handbook

Windows® SteadyState™

To help your computers stay the way you want them to – no matter **who** uses them

Microsoft®

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all 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.

Complying with all 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 in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Microsoft, Active Directory, ActiveX, Internet Explorer, MSDN, Systems Management Server, Visual Basic, Windows, Windows Live, Windows Server, Windows SteadyState, and Windows Vista are trademarks or registered 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

Introduction to Windows SteadyState

Windows® SteadyState™ helps make shared computers easier to set up and maintain for administrators, and more reliable and consistent for computer users. By using Windows SteadyState, you can more effectively:

- Defend shared computers from unauthorized changes to their hard disks.
- Restrict users from accessing system settings and data.
- Enhance the user experience on shared computers.

These capabilities make Windows SteadyState beneficial in situations where a computer is used by multiple people, such as schools, public libraries, community technology centers, and Internet cafés.

Protecting Shared Computers

A unique challenge exists for shared computer environments. Microsoft software is designed to offer users a great degree of flexibility in their ability to customize their experience and to make changes to their computer settings. However, in a shared computer environment, administrators will typically not want to provide the full set of customization and change capabilities because doing so could allow changes to be made that affect the health of the computer and the experience for other users. On a shared computer, privacy and uniformity are very important elements of the maintenance and use of the system. Windows SteadyState helps an administrator protect a shared computer against unwanted changes.

What This Handbook Includes

Windows SteadyState Handbook is designed to help you install Windows SteadyState, set up and customize user profiles and computer settings, and use other Windows SteadyState features and capabilities quickly and efficiently.

This section provides a brief overview of the installation and configuration tasks and procedural steps provided in this handbook.

Note: *Comments about this handbook or Windows SteadyState can be entered on the Windows SteadyState Community Web site at: http://go.microsoft.com/fwlink/?LinkId=77957.*

Installing Windows SteadyState

Prepare your computer for a shared user environment with these step-by-step procedures for installing Windows SteadyState. Included are preinstallation tasks to make the installation process more efficient.

Creating User Accounts and Configuring User Settings

With Windows SteadyState, you can apply different system and feature restrictions to each user account on the computer so that users have limited access to Windows system tools, as well as other services, applications, files, and data.

Setting Computer Restrictions

Set Computer Restrictions helps you to set privacy and security restrictions that will apply to the computer as a whole and help you design a uniform user experience.

Scheduling Important Software Updates

Windows SteadyState includes Schedule Software Updates to help you download and install updates. Schedule Software Updates works with Windows Disk Protection to help ensure that important updates are applied to the computer and not removed.

Protecting the Hard Disk

Windows Disk Protection is designed to protect the Windows operating system and program files from being permanently changed. During the course of normal activity, users can perform actions which affect the hard disk. Windows Disk Protection discards any modifications made during a user's session and returns the Windows partition to the default environment at restart of the computer.

Exporting and Importing User Profiles

The Export and Import features help you to export shared user profiles created on one computer and import them to any computer on which Windows SteadyState is installed.

Scenarios for Advanced Administrators

The advanced scenarios provided in this section are intended for Windows SteadyState administrators with advanced technical expertise and experience in the configuration and administration of Microsoft® Windows XP.

Installing Windows SteadyState

Installation of Windows SteadyState consists of preparing the computer for the shared user environment and installing Windows SteadyState. This section covers:

- Confirming system requirements
- Configuring the system for shared use
- Performing preinstallation tasks
- Installing and uninstalling Windows SteadyState
- Using Windows SteadyState

Confirming System Requirements

Systems running Windows SteadyState must meet the minimum system configuration requirements listed in Table 1.

Table 1: System Requirements

Component	Requirement
Computer and processor	300 megahertz (MHz) or higher processor clock speed recommended; 233 MHz minimum required (single or dual processor system);* Intel Core/Pentium/Celeron family, or AMD K6/Athlon/Duron family, or compatible processor recommended.
Memory	128 megabytes (MB) of RAM or higher recommended (64 MB minimum supported; may limit performance and some features).
Hard disk	1.5 gigabytes (GB) of available hard disk space without Windows Disk Protection, or 4.0 GB of available hard disk space with Windows Disk Protection.
Operating system	Windows XP Professional, Windows XP Home Edition, or Windows XP Tablet PC Edition with Windows XP Service Pack 2 (SP2) installed. Note: Windows SteadyState does not run with Windows Vista™.
File System	NTFS file system.

Component	Requirement
Tools	Windows Scripting and Windows Management Instrumentation (WMI) must be working.
Access	Administrator level access.

Configuring the System for Shared Use

An efficient way to configure a computer for shared use is to first install the full set of features, services, and programs that you will want to offer users. Configuring the system in this way (before Windows SteadyState is installed) will help you to set up shared user profiles more efficiently and to defined settings and place restrictions on the existing configuration.

It is possible to add or remove programs after Windows SteadyState is installed; however, Windows Disk Protection must be turned off before doing so. Also, you must reconfigure each of the user settings to reflect the changes.

Important: *If you have turned on Windows Disk Protection, you must turn off this option before any new software is installed or new restrictions are set.*

Caution: *Some software is not optimized for a shared computer environment. For example, desktop search tools may reveal private information on the shared computer. E-mail clients requiring configuration, and Windows components such as fax services and Internet Information Services (IIS) can also add to the maintenance burden for the computer. They may also cause an inconsistent user experience on a shared computer.*

Accessibility

Windows SteadyState does not have any specific accessibility provisions. All accessibility provisions that are offered through Windows XP Professional are available when using Windows SteadyState.

Note: *We recommend restricting shared user access to **Control Panel** in Windows XP to avoid changes made by shared users to system settings on the computer. Note that if you set this recommended restriction, users can still modify the Accessibility settings from the **Accessories** menu in Windows XP.*

Performing Preinstallation Tasks

Before you install Windows SteadyState:

- Uninstall Microsoft Shared Computer Toolkit for Windows XP, the predecessor to Windows SteadyState, if necessary. See the “To Uninstall Shared Computer Toolkit” procedure in this handbook.
- Defragment system drives, configure display settings, and remove any software that should not be made available to any user profile. For shared systems, consider also clearing the Internet History folder and deleting files in My Documents.

Important: *It is critical that you perform this step before setting up Windows Disk Protection.*

- Download and install the latest critical updates from the Windows Update Web site at: http://go.microsoft.com/fwlink/?LinkId=83424.
- Download and install up-to-date antivirus software.
- Scan for viruses, unwanted software, and malicious software.
- Set the Administrator password.
- Install all of the features, services, and programs that you want to make available to your users (recommended). For more information on configuring your shared access computer before you install Windows SteadyState, see the "Configuring the System for Shared Use" section in this handbook.

► To Uninstall Shared Computer Toolkit

Important: *Shared user profiles will retain any restrictions placed on them after Shared Computer Toolkit is uninstalled because they remain on the computer after uninstallation. Existing shared user profiles will be available on installation of Windows SteadyState.*

1. Turn off Windows Disk Protection:
   a. On the **Start** menu, click **Programs**, and then click **Microsoft Shared Computer Toolkit** to open the Shared Computer Toolkit.
   b. Click **Windows Disk Protection**.
   c. Click **Keep Off**.
   d. Restart the computer when prompted.
2. Remove restrictions placed on the shared user profiles if necessary.
3. Uninstall Shared Computer Toolkit:
   a. On the **Start** menu, click **Programs**, click **Microsoft Shared Computer Toolkit**, and then click **Uninstall the Shared Computer Toolkit**.

      A message appears stating: "Removing the Toolkit will automatically restart the computer."
   b. Click **Remove** to begin the uninstallation process.
   c. Click **Finish** to restart your computer.
4. Remove the User Profile Hive Cleanup Service (UPHClean):
   a. On the **Start** menu, click **Settings**, click **Control Panel**, click **Add or Remove Programs**, and then click **Remove Program**.

b. Select **User Profile Hive Cleanup Service**, and then click **Remove**.

   A message appears stating: “Are you sure you want to remove User Profile Hive Cleanup Service from your computer?”

c. Click **Yes** to start the Shared Computer Toolkit uninstallation program, which will take approximately five seconds to complete.

5. Shared Computer Toolkit required you to create a separate partition for Windows Disk Protection. You can now reclaim this hard disk space and remove this partition, as it is not required by Windows SteadyState.

Now that Shared Computer Toolkit is uninstalled, you can proceed with the installation of Windows SteadyState.

Installing Windows SteadyState

You can download the installation files for Windows SteadyState from the Microsoft Download Center or from a disc. You can then use the Windows SteadyState Installation Wizard to install Windows SteadyState on your computer.

Windows SteadyState can be installed only on computers running a genuine Microsoft Windows XP operating system. After you launch the Installation Wizard, you will be asked whether you want Microsoft to validate your installation of Windows XP. If your installation of Windows XP cannot be validated, you will have an opportunity to obtain a valid product key at that time.

For more information on the Windows Genuine Advantage, see the Windows Genuine Advantage Web site at: http://go.microsoft.com/fwlink/?LinkId=83431.

► To download installation files from the Microsoft Download Center

Downloading from the Microsoft Download Center will place the **Windows SteadyState Installation Wizard** icon on your desktop for easy reference.

1. Log on as Administrator or a member of the Administrators group on the shared computer.
2. Go to the Microsoft Download Center at: http://go.microsoft.com/fwlink/?LinkId=83430.
3. In the **Search** box, type **Windows SteadyState**
4. Follow the prompts on the Download Center Web site.
5. Double-click the downloaded installation file to start the Windows SteadyState Installation Wizard.

► To install Windows SteadyState

1. Log on as Administrator or as a member of the Administrators group on the shared computer.
2. Start Setup.exe from the installation disc or from the computer. To start Setup.exe, double-click the file icon.
3. Click **Validate** to verify your copy of Windows is genuine. You can click **Cancel** to exit the Windows SteadyState Installation Wizard.
4. When the verification has successfully completed, you will see the **Microsoft Software License Terms** page.
5. If you agree to the terms, click **I accept the license terms**, and then click **Next** to install Windows SteadyState.
6. Click **Finish** to complete the Windows SteadyState installation.

