsf
 - UserProfiles.wsf
 - SleepWakePC.wsf
 - Welcome.wsf

Introduction to the Toolkit

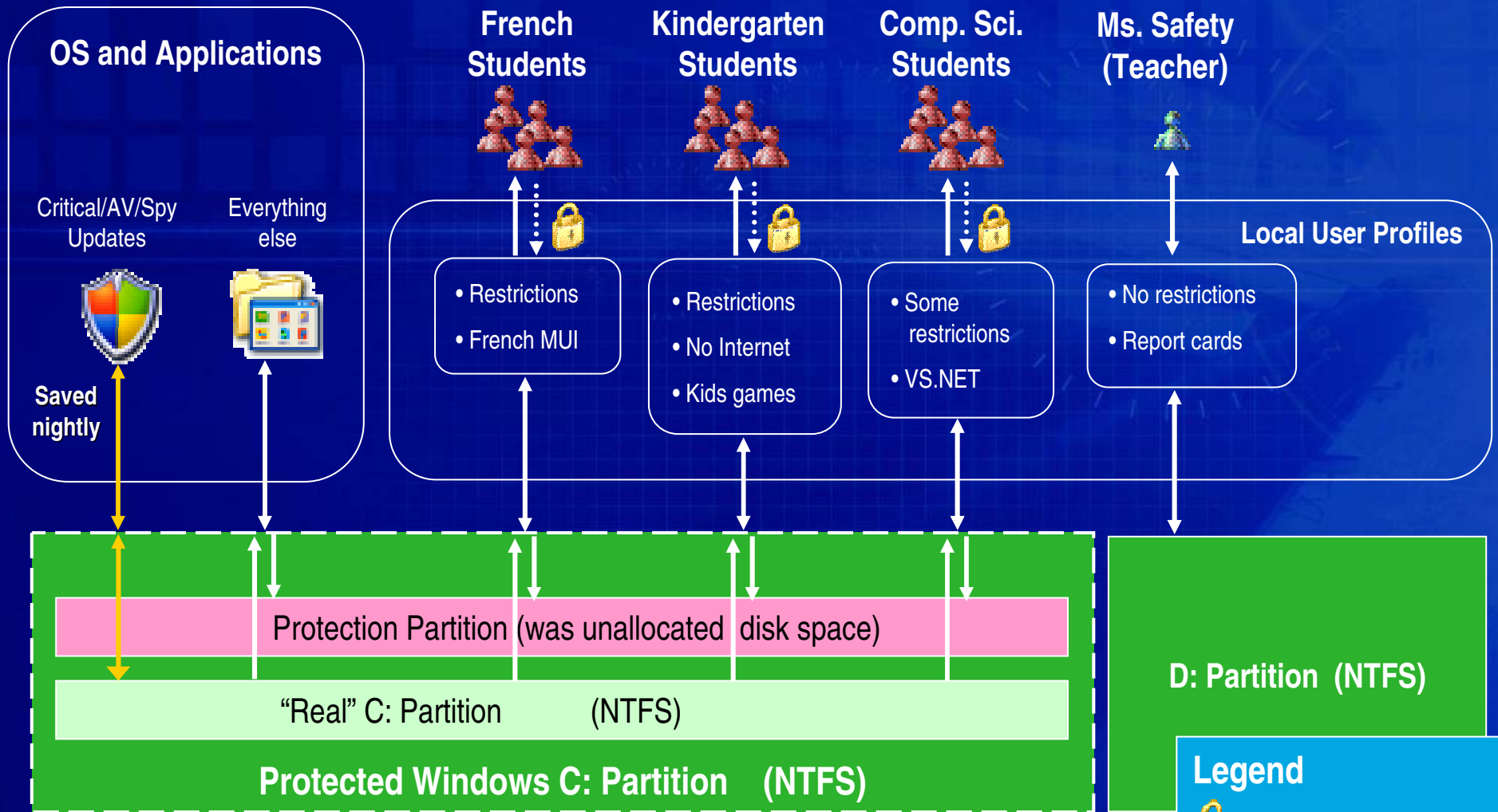
Welcome to the Microsoft Shared Computer Toolkit for Windows XP Help.

