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*

- **Non-focus**
  - Untrusted, often unknown users

- **At work**
  - Universities
  - Community colleges
  - K-12 Schools

- **At school**
  - Public libraries
  - Internet Cafes
  - Rural kiosks
  - Community centers

- **Around town**
  - Airports
  - Hotels
  - Business Conferences

- **On the road**
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

# Ideal Customers

<table>
<thead>
<tr>
<th>Organizations</th>
<th>People / Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>• K-12 schools</td>
<td>Depending on the size of the org.:</td>
</tr>
<tr>
<td>• Colleges and universities</td>
<td>• Technology Coordinators</td>
</tr>
<tr>
<td>• Libraries</td>
<td>• Teachers and Librarians</td>
</tr>
<tr>
<td>• Community technology centers</td>
<td>• Volunteers</td>
</tr>
<tr>
<td>• Internet and gaming cafes</td>
<td>• IT Managers</td>
</tr>
<tr>
<td>• Owners of Internet kiosks</td>
<td>• Network or System Engineers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Not Ideal</th>
<th>Environments</th>
</tr>
</thead>
<tbody>
<tr>
<td>• “Enterprise” customers, employee computers, servers</td>
<td>• Workgroup or standalone computers</td>
</tr>
<tr>
<td>• Consumers looking for parental controls</td>
<td>• All tools</td>
</tr>
<tr>
<td>• Special purpose kiosks</td>
<td>• Domain-joined computers</td>
</tr>
<tr>
<td></td>
<td>• Some tools</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Threats</th>
<th>Attack Vectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accidents</td>
<td>Windows is flexible</td>
</tr>
<tr>
<td>“Just for fun” hackers</td>
<td>Too flexible for the shared computer environment</td>
</tr>
<tr>
<td>Malware and spyware</td>
<td>Command-line access</td>
</tr>
<tr>
<td>Rootkits</td>
<td>Scripts and macros</td>
</tr>
<tr>
<td>Vandals</td>
<td>Starting &amp; stopping processes</td>
</tr>
<tr>
<td>Stalkers, predators, and spies</td>
<td>Editing the registry</td>
</tr>
<tr>
<td></td>
<td>Privilege escalation</td>
</tr>
<tr>
<td></td>
<td>Every application offers new possibilities</td>
</tr>
</tbody>
</table>
Attack Vectors

Windows Task Manager

- Image Name: svchost.exe, User Name: SYSTEM, CPU: 0%, Mem: 4.056 KB
- Processes: 83, CPU Usage: 4%, Commit Charge: 526 MB / 3917 MB

Create New Task

- Open: EXPLORE.EXE

Registry Editor

- My Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
  - HKEY_CURRENT_CONFIG

- (Default) REG_SZ
  - (value not set)

C:\WINDOWS\system32\cmd.exe

- G:\WINDOWS\system32\cmd.exe

Documents - Microsoft Word

- Open: aspell

- Bad code in here!
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.


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

Disk Management window showing a Windows Partition (C:) with 36.00 GB free space and 64% free.

Another window showing a CD-ROM (D:) with No Media.

A third window showing a CD-ROM (E:) with No Media.
## 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.
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](image)
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

User Profiles
- User files and settings
- Stored on disk

Tips
- Accounts and Profiles are distinct, yet related
- User Profile is created with first logon
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.
The Windows Restrictions Tool

Microsoft Shared Computer Toolkit for Windows XP

Select a Profile...  Public

Lock this profile

General Settings
Home Page: http://www.msn.com/
Session Timers:
  Log off after 60 minutes of use
  Log off after 1 minutes idle
Restart at Logoff:

Recommended Restrictions for Shared Accounts
- Start Menu Restrictions
- General Windows XP Restrictions
- Internet Explorer Restrictions
- Microsoft Office 2003/XP Restrictions
- Software Restriction Policy

Optional Restrictions
- Additional Microsoft Program Restrictions
- Start Menu Program Icon Restrictions

Apply  OK
The Windows Restrictions Tool

Microsoft Shared Computer Toolkit for Windows XP

General Settings
Home Page:
Session Timers:
Restart at Logoff:

Recommended Restrictions
- Start Menu Restrictions
- General Windows Policies
- Internet Explorer Policies
- Microsoft Office Policies
- Software Restrictions

Optional Restrictions
- Additional Microsoft Program Restrictions
- Start Menu Program Icon Restrictions

Select Drives to Restrict
Select which drives should not appear within My Computer in Windows Explorer

Listed
A: B: C: D: E: F: G: H: I: J:

Restricted
Restrict All
OK

Apply
OK
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 on as the Toolkit administrator and then return here (**Getting Started**) to complete the remaining steps.
# The Accessibility Tool

## Contrast
- 1. Current/Default Contrast
- 2. High Contrast with White Text
- 3. High Contrast with Black Text
- 4. High Contrast with Green Text

## Visuals
- A. Extra Large pointer
- B. Magnifier

## Keyboard and Mouse
- C. StickyKeys
- D. FilterKeys
- E. MouseKeys
- F. On Screen Keyboard

## Sound
- G. Narrator
- H. SoundSentry
- I. ShowSound

[Image of the Accessibility Tool interface with options for contrast, visuals, keyboard and mouse, and sound settings.]
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

Microsoft Shared Computer Toolkit for Windows XP

Windows Disk Protection Is Off
- Restart Action: Turn On
- Keep Off

Restart Option:
- Clear changes with each restart
- Save changes with next restart
- Retain changes for one restart
- Retain changes indefinitely

Critical Updates
- Updates Schedule: EveryDay
- Time: 3:00 AM
- Microsoft Updates: Enabled
- Antivirus Script: Set...
- Other Script: Set...
The Windows Disk Protection Tool

Microsoft Shared Computer Toolkit for Windows XP

Windows Disk Protection Is Off
Restart Action: [ ] Turn On [ ] Keep Off

Restart Option:

Critical Updates
Updates Schedule:
Microsoft Updates: [ ] Enabled [ ] Disabled
Antivirus Script: [ ] Set...
Other Script: [ ] Set...

Windows Disk Protection
eTrust Antivirus 7.0 software detected!
Do you want to specify the default signature update script?
[ ] Yes [ ] No

OK
The Windows Disk Protection Tool

Microsoft Shared Computer Toolkit for Windows XP

Windows Disk Protection Is Off

Restart Action:
- Turn On
- Keep Off

Restart Option:
- Clear changes with each restart
- Save changes with next restart
- Retain changes for one restart
- Retain changes indefinitely

Critical Updates
Updates Schedule:
- Every Day
- 3:00 AM

Microsoft Updates:
- Enabled
- Disabled

Antivirus Script:
- SCTeTrustVirusUpdate.vbs

Other Script:

Set...
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

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.
A defense-in-depth approach to software security:
Trustworthy computer + restricted profiles + locked profiles + protected OS partition + critical updates + Windows Firewall
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