

Protect computers with Windows SteadyState (Part 1)

If you have ever managed shared computers such as computers in schools, public libraries, Internet cafés, computer stores, etc., you might know how difficult it is to keep nh

Jakob H. Heidelberg

In Part 1 of this series, I will give you a brief introduction about Windows SteadyState (WSS). By looking at the latest version, compared to the pre-existing version, system requirements, Windows Disk Protection (WDP) and how to get started. In the following sections we will learn more about the classes of this useful toolkit. However, first of all, let's focus on the basic components.

Shared computers

If you have ever managed shared computers such as computers in schools, public libraries, Internet cafés, computer stores, etc., you might know how difficult it is to keep These computers run stably as well as security at a high level and are upgraded promptly without the need for too much work. What we need for computers of this type is a solution that enables hard drive protection to avoid unauthorized changes - except for necessary changes (such as updates).

Maybe you, like me, have also tried hardware solutions with some hard disk controller operations in the system / boot section, then a hidden partition is used every time you reboot. This is a good solution, though we face a problem when upgrading computers such as Windows Update, Office Update and updates to antivirus software, . In this case, computers must be started in 'manager' or 'admin' mode before any changes can be made.

You may have tried downloading tons of local Group Policy settings to avoid unauthorized operations with system settings, Start Menu & Desktop options, etc., making your computer more secure. However you will not feel secure enough with this scenario - perhaps partly because of the fact that all local users are having problems because of the limitations of similar local policies, even like administrators and support members. To improve that situation, Microsoft has provided a solution for administrators to help deal with some common problems. The toolkit is called Windows SteadyState - no additional hardware required . you only need one download, some mouse clicks and support to complete the system protection.

What's new here?

If you've ever dealt with the issues mentioned above, you may have tried the Microsoft Shared Computer toolkit, which is a pretty good set of tools. Windows SteadyState is an enhanced version of this toolkit - it allows for easier installation, configuration, and administration.



Figure 1

Some new features are added to the toolkit

1. The new user interface has table navigation that allows you to easily manage shared computers with one console
2. Windows Disk Protection allows you to set up and install without changing the drive's partition.
3. The Windows Disk Protection currently supports Group Policy, so you can manage it in an Active Directory environment.
4. Software restriction options allow for more rigorous control over which programs can be used.
5. There are more options to restrict users, including significant improvements to Internet Explorer control.
6. High, medium and low security defaults allow for easier and faster customization
7. Import and export easily restrict users directly from the interface without using command line tools.
8. Installation is easier and there are many supporting documents that make it easy to get started.

With such great enhancements, let's put together a solid foundation and the most important technology with Windows SteadyState for Windows XP: Windows Disk Protection!

Windows Disk Protection (WDP)

WDP may be the main reason why Windows SteadyState is such an essential tool. This feature is designed to protect system and data settings on the Windows partition. During the login process, there may be many changes made to the system by the user and the system itself. On a shared computer, the goal is to create a tight environment, this boot needs to be completely identical to another boot - no difference for the user.

When Windows Disk Protection is enabled, it deletes all changes to the operating system partition. The most common scenario is to remove all changes when rebooting. With this setting, Helpdesk only requires the user to restart the computer, and as such these computers will be restarted with the previous state unless a hardware error occurs.

WDP is not a default feature because you as well as an administrator may want to adjust the system, install applications, create users . before activating this important feature - unless you want to repeat those jobs forever.