► To uninstall Windows SteadyState

1. Turn off Windows Disk Protection. For instructions, see the "Protecting the Hard Disk" section in this handbook.
2. Remove restrictions placed on the shared user profiles. Shared user profiles will remain on the shared computer even after Shared Computer Toolkit or Windows SteadyState has been uninstalled and will retain any restrictions applied to them. If you want to keep the restrictions in place on user profiles after Windows SteadyState is uninstalled, go on to step 3.
3. On the **Start** menu, click **Settings**, click **Control Panel**, and then select **Add or Remove Programs** from the **Pick a Category** list.
4. Click **Remove Programs**.
5. Select **Windows SteadyState,** and then click **Remove**.

Using Windows SteadyState

The main screen of Windows SteadyState is your starting place to access each setting and restriction you can apply. These settings are divided into two types of settings, as shown in Figure 1:

- **Computer Settings**—Use these settings to protect and schedule software updates for the entire computer.
- **User Settings**—Use these settings to configure and restrict specific user accounts.

Additional information on the settings and options available in the **Windows SteadyState** main dialog box are provided in Table 2.

Tip: *For additional information and support, the left navigation pane of Windows SteadyState includes links to several resources, such as the Windows SteadyState Community Web site.*

Figure 1: Settings and options in the Windows SteadyState main dialog box.

Table 2: Description of Settings and Options in Windows SteadyState

Setting or option	Description
1. Protect the Hard Disk	• Turn Windows Disk Protection on or off. • Set protection levels for the system drive.
2. Schedule Software Updates	• Schedule software and antivirus updates automatically or manually. • Add custom scripts that run at scheduled intervals.
3. Set Computer Restrictions	• Set system-wide, global computer restrictions. • Select privacy options, security restrictions, and other settings for the entire shared computer.
4. User Profiles	• Select user profiles, configure Windows and feature restrictions, and block programs for a selected profile. • Lock or unlock a user profile. • Set the session timer, change passwords, change user profile picture, and delete a user profile.
5. Add a New User	• Add a new user, create a user name, set passwords, and select where a user profile is stored. • Select a picture to identify the user profile.

Setting or option	Description
6. Export User	• Export existing user profile. • Save a user profile so that it can be moved to another shared computer.
7. Import User	• Import an existing user profile. • Import an exported user profile to a shared computer with Windows SteadyState installed.
8. Additional Support	• Find links to additional resources for Windows SteadyState.

Creating User Accounts and Configuring User Settings

After installing Windows SteadyState, your next step is to create new user accounts and configure their corresponding user profiles for shared computer use.

This section covers:

- Understanding shared user terminology
- Creating a shared user account
- Configuring the shared user profile
- Understanding shared user profile settings and restrictions
- Testing shared user profiles

Shared User Terminology

The terms and definitions provided in Table 3 are specific to Windows SteadyState or a shared computer experience, and apply to the content in this handbook. For more information on terms and definitions, see "Appendix A: Windows SteadyState Glossary" in this handbook.

Table 3: Shared User Terminology

Term	Definition
Shared user profile	A shared user profile is a single user profile, attached to a single user account that is shared by multiple users on one computer.
User	A user is a person who uses a shared computer.
Shared user account	A single user account that is logged on to by multiple users.

Figure 2 shows the differences between a user profile in Windows XP and a shared user profile in Windows SteadyState. When shared user profiles are created in Windows SteadyState, settings and restrictions are applied to all users who access the shared user account on the computer.

Figure 2: User profiles in Windows XP and shared user profiles in Windows SteadyState.

Creating a Shared User Account

You can create shared user accounts and apply different system and program restrictions to each shared user account on the computer so that users have specified access to Windows system tools, as well as other services, applications, files, and data.

Typically, names for user accounts are chosen to describe the individual or group of individuals who will have access to the shared computer. The user account name should reflect the group or category of user for which the account is intended. Before naming a user account, determine who your users are and what levels of restrictions that must be applied to the user account. For example, consider whether your users are:

- Staff members who can access most of the applications on the computer and can use many computer configuration applications, such as **Control Panel** settings, but should be restricted from most advanced administrative tools and applications.
- Adults who can access most of the applications on the computer but should not alter computer configuration settings.
- Children who should have restricted Internet access.

► To create a shared user account

1. In the **Windows SteadyState** main dialog box, under **User Settings**, click **Add a New User**.
2. In the **Add a New User** dialog box, in the **User Name** box, type a user name.
3. Type a password in the **Password** and **Confirm Password** boxes.

Note: *Password policy requirements that apply for Windows XP also apply for Windows SteadyState, including well-formed password requirements. For more information on creating passwords, see: http://go.microsoft.com/fwlink/?LinkId=83432.*

4. In the **User Location** drop-down list, select the drive on which you want to save the shared user profile associated with this shared user account. Normally, the files and directories associated with user profiles are stored on the system drive where Windows XP is installed.
5. Select a picture from the **Picture** box to associate with the shared user profile, and then click **OK**.

In most cases, you will want to save the shared user profile on the same drive on which Windows XP is installed. However, if you have turned on Windows Disk Protection and want a user to be able to save information to the computer for later access, you can save the user profile as an unlocked profile on a different drive. Windows Disk Protection only protects the partition containing the operating system files. Saving an unlocked user profile on a different drive will prevent removal of the user's data by Windows Disk Protection.

For more information on permanent user profiles and data, see the "Creating Permanent User Profiles on a Separate Partition" section in this handbook.

For more information on locked user profiles, see the "Lock Profile" section in this handbook.

Configuring the Shared User Profile

After creating the shared user account, you can manually configure specific settings and restrictions for the associated shared user profile. You can customize the shared user profile and create an environment for users of the shared user profile.

As a Windows SteadyState administrator, you can choose a default restriction level of High, Medium, or Low that automatically applies the recommended settings to the user account you select. You can also choose **Custom restrictions** and set restrictions that are customized to each shared user account that you create in Windows SteadyState.

You can create as many shared user accounts as you require on the shared computer and customize restrictions for each user account in Windows SteadyState. To simplify the number of user accounts you have to create for a public use environment, you can create one account for each level of user that might use the computer, and then apply specific restrictions to each

account. For example, you might want to create a user account for each of the following classifications of users:

- Adult
- Child
- Teen

In this example, you can set the **Low restrictions** option on the Adult user account because they are more technically advanced or require access to system resources. You can set the **Medium restrictions** option on the Teen user account to limit their access to system settings while still allowing access to computer resources. The Child user account can have the restrictions option set on **High restrictions** for maximum protection of the shared computer system files and limited access to external resources.

Shared User Profile Settings and Restrictions

In the **User Settings** dialog box, you can configure the session limits and program and feature restrictions that you want to apply to the shared user profile. There are four tabs in the **User Settings** dialog box that help you to configure profile settings and restrictions:

- General
- Windows Restrictions
- Feature Restrictions
- Block Programs List

General

On the **General** tab, you can lock the user profile and set session timer limits. Figure 3 shows the **General** tab in the **User Settings** dialog box.

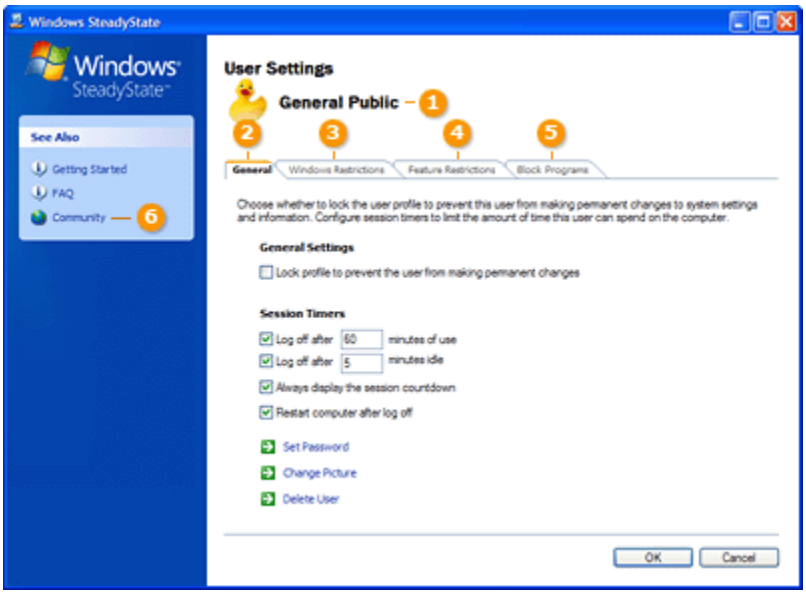

Figure 3: The General tab in the User Settings dialog box.

Additional information on the user settings and options available in the **User Settings** dialog box are provided in Table 4.

Table 4: Description of Settings and Options in the User Settings Dialog Box

Settings and options	Description
1. User	Displays user name and picture for selected user.
2. General	Lock or unlock a user profile. Set session timers, change passwords, change a user profile picture, and delete a selected user profile.
3. Windows Restrictions	Set level of Windows restrictions: High, Medium, Low, No, or Custom. Set **Start** menu and general system restrictions. Hide or display drives.

Settings and options	Description
4. Feature Restrictions	Set level of Feature restrictions: High, Medium, Low, No, or Custom. Set user-specific Internet Explorer and Microsoft Office Restrictions. Enter the home page and specific Web site addresses that user is allowed to view.
5. Block Programs	Select programs to block user from accessing and view currently blocked programs. Browse to add a program on the computer that is not listed.
6. Additional Support	Find links to additional resources for Windows SteadyState.

Lock Profile

On the **General** tab, under **General Settings**, select the **Lock profile to prevent the user from making permanent changes** check box to remove cache files or system history created by the user when the user logs off from the current session. We recommend that you limit the permanent changes made by users on a shared computer by locking the user profile.

There are important distinctions between locked user profiles and Windows Disk Protection. Table 5 shows some of the similarities and differences between locked profiles and Windows Disk Protection.