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 the user experience. The Toolkit runs on genuine copies of Windows XP Professional, Windows XP Home Edition, and Windows XP Tablet PC Edition.

Toolkit Software Security Summary



A defense-in-depth approach to software security:

Trustworthy computer + restricted profiles + locked profiles + protected OS partition + critical updates + Windows Firewall

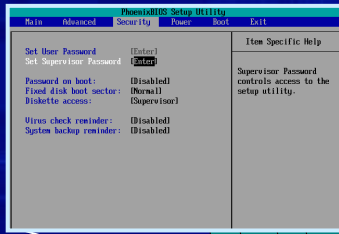
Toolkit Computer Security (Guidance)



Physical Monitoring

Administrator account security

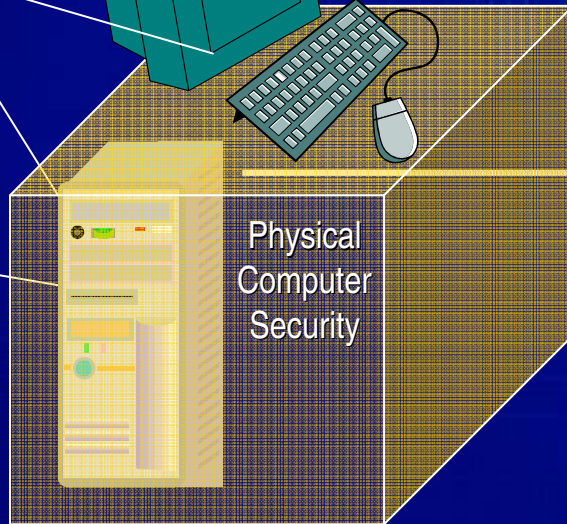
BIOS Security



Physical Network Access Security



* Basic Site Filtering



Physical Computer Security

Network Firewall



Internet

* Third-party site and content filtering services

Wireless network segmentation



A defense-in-depth approach to computer security:
Admin, BIOS, physical, and network security

* Filtering technologies are related to the user experience, not security

Advanced Toolkit Scenarios - Handbook

- Providing Persistent User Data
- Customizing Start Menus
- Restricted Administrators
- Blocking ActiveX Controls
- Simple Site Filtering
- Central Client Management
- Restricting a Family Computer
- Cloning a Computer with the Toolkit

Toolkit & Active Directory - Handbook

Windows Restrictions

- For local, shared accounts
- Active Directory and Group Policy has better central management
- Locked user profile = mandatory user profile
- Useful for:
 - Default profile restrictions
 - Local user restrictions in Domain environment
 - Getting started with Group Policy

Windows Disk Protection

- Works well on domain-joined computers
 - Machine account password management addressed
- **Caution:** Don't stay in Retain Changes mode for long (<30 days)
- UserProfiles command-line tool can create domain user profiles on alternative partitions for persistence

Shared Computer Toolkit Benefits

Restrict *untrusted users from accessing system settings and data*

- Create different user profiles for different types of untrusted users
- Restrict user profiles so users can only access the system resources they need
- Lock user profiles so user data, settings, and browser history are protected from other users

Defend *shared computers from untrusted users, viruses, and spyware*

- Prevent unapproved changes to a computer's hard disk. Changes are automatically reversed each time the computer re-starts
- Allow critical security updates and antivirus definitions to be permanently saved
- Learn additional security techniques from the user handbook

Enhance *the user experience*

- Simplify the user interface
- Increase privacy and security
- Make accessibility features easier

Call To Action

- **Download the Beta today!**

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

- Newsgroup support and feedback
- Aggressive schedule for the 1.0 release
- Early feedback appreciated

- **Questions? Feedback?**

<news://news.microsoft.com/microsoft.public.windows.sharedaccess>