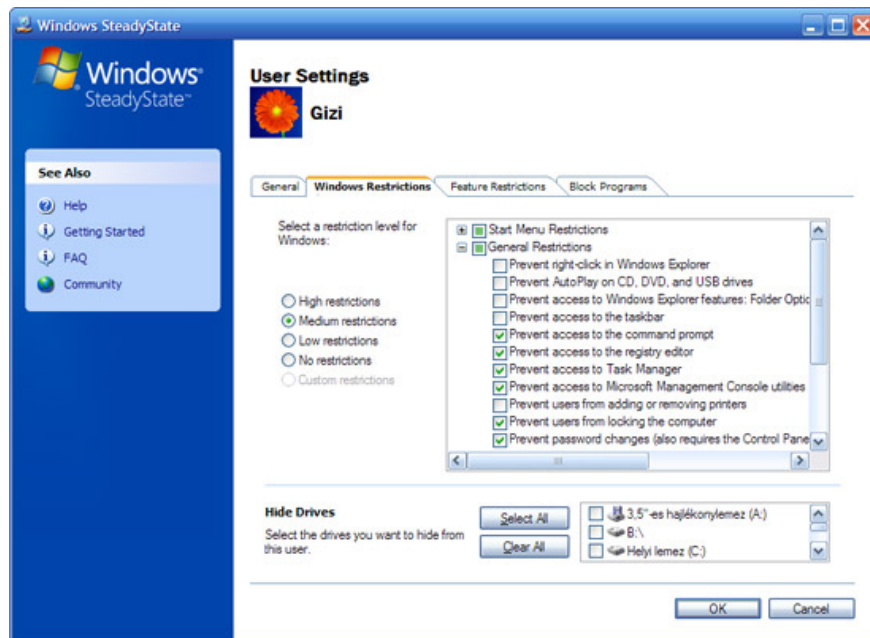
When you are ready to use it and the system is also 100% ready to perform production tasks (eg, defragmenting and deleting temporary files has been completed .), turn on this feature and track changes. that you do not want from other users. They all can't do anything with those adjustments!

Behind the script, WDP creates and stores a large archive file (at least 2GB) to save changes to the operating system and program files. It requires at least 4GB of disk space that is not used on the Windows partition to create an archive file, but the default size is approximately 50% of the available disk space.

During the restart process - WDP deletes the contents of the cache and restores the system correctly with the enabled state. If you want to allow users to save information to Desktop folders, Documents . you can do so by defining the user profile as a profile that is not locked on another partition (because WDP only protects operating system partition file).

The same functionality is available with many solutions for hardware controllers - so why is WDP better? The reason to answer this question is that you can schedule and apply them permanently even when WDP is turned on.

With Windows SteadyState, if you appropriately configure important Microsoft updates and antivirus software upgrades are not removed when the computer is restarted. The system will execute the logout of any user during the schedule upgrade, restart, and perform necessary updates. We will return to this issue in the next article.



System requirements

Systems running Windows SteadyState must have the minimum configuration required as shown in Table 1 below:

Ingredient

Request

CPU 300MHz or higher

Minimum 233MHz (one CPU or dual system); Intel Core / Pentium / Celeron or AMD K6 / Athlon / Duron series or compatible processor. 128MB RAM or higher memory

Minimum 64 MB is supported but may limit performance and other features. 1.5GB **hard** disk space is available without Windows Disk Protection (WDP), 4.0 GB of disk space is available when WDP is available. Windows XP Professional, Windows XP Home Edition, or Windows XP Tablet PC Edition operating system with Windows XP Service Pack 2 (SP2)

Note :

Windows SteadyState does not work with Windows Vista. This is a limitation but hopefully the next version will overcome this phenomenon. NTFS **file** system (Windows system will be nearly insecure when not in this mode) Windows Scripting and Windows Management Instrumentation (WMI) tools. Access **Permissions** as Administrator

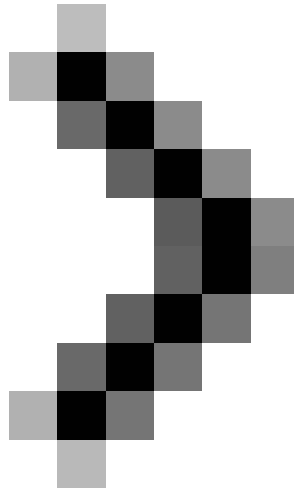
Table 1

Other requirements are to pass the Windows Genuine Advantage test.

Conclude

We introduced you to the best features that Windows SteadyState can provide administrators with shared computers. We also introduced the new version and its improvements, introduced the system requirements. Consider the extensive link section - what you need when you start .

Try using this great set of tools, maybe on a virtual computer to start the test. Once you have seen the effects it brings, then deploy with the real system.



Part 2: Protect computers with Windows SteadyState

You finished reading the article "**Protect computers with Windows SteadyState (Part 1)**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.