Table 5: Comparison of Locked Profile and Windows Disk Protection

Feature	Similarities	Differences	When applied
Locked Profile	Removes changes user has made to the user profile. Cache files, global history, and environment settings are cleared or restored to the default state.	User profile is restored to the default state configured by administrator.	At log off of user account.
Windows Disk Protection	Removes changes a user has made to the profile, to the system partition, and any files or data the user has saved on the shared computer or to another partition or drive.	If **Remove all changes at restart** option is selected, restores the entire system partition to the original state configured by the administrator.	At restart of shared computer.

Note: *If a user profile is locked, Windows Disk Protection restores the profile to its default configuration regardless of whether the locked profile is saved to the protected system partition or on another drive.*

For more information on permanent user profiles and data, see the "Creating Permanent User Profiles on a Separate Partition" section in this handbook.

Session Timers

On the **General** tab, under **Session Timers**, you can configure the session timers to define the duration of a logon session or of the idle time before a session terminates. Select the check box for the session timer you want to configure, and then type the number of minutes desired in the text box.

Session Countdown

On the **General** tab, under **Session Timers**, you can select the **Always display the session countdown** check box to configure a notification to appear telling users when their session is about to end. The notification remains on the screen throughout the session. The notification can be moved but it cannot be minimized or turned off by the user. Figure 4 shows the session timer notification.

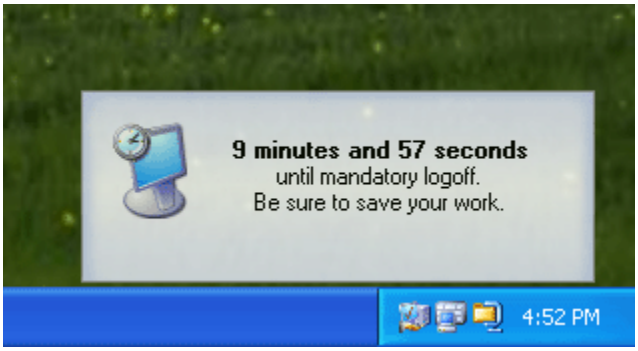

Figure 4: Session timer notification.

Restart Computer After Log Off

On the **General** tab, under **Session Timers**, you can select the **Restart computer after log off** check box to configure the computer to automatically restart when each user session ends.

Windows Restrictions

On the **Windows Restrictions** tab, you can set restriction levels that define the content of menus and the Windows XP tools and features that a user has access to.

The **Windows Restrictions** tab is divided into:

- Levels of restrictions
- Types of restrictions

Figure 5 shows the **Windows Restrictions** tab.

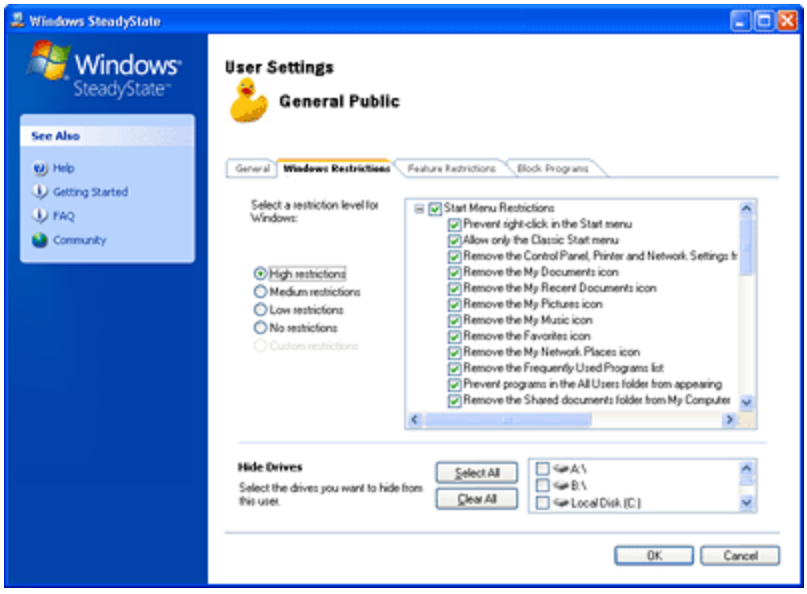

Figure 5: The Windows Restrictions tab.

When you select the **High restrictions**, **Medium restrictions**, or **Low restrictions** option on the **Windows Restrictions** tab, the appropriate types of restrictions are automatically selected. When you select **Custom restrictions,** you can manually select the types of restrictions that you want to apply. Windows Restrictions include:

- **Start Menu Restrictions**—These restrictions help you to prevent various program icons and features from appearing on the **Start** menu. Some options, such as **Command Prompt** or **Windows Explorer** will still appear on the **Accessories** menu, but the user will receive an error when selecting these items if you have restricted them.
- **General Restrictions**—Windows XP offers many additional features and programs aside from those listed on the **Start** menu that you may not want to make available to your users.

We recommend that you do not change the default restriction selections. Changing these restrictions can affect other restrictions in Windows SteadyState.

Hide Drives

On the **Windows Restrictions** tab, under **Hide Drives**, you can select which drives are visible to the user in **My Computer**. You can select the option to hide all drives, show all drives, or to select specific drives that you do not want exposed to the user, including devices such as printers or removable storage devices.

Feature Restrictions

On the **Feature Restrictions** tab, you can restrict users from accessing program attributes that could damage or clutter the computer. For example, you can use program restrictions to prevent users from adding to the Clip Organizer, disabling macro menu items, running Microsoft Visual Basic®, or running system tools and other management tools. Feature restrictions include:

- Microsoft Internet Explorer® Restrictions
- Microsoft Office Restrictions
- Home Page
- Web sites Allowed

The **Feature Restrictions** tab is organized identically to the **Windows Restrictions** tab, with restriction level options on the left and the categories and restriction options in the list box on the right. When you select the level of restrictions, options on the list of restrictions to the right will appear as selected.

Internet Explorer Restrictions

With **Internet Explorer Restrictions** you can set restrictions in Internet Explorer to remove attributes and menu options you may not want users to access. For example, you can restrict shared users from the **Favorites** menu in Internet Explorer by selecting the **Remove Favorites** menu option.

Microsoft Office Restrictions

With **Microsoft Office Restrictions** you can restrict features in Microsoft Office. For example, one of the ways that you can restrict shared users from using macros is to select both **Disable macro shortcut keys** and **Disable Macro menu items in the Tools menus**. Both of these restrictions are available under **Microsoft Office Restrictions** on the **Feature Restrictions** tab**.**

Home Page Setting

In the **Home Page** check box, you can type the Web address of the home page you want to configure for the shared user profile. This is the home page a shared user will see each time they open Internet Explorer.

Web sites Allowed

If you select the **Prevent Internet access (except Web sites below)** option under **Internet Explorer Restrictions**, you can type the address of the Web sites available to the user profile in the **Web sites Allowed** check box. To enter

multiple web addresses, separate each web address with a semicolon. For more information about parental controls and advanced Internet filtering, see Windows Live™ OneCare Family Safety at: http://go.microsoft.com/fwlink/?LinkId=83433.

Block Programs

On the **Block Programs** tab, you can select the software you want to prevent the user from accessing.

To block a program, in the left-hand list box, select the programs that that you want to block, and then click **Block** (located between the two list boxes). The selected items will appear in the Block Programs list box to the right. You can search for a program by typing the name of the program in the **Search** box. You can also browse for programs not on the list by clicking **Browse**.

To unblock a program, select the program in the **Block Programs** list box, and then click **Remove**. To unblock all programs, click **Remove All**.

When you have added the programs you want to block, click **OK**.

Testing Shared User Profiles

Before setting computer restrictions and configuring Windows Disk Protection, test the shared user profiles you have created to ensure that the configurations and restrictions are working the way you intend them to work. The **Start** menu on a sample shared user account is shown in Figure 6.

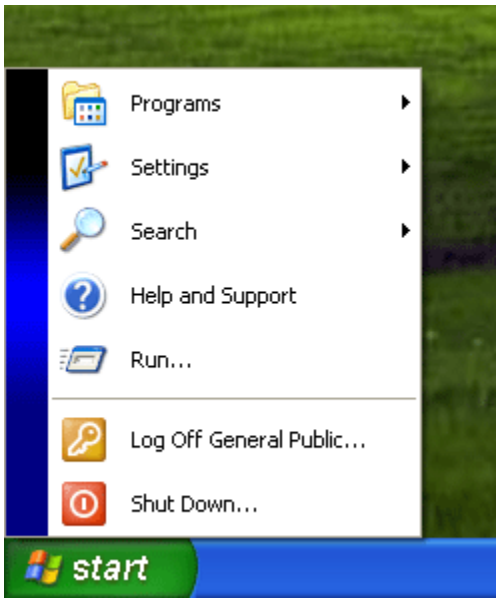

Figure 6: The Start menu on a sample shared user account.

To test a shared user account, log on to the computer with the configured shared user account and verify that:

- The **Start** menu appears correctly.
- The shortcuts on the **Start** menu and desktop work correctly.
- The programs you blocked do not appear on the **Start** menu.
- The user restrictions you have configured for the **Start** menu, desktop, and Internet Explorer are working properly.
- Session timers behave as configured.

Configuring Computer Restrictions

By configuring computer restrictions, you can also apply settings and restrictions at the system level that will enhance the privacy and security of all shared users who use the computer.

This section covers the computer restrictions that are available in the **Set Computer Restrictions** dialog box. These restrictions include:

- Privacy Settings
- Security Settings
- Other Settings

Privacy Settings

Privacy settings help you protect the privacy of all users of a shared computer. The **Privacy Settings** options in the **Set Computer Restrictions** dialog box in Windows SteadyState include:

- **Do not display user names in the Log On to Windows dialog box**—Selecting this option helps to ensure that the **User name** box in the **Log On to Windows** dialog box appears blank when a user logs off. When not selected, the name of the last user to log on appears in the **User name** box.

  Part of providing privacy to your users is helping to ensure that user names do not appear in the **User name** box when a user logs off. Although the computer has shared user profiles, you may also have private accounts on the computer for other users.

- **Prevent locked or roaming user profiles that cannot be found on the computer from logging on**—Typically, when a user logs on to a computer for the first time, Windows XP will generate a profile for that user. Selecting this option in **Set Computer Restrictions** in Windows SteadyState will prevent users without an existing profile from logging on.

- **Do not cache copies of locked or roaming user profiles for users who have previously logged on to this computer**—Selecting this option helps to improve privacy and saves disk space. A roaming user profile is one that resides on a networked system. When a user of a roaming user profile logs onto a client computer on the network, Windows XP copies the user's profile onto the client computer. Windows SteadyState prevents Windows XP from saving roaming user profiles on the local computer, which saves disk space and prevents shared users from accessing profile files that contain private information.

Security Settings

Security settings protect the computer from being compromised or damaged by user activities. The **Security Settings** options in Windows SteadyState include:

- **Remove the Administrator user name from the Welcome screen (requires pressing CTRL+ALT+DEL twice to log on to accounts not listed)**—The Windows Welcome screen lists all user account names residing on that computer. Selecting this option removes the Administrator user name from the list on this screen. To log on as Administrator, you must press CTRL-ALT-DEL twice to bring up the traditional logon screen.
- **Remove the Shut Down and Turn Off options from the Log On to Windows dialog box and Welcome Screen**—Selecting this option prevents users from shutting down or turning off the computer from the **Log On to Windows** dialog box and the Welcome screen.
- **Do not allow Windows to compute and store passwords using LAN Manager**—Selecting this option helps promote secure password storage by disabling the LanMan hash (LMHash) form of each password. LMHash is an encryption mechanism used to support backward compatibility with earlier Windows operating systems.
- **Do not store user names or passwords used to log on to Windows Live ID (requires restart of the computer)**—Selecting this option prevents Windows XP from saving users' Windows Live ID account and domain credentials and forces users to enter this information each time begin a session. This improves privacy and prevents users from logging on with the credentials of people who have previously used the computer.

Note: *If you select this option, you must restart Windows for it to become active.*

- **Prevent users from creating folders and files in drive C:**—Selecting this option changes the access control list (ACL) in the root of the system drive to prevent users from creating files and folders.
- **Prevent users from opening Microsoft Office documents from within Internet Explorer**—Selecting this option helps to ensure that Microsoft Office applications host their own documents so that the optional Microsoft Office software restriction works correctly.
- **Prevent write access to USB storage devices (requires restart of the computer)**—Selecting this option prevents users from saving files or data to USB storage devices.

Other Settings

Windows SteadyState utilizes the Windows Welcome screen to simplify the logon process:

- **Turn on the Welcome screen**—The Windows Welcome screen simplifies the logon process for users by displaying a list of all user names on that computer when Windows XP starts.

Scheduling Software Updates

Part of protecting a computer is ensuring that it is has all of the most up-to-date Microsoft Updates and antivirus information. In the **Schedule Software Updates** dialog box, you can schedule updates at a specific time of the day and at the frequency you want updates made to the shared computer. You can schedule updates and apply them permanently even when Windows Disk Protection is turned on, ensuring that important Microsoft updates and antivirus updates are not subsequently removed on restart of the shared computer.

This section covers the configurations and settings that you can apply in the **Schedule Software Updates** dialog box. These settings include:

- Scheduling automatic or manual updates
- Selecting automatic updates (Microsoft Update), antivirus updates, or custom scripts

Scheduling Updates

In the **Schedule Software Updates** dialog box, under **Schedule Updates**, you can select manual or automatic updates. After the updates have been scheduled, you can use the **Select Updates** options to select the types of updates you want to perform.

Manually Download and Install Updates

Scheduling and automating updates is not mandatory. If you want or need to install an update manually, you can do so by selecting **Manually download and install updates.** Selecting this option turns off scheduled updates to the shared computer. In addition, you must turn off Windows Disk Protection when you manually download and install updates or your updates will be cleared when the computer is restarted. Some instances in which you may want to install manual updates include:

- Installing updates spontaneously.
- Installing an update that requires your interaction, such as an update with a user agreement where you must specify that you agree to the terms.
- Installing updates to non-Microsoft software.
- Checking for recommended updates on the Microsoft Web site at: http://go.microsoft.com/fwlink/?LinkId=83424. Microsoft frequently offers enhancements and recommended changes not included as part of the critical update packages.

Caution: *If Windows Disk Protection is turned on and Remove all changes at restart is selected, any manual updates made during the session will be lost. To install manual updates, turn off Windows Disk Protection, perform the manual updates, and then turn on Windows Disk Protection so that updates will not be removed from the shared computer when you restart.*

Automatically Download and Install Updates

When you select the **Automatically download and install updates** option under **Schedule Updates**, you can specify the frequency of automatic updates. You can select a daily or weekly update, and you can select the hour of the day you want the update installed.

Note: *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 make sure that the **Retain all changes permanently** option is turned on in Windows Disk Protection. For more information, see the "Protecting the Hard Disk" section in this handbook.*

After scheduling updates, you can perform a manual update by:

- Selecting **Manually download and install updates**.
- Downloading and installing updates. To install manual updates, Windows Disk Protection must be set to **Retain all changes permanently** when manual updates are performed.
- Selecting **Automatically download and install updates** to reinstate the schedule.

Schedule Software Updates works with Windows Disk Protection to install updates by:

- Logging off any active user.
- Restarting the computer so that Windows Disk Protection can clear disk changes.
- Disabling shared user accounts to prevent unapproved disk changes from being introduced while updates are in progress.
- Turning on **Retain all changes permanently** in Windows Disk Protection to ensure that the updates are not removed the next time the computer restarts.
- Downloading and installing updates.
- Restarting the computer.
- Turning Windows Disk Protection back to **Remove all changes at restart**.

Selecting Updates

Important software updates include any Microsoft updates, security updates, or any custom updates required by applications installed on the computer.

Automatic Updates (Microsoft Update)

Select **Automatic Updates** to install operating system updates at the interval you scheduled in the previous step. Windows Disk Protection will install Microsoft Update, Windows Update, or Windows Server™ Update Services, depending on which of these is currently used by Windows XP.

Security Program Updates

Whether you are using antivirus software that Microsoft Update is capable of detecting or another program that uses a proprietary script to initiate, you can include security program updates with Windows SteadyState.

Existing Antivirus Program

You can perform security program updates automatically as part of the critical updates process if Windows SteadyState detects an antivirus or security product it knows how to update. At time of publication, Windows SteadyState currently detects and includes scripts for updating the following security products:

- Computer Associates eTrust 7.0
- McAfee VirusScan 2005
- McAfee VirusScan Enterprise 8.0
- Windows Defender

Antivirus Script

If you have an antivirus program other than those listed, you might want to prepare a signature update script for it as described in your antivirus software manual.

Custom Updates

To schedule a custom update script, click **Browse** to locate the script. The custom script will appear in the text window. Custom scripts should be tested by running Schedule Software Updates.

Custom scripts must be written so that they return only after actions in the custom script have been completed. For example, if a script launches another process and returns immediately, Schedule Software Updates will not detect the operation of the custom script process and may assume that the script has completed. This can result in partially updated files or failure of your custom script.

Important: *Custom scripts can only be used with Schedule Software Updates if they do not require any interaction from you.*

Warning: *Any users logged onto the computer when scheduled updates begin will be immediately logged off. While scheduled updates are in progress, only the Administrator or users with administrative privileges can log on. We recommend that you not log on while updates are in progress; however, if you do so, you will not be able to modify any configurations made with Windows SteadyState until the update process is complete.*

Protecting the Hard Disk

Windows Disk Protection is designed to help protect system settings and data on the partition on which Windows XP is installed from being permanently changed.

The activities performed by a user during a session cause many changes to the operating system partition. Program files are created, modified, and deleted. The operating system also updates system information as part of its normal functionality. On a shared computer, however, the goal is to create an environment of uniformity for all users. Each user who logs on should experience the same environment as all other users, and no user should be able to modify or corrupt the system. Windows Disk Protection clears all changes to the operating system partition at whatever specified interval you set.

If you choose to turn on Windows Disk Protection, you can select the disk protection level that determines when and if Windows Disk Protection clears changes to the protected system drive.

This section covers:

- Turning off, installing, and turning on Windows Disk Protection
- Attributes and configuration of the Windows Disk Protection cache file
- Choosing the level of disk protection you want on the shared computer

Windows Disk Protection Off

When Windows SteadyState is first installed, Windows Disk Protection is turned off by default and does not use any hard disk space on the system drive. When turned on, Windows Disk Protection creates a cache file to save all changes to the operating system and program files. The cache file that is created will reserve a significant amount of space on the system drive.

Windows Disk Protection should remain turned off until you are ready to use it. After you install and turn on Windows Disk Protection, turning off Windows Disk Protection will remove the cache file created upon its installation. Turning off Windows Disk Protection effectively uninstalls this protection feature.

Windows Disk Protection On

When Windows Disk Protection is turned on, it creates a cache file to retain all of the modifications to operating system or program directories. Histories, saved files, and logs are all stored in this cache file that has been created on a protection partition of the system drive. At intervals you can designate, Windows Disk Protection deletes the contents of the cache and restores the system to the state in which Windows Disk Protection was first turned on.

Installing and Turning on Windows Disk Protection

Before installing and turning on Windows Disk Protection, it is important to defragment the hard disk. If you did not perform this task during preinstallation, you should defragment the system drive and the hard disk now. Installing and turning on Windows Disk Protection on a fragmented hard disk can cause the creation of the Windows Disk Protection cache to fail.

► To install and turn on Windows Disk Protection

1. Log on as a SteadyState administrator.
2. In the **Windows SteadyState** main dialog box, under **Computer Settings**, click **Protect the Hard Disk**.
3. To turn on Windows Disk Protection, select **On**.
4. Click **Yes** to continue with the installation of Windows Disk Protection.

During installation, Windows Disk Protection will calculate the size of your hard disk and create a cache file equal to 50 percent (up to 40 gigabytes [GB]) of the free hard disk space. For example, if you have a 40-GB hard disk, and your operating system and programs use 10 GB, you have 30 GB of free space available.

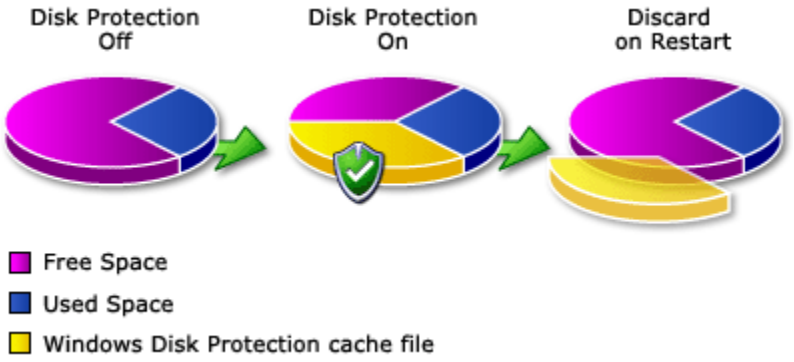

Figure 7: Illustration of cache file when Windows Disk Protection is turned on.

Clearing the Cache

When Windows Disk Protection is turned on, all changes to the hard disk and program files are cleared and the cache file is emptied at the specified interval you set. As users use the computer, the cache file fills with all changes to the operating system and program files. If the cache file fills to 70 percent capacity, the user will receive a warning message.

Windows Disk Protection created the cache file at 50 percent of the free disk space (up to 40 GB) to give shared users plenty of disk space to use. However, if the warning appears, you can clear the cache manually.

► To clear the cache

1. Have the shared user save files to a removable storage device (if possible) and log off of the computer.
2. Log on as an administrator.
3. Open Windows SteadyState.
4. Click **Protect the Hard Disk**.
5. Ensure that the **Remove all changes at restart** option is the selected.
6. Restart the computer.

The cache file is now cleared.

Resizing the Cache File

When Windows Disk Protection created the cache file, it claimed 50 percent of the free hard disk space (up to a maximum of 40 GB). We recommend leaving the cache file at the maximum size to offer your users plenty of hard disk space

in which to perform their activities. However, you do have the option to resize the cache if necessary.

When determining the cache size, you have many variables to consider. Some conditions will put the computer at greater risk of filling the cache file between restarts. You can minimize the risk of filling the cache between restarts by:

- **Removing all changes at restart**—Removing all changes at each restart of the computer is more effective if you frequently restart the computer.
- **Providing for a small number of users**—Generally, fewer users mean fewer changes to system or program files. Keep in mind, however, that a single user can sometimes perform an action which claims a large amount of hard disk space.
- **Setting a high level of restrictions**—Setting a high level of restrictions will prevent users from performing activities that claim large amounts of hard disk space. Activities such as downloading files and saving files to the hard disk can potentially take up large amounts of disk space. Both of these activities can be restricted on the **User Settings** dialog box or the **Set Computer Restrictions** dialog box

To adjust the size of the cache file, click the **Change cache file size** option, and then, on the **Change Cache File Size** dialog box, select the desired size of the cache.

Note: *The larger the cache file is, the longer it will take Windows Disk Protection to create.*

Windows Disk Protection Levels

When you select the disk protection level you are defining when and if Windows Disk Protection clears changes to the hard disk. The level of protection you select depends on how the computer is used and whether or not your users want to save data for any length of time. You can:

- Remove all changes at restart.
- Retain changes temporarily.
- Retain all changes permanently.

Remove All Changes at Restart

As shared users use the computer, the cache file fills with the changes to the operating system and program files. As a result, the longer the computer is up and running, the larger the cache file will grow. We recommend selecting the **Remove all changes at restart** option and restarting the computer daily. With more frequent restarts, a smaller cache size is required.

The **User Settings** dialog box offers you an option to restart the computer whenever a user using the shared user profile logs off. If you select this option on all of your shared user profiles, and if you also select the **Remove all changes at restart** option in the **Protect the Hard Disk** dialog box, each user will have an identical user experience. If you do not select the option to restart

after each user logs off, we recommend restarting the computer frequently to clear it of any changes collected in the cache file.

Retain Changes Temporarily

You might want to retain user files and data for a specified period of time. For example, you might have a user who is working on a project and wants to access project research files over a period of two weeks. In this case, you would select the **Retain changes temporarily** option, and then set the date and time duration. Windows Disk Protection will not erase any changes when the computer restarts until the specified date and time are reached.

When the specified date and time are reached, users receive a warning message stating that the next time the computer restarts, all changes will be cleared from the hard disk. This gives shared users an opportunity to save their files to a removable storage device before shutting down the computer.

Retain All Changes Permanently

After you turn on Windows Disk Protection, turning it off will delete the cache file, which is time consuming to create. When it is time to install patches, upgrades, or new programs, select the **Retain all changes permanently** option to prevent your modifications from being lost. Any action you perform while this option is selected will not be removed by Windows Disk Protection. Because the cache file still exists when this option is selected, you can easily return to one of the other two options without repeating the time-consuming process of turning on Windows Disk Protection.

Note: *If you have a user who wants to be able to retain changes between restarts, you can exempt the user from Windows Disk Protection by creating the user's profile on a partition other than the operating system partition. For example, if Windows XP is installed on the C drive, you can configure the user profile to reside on drive D. All of the user restrictions you want to enforce from Windows SteadyState can still be applied, but this user's data will not be subject to removal by Windows Disk Protection. If you opt to create a user profile on an alternate drive, you must remember not to lock the profile. A locked profile will remove any profile modifications no matter where it resides. For more information on locking a user profile, see the "Lock Profile" section in this handbook.*

Exporting and Importing User Profiles

After you have created shared user profiles on your shared computer, it is possible to export and import these configured user profiles to other computers on which you have installed Windows SteadyState. With the Export and Import features provided in Windows SteadyState, you can easily provide uniform shared user profiles on all of your shared computers.

This section covers:

- Exporting User Profiles
- Importing User Profiles

Exporting User Profiles

You can use the Export feature to export fully configured shared user profiles to other computers running Windows SteadyState.

► To export user profiles

1. Click **Export User**.
2. In the **Export User** dialog box, select the user profile you want to export from the **User name** drop-down list box.
3. Select the location you want to save the profile. Note that the name of the shared user profile appears in the **File name** list with an .ssu extension.
4. Click **Save**. A message appears stating that the shared user profile was successfully exported to the location you have chosen. Click **Ok**.
5. Repeat steps 1 through 5 in this procedure with each user profile you want to export.

All of the user profiles are now saved to a place where they can be imported to your shared computers running Windows SteadyState.

Importing User Profiles

Now that the shared user profiles have been exported, you can use the Import feature to import them to your shared computers running Windows SteadyState.

Note: *Make sure that Windows Disk Protection is set to **Retain all changes permanently** before importing the shared user profiles. Otherwise, Windows Disk Protection will remove them when the computer restarts.*

To import user profiles

1. If you exported the user profiles to removable storage device, insert the storage device into the appropriate drive or USB port.
2. Open Windows SteadyState.
3. Click **Import User.**
4. In the **Import User** dialog box, select the location in which you saved the exported user profiles.
5. You will see the file names of the shared user profiles in the **Import User** dialog box. Note that the name of the shared user profiles appear in the **File name** list with an .ssu extension. Select a shared user profile and click **Open**.
6. Enter the shared user profile password in the **Password** box. The user name already appears in the **User Name** box.
7. Enter the user password in the **Password** and **Confirm Password** boxes. You can enter any password which complies with Windows XP password policy requirements; however, for ease of administration we recommend that you make the password consistent on all of the shared computers in your environment. Click **OK**.

A message will appear stating that the shared user profile has been successfully imported. The shared user profile user name will now be included in **User Settings** in the **Windows SteadyState** main dialog box.

Scenarios for Advanced Administrators

This section covers common advanced scenarios that occur when you manage a shared computer environment by using Windows SteadyState. The techniques offered in this section are intended for Windows SteadyState administrators with advanced technical expertise and experience in the configuration and administration of Windows XP.

With Windows SteadyState, you can configure shared computers so that a user profile or user data is retained after the user has logged off. You have three ways to store permanent user data:

- **Redirect the My Documents folder to a USB drive or remote network drive**—Users can save data to a remote drive specified by the Windows SteadyState administrator. You must make sure that you remove any restrictions that restrict a shared user from accessing a remote drive before you modify the location where a user can save data.
- **Create permanent user profiles on a separate partition**—Create or redirect user profiles and user data to a separate partition. You can use this method to create permanent user profiles that allow users to return to their settings and saved files while still protecting the system files on the shared computer.
- **Create permanent user profiles for all accounts**—Create user profiles for all user accounts on a separate partition where they are not affected by Windows Disk Protection. If you use this method, you must customize the computer operating system installation so that the default location for user profiles is not on the Windows Disk Protection protected partition.

Redirecting the My Documents Folder

By default, Windows SteadyState saves the user's data to the My Documents folder associated with the user profile. Windows XP provides the capability to redirect the My Documents folder to a different location.

If you use Windows Disk Protection, but still want to provide users with the capability to save documents to the same location each time they log on the user profile, you can redirect the My Documents folder so that users can save data to a separate partition, a removable drive such as a USB drive, or to a mapped network drive. If you choose to save data to a separate partition, it must be a separate partition from the partition protected by Windows Disk Protection.

Before you redirect the My Documents folder to a different location, make sure that the Windows SteadyState environment is properly configured for the redirection of user data.

► To configure Windows SteadyState for the redirection of user data

1. Restart the computer to clear recent disk changes.
2. Log on to the shared computer and start Windows SteadyState.
3. Click **Protect the Hard Disk**, verify that Windows Disk Protection is turned on and that the **Retain all changes permanently** option is selected, and then click **OK**.
4. Under **User Settings**, click the user profile for which you want to redirect the My Documents folder.
5. Turn off all restrictions for the user profile.
6. Restart the computer for Windows Disk Protection to save changes.

► To redirect the My Documents folder

1. Log on to the user profile for which you want to redirect the My Documents folder.

Note: *If you are redirecting user data to a USB drive, follow Step 2. If you are redirecting user data to a separate partition or to a network drive, proceed directly to Step 3.*

2. If you are saving user data to a USB drive, insert the USB drive into the USB port of the shared computer.
3. Click **Start**, right-click **My Documents**, and then click **Properties**.
4. In the **My Documents Properties** dialog box, click **Move**.
5. In the **Select a Destination** dialog box, select the drive where you want to save user data, and then click **OK**.
6. In the **My Documents Properties** dialog box, click **OK**.
7. In the **Move Documents** dialog box, click **Yes** to move the documents or **No** to leave the existing documents in the old location.
8. Log off the user profile and then log on as the Windows SteadyState administrator. If you turned off any user restrictions when you configured Windows SteadyState for the redirection of user data, reset those restrictions now.
9. Restart the computer for Windows Disk Protection to save changes.
10. Log on as the administrator.
11. Click **Protect the Hard Disk**, verify that Windows Disk Protection is turned on and that the **Remove all changes at restart** option is selected, and then click **OK**.

Creating Permanent User Profiles on a Separate Partition

You may want to permanently store the changes a user makes to their preferences and settings during the logon session. You can create unlocked user profiles on a partition separate from the Windows Disk Protection protected partition so that the environment settings a user is allowed to make during a session are not cleared when they log off the shared computer.

For information on creating all user profiles for all accounts on a separate partition each time a user profile is created, see the "Creating Permanent User Profiles for All Accounts" section in this handbook.

Note: *If you have Windows SteadyState installed on a drive with multiple partitions, the partition on which Windows SteadyState resides is the protected system partition. If you are setting up a separate partition after you have installed Windows SteadyState, you should defragment your hard drive before running disk partitioning software. When you run any disk partitioning software with Windows SteadyState installed on the shared computer, you must turn off Windows Disk Protection before you defragment the drive to avoid damaging the cache file created by Windows Disk Protection.*

We recommend that you defragment your hard disk drive and set up any separate partitions you may require before you install Windows SteadyState.

► To create a user profile on a separate partition

1. Log on as the administrator.
2. Click **Start**, point to **All Programs** and then point to **Windows SteadyState**.
3. Under **User Settings**, click **Add a New User**.
4. In the **User Name** box, enter the user name for the profile you want to create.
5. In the **Password** box, type the password for the user account. Ensure that the password you choose meets the password policy requirements. Enter the password in the **Confirm Password** box.
6. In the **User Location** box, select the drive on which you want to save the new user profile, and then click **OK**.

After a user profile is created on a partition separate from the Windows Disk Protection protected partition, the profile remains on that unprotected partition until the Windows SteadyState administrator deletes the user profile. If you later decide that the user profile should no longer be permanent, the protected user profile cannot be copied or moved to another Windows partition. If you want the same user profile to reside on the Windows Disk Protection protected partition so that user changes are cleared when the user logs off or restarts the computer, you must create a new profile with the desired restrictions on the protected partition.

► To delete a permanent user profile

1. Under **User Settings**, select the user profile you want to delete.
2. Click **Delete User**. You will be asked if you are sure you want to delete the user's account. If you are sure that you want to delete the user account, click **OK**.

After the user account is deleted, you can recreate the user profile on the desired partition or on the Windows protected partition. Be aware that after the user profile is created on the Windows partition, the profile is no longer permanent and any changes made to the user's environment will not be saved.

Creating Permanent User Profiles for All Accounts

If you want to ensure that all of the user profiles created for all accounts are placed on a partition where they are not affected by Windows Disk Protection, you must customize the computer operating system installation so that the default location for user profiles is not on the Windows Disk Protection protected partition.

The only supported way to change the default location for all user accounts 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 directs Windows to automatically create profiles on a separate partition and overrides the default system drive location for user profiles when they are created by Windows SteadyState.

Answer files are text files that contain responses to some, or all, of the queries that occur during the installation process. After creating an answer file, called Unattend.txt, you can apply it to as many computers as necessary. It can also be included in scripts that automate installation on multiple computers.

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 "Automating and Customizing Installations" in *Windows XP Resource Kit*. The answer file you create by using Setup Manager can include other information, such as the time zone and network settings.

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

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

Customizing Individual User or Administrative Accounts

We recommend that you limit the actions of users on a shared computer by restricting the profiles for shared user accounts as discussed in the "Configuring the Shared User Profile" section of this handbook. Through the use of shared

user accounts, administrators can ensure that users will not be able to access any administrative tools and privileges that may allow them to make unwanted changes to the operating system or to the programs installed on the shared computer.

There are applications that you may want to allow users to run that will require enhanced access to the shared computer.

Creating a Restricted Shared Administrative Account

For users to run applications that are not designed to run on Windows XP, a restricted shared administrative account can be created for the purpose of operating nonstandard software, such as Internet-based and network-based multiplayer games. Some older educational programs also require more administrative access than is allowed with a typical Windows SteadyState user account with a restricted shared user profile.

For a list of non-Microsoft programs that do not work with typical Windows SteadyState shared user accounts, see Microsoft Knowledge Base Article #307091 at: http://go.microsoft.com/fwlink/?LinkId=83434.

A restricted shared administrative account is an unlocked user profile in which most restrictions have been removed. This type of unrestricted user account allows access to the increased permissions necessary to run nonstandard applications.

Before you create a shared administrative account for general users, consider the following questions:

- Can the nonstandard software can be upgraded to or replaced with a version that runs correctly with limited user privileges on Windows XP?
- Can the software be removed from your environment with a limited effect on your business needs?

If the answer to either of the preceding questions is “no,” you can create a restricted shared administrative account.

Note: *If the shared computer is connected to a network, network policy might prevent you from completing this procedure if you are not an administrator of the network domain.*

► To add a shared user account to the Administrators group on the computer

1. Log on as the Windows SteadyState administrator. You must also be logged on as an administrator or a member of the Administrators group to add a shared user account to the Administrators group on the computer.
2. Click **Start**, and then click **Control Panel**.
3. In **Control Panel**, double-click **User Accounts**.

4. On the **Users** tab, under **Users for this computer**, click the shared user account that you want to add to the Administrators group, and then click **Properties**.
5. On the **Group Membership** tab, select the **Other** option, choose **Administrators** from the drop-down list, and then click **OK**.

After the shared user account has been added to the Administrators group, use Windows SteadyState to restrict the shared administrative account access to all programs and settings, with the exception of the increased permissions that are necessary to run nonstandard applications.

Important: *Removing restrictions on a user account to open up administrative access for non-Microsoft software can increase exposure to security risks associated with allowing unrestricted accounts in Windows SteadyState, and may produce an unstable environment on the shared computer.*

► To restrict a shared administrative account

1. Log on as the Windows SteadyState administrator.
2. Click **Start**, point to **All Programs** and then point to **Windows SteadyState**,
3. On the **Windows SteadyState** main dialog box, under **User Settings**, click the shared administrative user profile you created.
4. On the **General** tab, under **General Settings**, select the **Lock profile to prevent the user from making permanent changes** box.
5. On the **Windows Restrictions** tab, select the **High restrictions** option. Under **Start Menu Restrictions** in the list, you may want to leave all of the restrictions selected; clearing any of the restrictions may create a security risk for the shared computer. However, for individual nonstandard applications you can turn off some of these restrictions.
6. In the **Hide Drives** section, select the drives you want to hide from the restricted administrative user.

For security on the shared computer, you may want to configure the following restrictions to limit a restricted administrator's access to system files and program folders:

- On the **Windows Restrictions** tab, under **General Restrictions** in the list, select the **Disable Notepad and WordPad** check box. This will prohibit the restricted administrator user account from modifying critical scripts and batch files to bypass security.
- On the **Windows Restrictions** tab, under **Start Menu Restrictions**, select the **Prevent programs in the All Users folder from appearing** check box and the **Remove the Help and Support icon** check box. This will prevent programs from appearing on the **Start** menu when the restricted administrative user is logged on.

- On the **Feature Restrictions** tab, click the **Microsoft Office Restrictions** check box. This will prohibit the restricted administrator from running Microsoft Office programs that are unrelated to nonstandard applications that they are running.

Specifying a Different Language for User Profiles

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

MUI is useful for Windows SteadyState administrators who manage shared computers in a large organization or on an enterprise level, and who want to provide alternate language resources for their users. The MUI is sold only through Microsoft Volume Licensing programs such as the Microsoft Open License Program (MOLP/Open), Select, and Enterprise agreement.

MUI Pack Requirements

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

MUI is sold only through Microsoft 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 to ensure that customers have the English version of the operating system running on their computers before they install MUI.

Configuring Windows SteadyState for MUI Installation

The input language can be configured for the computer when text is entered by using the keyboard. With multiple languages configured, a user can switch between languages as required. You can add an input language in a user profile as long as you have installed the appropriate language from MUI.

Before you add an input language to a user profile, make sure that the Windows SteadyState environment is properly configured for the addition of the language.

► To prepare Windows SteadyState for MUI installation

1. Log on as administrator.
2. Click **Protect the Hard Disk**, verify that Windows Disk Protection is turned on and that the **Retain all changes permanently** option is selected, and then click **OK**.
3. Under **User Settings**, click the user account for which you want to change the user input language.
4. Turn off all restrictions for the user account.

5. Install the MUI.

   For more information about the requirements and installation of the Windows MUI Pack, see the MSDN® article at: http://go.microsoft.com/fwlink/?LinkId=83435.

6. Log off as Windows SteadyState administrator to save changes to the computer.

Changing the User 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.

► To add an input language for a user profile

1. Log on to the specific user account for which you want to change the user input language.
2. Click **Start**, and then click **Control Panel**.
3. In **Control Panel**, double-click **Regional and Language Options**.
4. In the **Regional and Language Options** dialog box, click **Languages**, and then, under **Text Services and Input Languages,** click **Details**.
5. In the **Text Services and Input Languages** dialog box, choose the user input language you want to add to the user's profile from the list under **Default input language**. You can add additional services for the selected input language under **Installed services**.
6. When the input language has been added, log off the user account and log on as the Windows SteadyState administrator.
7. Reset the restrictions you want on the user profile you have just modified.

Installing Windows SteadyState on Multiple Computers

When you install Windows SteadyState 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:

- **Configuring a reference computer**—Configure a computer that you will use to replicate the Windows SteadyState installation image on other computers in your environment. Follow the installation instructions in the "Installing Windows SteadyState" section of this handbook to prepare your reference computer for disk imaging and installation on multiple computers.
- **Preparing the reference computer with the System Preparation Tool**—After Windows SteadyState is installed, user profiles have been created, and security and critical updates have been installed, use the System Preparation Tool (Sysprep) to prepare the computer for imaging

(optional). You can find Sysprep on the Windows XP Operating System CD. For more information on the use of Sysprep, see Microsoft Knowledge Base Article #302577 at: http://go.microsoft.com/fwlink/?LinkId=83437.

- **Creating an image of the reference computer**—Create an image of the reference computer hard disk and transfer that image to the hard disk of other computers. There are several non-Microsoft disk imaging software applications that can be used for this task. For more information about disk duplication of Windows XP installations, see Microsoft Knowledge Base Article #314828 at: http://go.microsoft.com/fwlink/?LinkId=83438.
- **Transferring and setting up the image on multiple computers**—After the disk image has been transferred to multiple computers, a Mini Setup Wizard will start that validates and activates Windows XP for use on the new computer.
- **Turning on Windows Disk Protection on All Shared Computers**—After the disk image has been transferred to other computers and after you have confirmed that all user profiles are in place on each shared computer, turn on Windows Disk Protection.

Configuring a Reference Computer

We recommend that you configure a reference computer that will be used to create the master disk image for multiple installations of Windows SteadyState by setting up your reference with a clean installation of the operating system. For more information on preparing your computer for Windows SteadyState installation, by using Windows Disk Protection, creating user accounts, and configuring user profiles, see the “Installing Windows SteadyState” section of this handbook.

Preparing the Reference Computer with 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 requirement, Windows XP Professional provides a tool called the System Preparation Tool (Sysprep) 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 can use a disk duplication tool to create a disk image. The disk image is a compressed file that contains the contents of the entire hard disk on which the operating system is installed.

Sysprep can be used to prepare a reference computer with Windows SteadyState for disk imaging. You can then replicate the disk image on multiple computers with the same or similar hardware configurations.

When you run Sysprep on a computer with Windows SteadyState, ensure that all user profiles are unlocked before running the tool. Sysprep.exe does not recognize locked or mandatory profiles and will copy a new Ntuser.dat file into the <user> folder. Additionally, Sysprep.exe creates a new user SID. After

running Sysprep.exe, existing Windows SteadyState user profiles (Ntuser.man) become invalid as they are no longer linked to the new SIDs.

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 Microsoft Software License Terms, regional options, user name and company, and product key.

You can further automate the imaging process by including a special answer file named Sysprep.inf with your master image. Sysprep.inf is an answer file that automates the Mini Setup Wizard. It uses the same INI file syntax and key names (for supported keys) such 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 Sysprep, see the following resources:

- For an overview of the process of imaging clients, including the use of Sysprep to prepare a system for imaging, see: http://go.microsoft.com/fwlink/?LinkId=83440.
- For information about how to customize Sysprep installations, see: http://go.microsoft.com/fwlink/?LinkId=83441.

Creating an Image of the Reference Computer

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 non-Microsoft imaging tool to create an image of the computer hard disk.

For more information about disk duplication of Windows XP installations, see Microsoft Knowledge Base Article #314828 at: http://go.microsoft.com/fwlink/?LinkId=83438.

Transferring and Setting up the Image on Multiple Computers

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, you must complete the following tasks:

- **Activating Windows**—For more information about activating Windows, see Microsoft Knowledge Base Article #302806 at: http://go.microsoft.com/fwlink/?LinkId=83442.
- **Validating Windows XP**—You can validate Windows through the Windows Genuine Advantage Web site at: http://go.microsoft.com/fwlink/?LinkId=83431. If you used Sysprep to prepare the computer for imaging, you will be required to validate Windows again before using Windows SteadyState.

Turning on Windows Disk Protection on All Shared Computers

After your disk image has been installed on all shared computers, you will want to turn on Windows Disk Protection to protect the system drive and save the unlocked user profiles on each computer. Make certain that the **Retain all changes permanently** option is selected for every computer when you are configuring system drive restrictions. Otherwise, Windows Disk Protection will remove the newly installed unlocked user profiles when each computer restarts.

For more information about exporting and importing user profiles, see the "Exporting and Importing User Profiles" section in this handbook.

Using Windows SteadyState with Active Directory and Network Domains

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 by 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 an environment for centrally managing user accounts that require access to network resources. In this environment, users must log on with the same credentials on multiple computers, as many educational institutions require. For these reasons, Windows SteadyState has been designed to work as favorably in domain environments as it does for workgroup computers.

Please note that most of the settings and restrictions available in Windows SteadyState are also available through the Group Policy template (SCTSettings.adm) provided with Windows SteadyState. When considering the installation of Windows SteadyState on shared computers that are connected to a domain network, Group Policy is more effective than using Windows SteadyState for restricting multiple user accounts across numerous computers on a domain network.

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 computer account password to authenticate with the domain and gain access to domain resources. By default, the domain-joined computer initiates a change to the computer 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 capable of accessing 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 helps keep 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 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 (SMS), can provide the flexibility to schedule software updates to occur at any time, but with Windows Disk Protection, software updates must be scheduled at specific times.

If your organization requires regularly changing the schedule for software updates, instead of 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 have a situation in which central software distribution and Windows Disk Protection can work together.

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

Creating a Mandatory Profile for Multiple Users

Mandatory user profiles are roaming user 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 to the master mandatory profile and a user can access that profile on any shared computer that is connected to a the network. The potential disadvantage of mandatory profiles is that the shared computer must have network access for a user to log on. If the shared computer cannot access the network, mandatory user profiles are unavailable and users cannot log on.

► To create a mandatory profile for multiple users

1. Create a shared folder on a network server that will store mandatory profiles.
2. Create a subfolder in that shared folder for each mandatory user profile you want to use.
3. Click **Start**, and then click **Control Panel**. In **Control Panel**, double-click **Administrative Tools**, and then double-click **Computer Management**.

4. In **Computer Management**, click **Local Users and Groups**, and then double-click **Users**.
5. For each user account that will use the mandatory profile, right-click the account and then click **Properties**.
6. In **Properties**, click **Profile**, and then, in **Profile** path, type the network path to the shared folder where the mandatory profile is saved (for example, *server1**profiles**user1*).
7. Create, configure, and restrict a user profile in Windows SteadyState and then copy that user profile to the appropriate network shared folder.
8. In the network shared folder, in the profile folder, rename the Ntuser.dat file to Ntuser.man. This changes the user profile from a simple roaming profile to a mandatory profile.

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

- For general information about roaming and mandatory profiles, see "User profiles overview" in the Windows XP Professional Product Documentation at: http://go.microsoft.com/fwlink/?LinkId=83443.
- For steps on how to assign a mandatory profile to a user account in Windows XP, see Microsoft Knowledge Base Article # 307800 at: http://go.microsoft.com/fwlink/?LinkId=83444.

Creating User Restrictions for Unrestricted Domain Accounts

Some organizations must 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 CD or DVD creation labs or other types of dedicated computer kiosks.

Similarly, operators may want 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 during an initial logon (usually caused by tampering, such as the well-timed removal of a network cable).

Note: *If you copy the Default User folder to the NETLOGON shared folder on a domain controller, the settings and restrictions of this default profile will apply to all domain users 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.*

All of these scenarios can be addressed by setting restrictions on the Default User profile in Windows SteadyState. The Default User profile is then used as the 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.

Note: *It is advisable to create a backup of the Default User profile before you customize the profile for use on the domain. To do this, make a copy of the Default User folder located in the Documents and Settings folder.*

► To create a custom Default User profile

1. Log on as the Windows SteadyState administrator.
2. Create a new local user profile.
3. Log off and then log on as the local user that you just created.
4. Customize the user settings and environment. 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 Windows SteadyState administrator.
6. Configure and apply restrictions for the newly created user 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 and must be visible 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 **\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**.

After the Default User profile is customized, Windows XP assigns the 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 customized Default User profiles along with Windows Disk Protection to clear the new user profiles that are created on the Windows partition with each restart of the computer.

Creating Group Policy Restrictions with SCTSettings.adm

Windows SteadyState includes a Group Policy template called SCTSettings.adm in the bin folder commonly located under \\Program Files\Windows. This template reproduces most of the settings included in Windows SteadyState **Feature Restrictions** tab of the **User Settings** dialog box, and can be used to deploy restrictions to users who are members of an Active Directory domain.

Group Policy for a domain can be configured either with the Group Policy Management Console, an add-in 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 user accounts on shared computers.

The SCTSettings.adm Group Policy template included with Windows SteadyState also includes the capability to set idle and mandatory logoff timers, if Windows SteadyState is installed on your computers.

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

► To use Active Directory Users and Computers to manage Windows SteadyState restrictions

1. Start Active Directory Users and Computers on a computer running Microsoft Windows Server™ 2003 by clicking **Start**, and then clicking **All Programs.**
2. Click **Administrative Tools**. In Active Directory Users and Computers, right-click the organizational unit (OU) for which you want to configure policy, and then click **Properties**.
3. On the **Group Policy** tab, select 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, commonly located in C:\Program Files\Shared Computer Toolkit\bin.
6. Browse the settings in the **All Windows SteadyState Restrictions** folder and note their similarity to the program and user restrictions settings in Windows SteadyState. Descriptions are given for each setting.
7. Make any restrictions changes that you want and then exit Group Policy Editor.

Note: *We recommend 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.*

Group Policy Software Restriction Policies

Windows SteadyState provides administrators with an effective way to restrict software, especially for a single shared computer or for a small environment of shared computers. However, when administrators want to centrally manage software restrictions across many computers or users, we recommend that you set software restrictions by using Group Policy Software Restriction Policies. Software restrictions that are implemented by using Software Restriction Policies across a large number of shared access computers on a given site, domain, or range of organizational units are more efficiently administered than the restrictions that can be implemented by using Windows SteadyState.

Software restrictions that can be applied by using Software Restrictions Policies are identical to those restrictions that can be applied in Windows SteadyState.

For more information on using Group Policy Software Restrictions Policies, see: http://go.microsoft.com/fwlink/?LinkId=83445.

Duplicating Software Restrictions by Using Software Restrictions Policies in Windows XP

If you want to use Software Restrictions Policies in Windows XP to directly duplicate the Windows and program restrictions settings that a Windows SteadyState administrator can configure, create the path rules defined in the following sections. Optionally, you can also restrict Notepad and WordPad and prevent Microsoft Office programs from running using Software Restriction Policies.

For example, to duplicate the effect of the **Allow only programs in the Program Files and Windows folders to run** feature in the **Windows Restrictions** tab in Windows SteadyState, use a Software Restriction policy to set the Software Restriction Policy Security Level to **Disallowed**, and then create additional rules to unrestrict or allow each of the following paths, as shown in Table 6.

Table 6: Software Restriction Rules

Rule	Description
%ProgramFiles%	Allows programs to run
%Windir%	Allows Windows programs to run
*.lnk	Allows **Start** menu and desktop shortcuts to work

As an added security measure, you can also create an additional path rule that restricts files from being run in the Temp folder. To restrict users read/write permissions to the Temp folder, add the following rule by using Software Restrictions Policies.

```
%WinDir%\Temp
```

For more information on using Group Policy Software Restrictions Policies, see: http://go.microsoft.com/fwlink/?LinkId=83445.

Configuring Restart After Log off by Using a Logoff Script

When a computer running Windows XP is joined to a domain, it is more difficult to ensure changes are cleared between user logon sessions. If you use Group Policy and Software Restrictions Policies, use a logoff script to reproduce the **Restart computer after log off** option, commonly located under General Settings in Windows SteadyState.

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

1. Open the Group Policy Object for the domain or OU 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.

Note: *You can use the shutdown command in a batch file to restart the computer. At the command prompt, type the following 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 Windows SteadyState to restart the computer.

Appendix A: Windows SteadyState Glossary

Included in this glossary are definitions for the terms, phrases, and feature names that are commonly associated with Windows SteadyState and are used throughout this handbook.

Active Directory

The Windows-based directory service. Active Directory stores information about objects on a network and makes this information available to users and network administrators. Active Directory gives network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with an intuitive, hierarchical view of the network and a single point of administration for all network objects

administrator

The person responsible for administering use of a shared computer system, communications system, or both. A system administrator performs such duties as assigning user accounts and passwords, establishing security access levels, allocating storage space, and watching for unauthorized access.

antivirus update

A periodic update from software manufacturers to their antivirus software.

Automatic Updates

A feature that works with the Windows Update Web site to deliver updates (patches and fixes) for Windows as they become available according to settings that users can choose.

Block Programs List

A tab in the **User Settings** dialog box used to block a given user from accessing listed programs.

cache

Generally, a file used to store information temporarily. Windows Disk Protection utilizes a cache file to store changes made to system and profile files during user sessions. This cache file is emptied of contents at intervals, depending on how Windows Disk Protection is configured.

clear

To erase or empty the cache file on the hard disk when a user logs off or the computer is restarted (only when Windows Disk Protection is turned on).

computer restrictions

Settings that limit operating system functionality, including privacy and security.

critical update

A broadly released fix for a specific problem addressing a critical, non-security related issue or bug.

custom update

Update, patch, or upgrade to software other than those available through Microsoft Update.

defragmentation

The process of rewriting parts of a file to contiguous sectors on a hard disk to increase the speed of access and retrieval. In Active Directory, defragmentation rearranges how the data is written in the directory database file to compact it.

disable

To deactivate or turn off.

domain

A collection of computers in a networked computer environment that share a common domain database and security policy. A domain is administered as a unit with common rules and procedures, and each domain has a unique name.

drive restrictions

Feature on the **Windows Restrictions** tab of the **User Settings** dialog box that allows administrator to select which drives on the computer are accessible and visible to the users of the shared user profile.

enable

To activate or turn on.

export

To output data and database objects to another database, spreadsheet, or file format so another database, application, or program can use the data or database objects. You can export data to a variety of supported databases, programs, and file formats.

Family Safety

A feature set in Windows Vista that allows parents and individuals to customize key aspects of their online and computing experience as they feel appropriate for their child or themselves (specifically, people they interact with and information they see).

Feature Restrictions

Settings that limit customer use of, or access to, specific feature attributes and commands.

imaging

The process of capturing an installation of Windows for deployment to one or more destination computers.

import

To bring information from one system or program into another. The system or program receiving the data must somehow support the internal format or structure of the data.

kiosk

A freestanding computer or terminal that provides information to the public, usually through a multimedia display.

lock

To allow the shared user profile configuration set by the administrator to remain static from one user session to another.

locked user profile

A user account whose user profile settings return to a state defined by Windows SteadyState every time a user logs on to the account; no matter where the user profile settings are physically located.

mandatory user profile

A user profile that is not updated when the user logs off. It is downloaded to the user's desktop each time the user logs on, and it is created by an administrator and assigned to one or more users to create consistent or job-specific user profiles. Only members of the Administrators group can change profiles.

Microsoft Update

A Microsoft Web site that provides updates (patches and fixes) for multiple Microsoft products in one place, including Windows operating system software and Windows-based hardware, Microsoft Office system, Microsoft SQL Server™, and Microsoft Exchange Server.

notification

A message or announcement sent to the user or administrator of a system. The recipient may be a person or an automated notification manager.

notification area

The area on the taskbar adjacent to the system control area that contains icons that appear when certain events occur, such as when you receive e-mail.

partition

A portion of a physical disk that functions as though it were a physically separate disk. After you create a partition, you must format it and assign it a drive letter before you can store data on it. On basic disks, partitions are known as basic volumes, which include primary partitions and logical drives. On dynamic disks, partitions are known as dynamic volumes, which include simple, striped, spanned, mirrored, and redundant array of independent disks (RAID)-5 volumes.

privacy settings

Settings that allow the administrator to control the collection, use, and distribution of personal data.

protected partition

A partition on a shared computer whose state is made static by Windows Disk Protection.

public computer

A computer in a public environment that is accessed by several different users on a daily basis. Often this type of computer is utilized as a public access computer, Internet kiosk, lab computer, or instructional computer.

remote management

For an administrator, the process of managing Windows Disk Protection in Windows SteadyState from a remote computer through Active Directory Group Policy.

restrict

To block access to a program or operating system functionality.

restricted user

A user account that has settings or restrictions applied by Windows SteadyState.

restriction

A setting that blocks access to program or operating system functionality.

restriction level

A pre-defined set of program restrictions that are automatically applied.

retain

When Windows Disk Protection is turned on, to keep (not erase) the cache file on the hard disk when a user logs off or the computer is restarted.

roaming user profile

A server-based user profile that is downloaded to the local computer when a user logs on and that is updated both locally and on the server when the user logs off. A roaming user profile is available from the server when logging on to a workstation or server computer. When logging on, the user can use the local user profile if it is more current than the copy on the server.

Schedule Software Updates

Feature in Windows SteadyState used to set schedules for software and operating system updates. Tool works in conjunction with Windows Disk Protection to ensure that updates are saved permanently.

Security Center

Windows launch point to manage security settings for automatic updates, internet options, or Windows Firewall.

security settings

Settings used to specify privacy, security, and logon configurations for Windows.

session countdown

Feature on the General tab of User Settings that allows the administrator to display the session countdown interface to alert users of how much time is left before the end of their sessions.

session timer

Feature on the General tab of User Settings that allow the administrator to set session limits and display attributes.

shared access computer

A computer in a public environment that is accessed by several different users on a daily basis. Often this type of computer is utilized as a public access computer, Internet kiosk, lab computer, or instructional computer.

shared user account

A single user account that is logged on to by multiple users.

shared user profile

A file that contains configuration information for a specific user including settings and restrictions applied by Windows SteadyState. Each user's preferences, such as desktop settings, persistent network connections, and application settings, are saved to a user profile that Windows uses to configure the desktop each time a user logs on.

Start Menu Restrictions

Settings that allow the administrator to restrict **Start** menu attributes.

System Preparation Tool (Sysprep)

The tool that prepares an operating system for imaging. Sysprep removes system-specific settings and other data that should not be copied to a destination computer. Sysprep also resets the Windows installation to start Windows Welcome or in audit mode.

unallocated disk space

Unpartitioned and unformatted space on a hard disk.

unlock

Allows the shared user profile configuration set by the administrator to be modified by users from one session to another.

unlocked user profile

A user account whose settings that are changed in a user session are retained every time the user logs on to the account.

user

A person working with software on a computer; a computer operator.

user icon, picture

Picture associated with shared user profile in Windows SteadyState.

user profile

A file that contains configuration information for a specific user, such as desktop settings, persistent network connections, and application settings. Each user's preferences are saved to a user profile that is used to configure the computer each time a user logs on.

User Profile Hive Cleanup Service (UPHClean)

A service that helps to ensure user sessions are completely terminated when a user logs off. System processes and applications occasionally maintain connections to registry keys in the user profile after a user logs off. In those cases the user session is prevented from completely ending.

User Settings

Windows SteadyState feature used for configuring shared user profiles.

Windows Disk Protection

A feature that helps protect the Windows partition that contains the Windows operating system and other programs from being permanently modified from user session to user session. After Windows Disk Protection is installed, the administrator can choose to retain all changes, retain changes for a specified duration, or to remove all changes to the Windows partition at each computer restart.

Windows Genuine Advantage (WGA)

A program for licensed Windows software that provides access to updates, value-added downloads, free software trials, and special promotions.

Windows Live ID

A single set of sign-in credentials (e-mail address and password) that provide user access to Windows Live ID sites and services.

Windows Restrictions

Restricts user access to programs, settings, **Start** menu items, and locks shared local user profiles against permanent changes.

Windows SteadyState

A software application that is used by administrators of one or more public shared computers to help maintain computer reliability and stability from one user session to the next.

Windows Update

A Microsoft Web site from which Windows users can install or update device drivers. By using an ActiveX® control, Windows Update compares the available drivers with those on the user's system and offers to install new or updated versions.

workgroup

A grouping of computers organized to allow users to access and share resources, such as printers and shared folders, within the specified group. Workgroups in Windows do not offer the centralized user accounts and authentication offered by domains.

Index