

System Restore

System Restore is a feature of Windows XP that allows you to restore your computer to a previous known working state in the event of a problem. This is done without loss of personal files or data such as word processing documents, spreadsheets, music, images, etc. This feature is enabled by default and runs in the background making backups after certain events happen on your computer. System restore functions are only available to an administrator of the computer, therefore if you are not an administrator, you will not be able to follow this tutorial.

System Restore protects your computer by creating backups of vital system configurations and files. These backups are known as restore points. These restore points are created before certain events take place in order to give you a recourse in case something bad happens during that event. These events are as follows:

- If you install a new application and that application's installation program is compliant with the System Restore API, which most are these days, then a new restore point will be created.
- Installation of Microsoft security and OS updates will trigger a Restore Point creation.
- If you choose to use system restore to restore to a previous restore point, system restore will create a new restore point prior to restoring a previous state in case something goes wrong.
- Before a Microsoft Backup Utility Recovery operation.
- Before installing an Unsigned driver.
- By manually creating a new restore point.
- By default at a 24 hour interval a new restore point will be made. This restore point will only be made if the system is in an idle state.

If system restore is disabled and then reenabled a new restore point will be made. These restore points contain configuration and settings and files that are necessary for your computer to run correctly. The following are some of the settings and files that are saved in a Restore Point:

- Registry (Contains Configuration information for application, user, and operating system settings)
- Windows File Protection files in the dllcache folder. (Used for protecting system files)
- COM+ Database
- Windows Management Instrumentation Database
- IIS Metabase (Contains configuration for Internet Information Server)
- Files with extensions listed in the Monitored File Extensions list in the System Restore section of the Platform SDK
- Local Profiles

What System Restore does not store in a Restore Point include:

- Windows XP passwords and hints are not restored. This is done so that you do not by accident restore an old password and then lock yourself out of the computer..
- Microsoft Internet Explorer and Content Advisor passwords and hints are not restored.

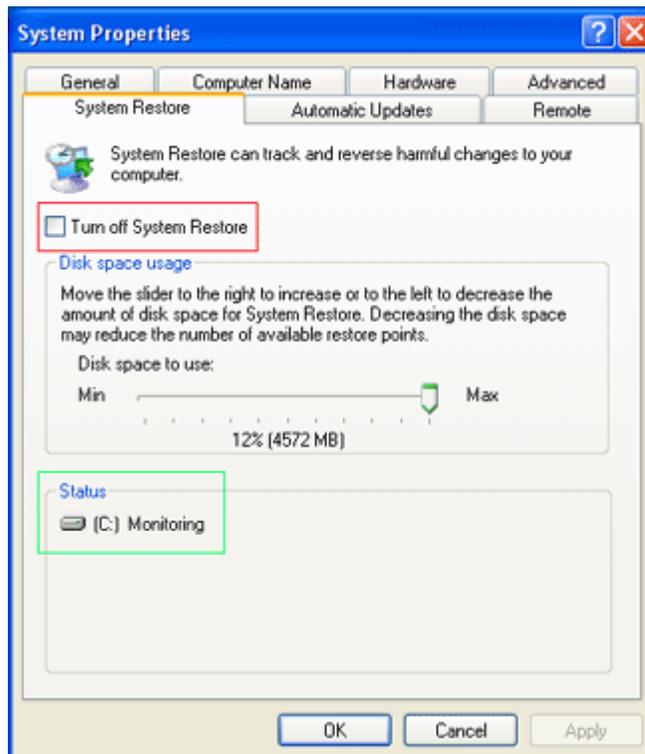
- Any file types not monitored by System Restore like personal data files e.g. .doc, .jpg, .txt etc.
- Items listed in both Filesnottobackup and KeysnottoRestore (More on that later)
- User-created data stored in the user profile
- Contents of redirected folders

Disabling System Restore

NOTE: You need to be logged in as an Administrator to administer System Restore. If you are not logged in as an administrator you will not be able to follow these steps

WARNING: By disabling system restore you will delete all stored restore points.

You should first go into the Control Panel and then double click on the System icon. If you are in the control panel and do not see the System icon, click on the link that says "Switch to classic view" in the upper left hand side of the window. Now you should be able to see the System icon. After you double click on it you should then click on the System Restore tab.

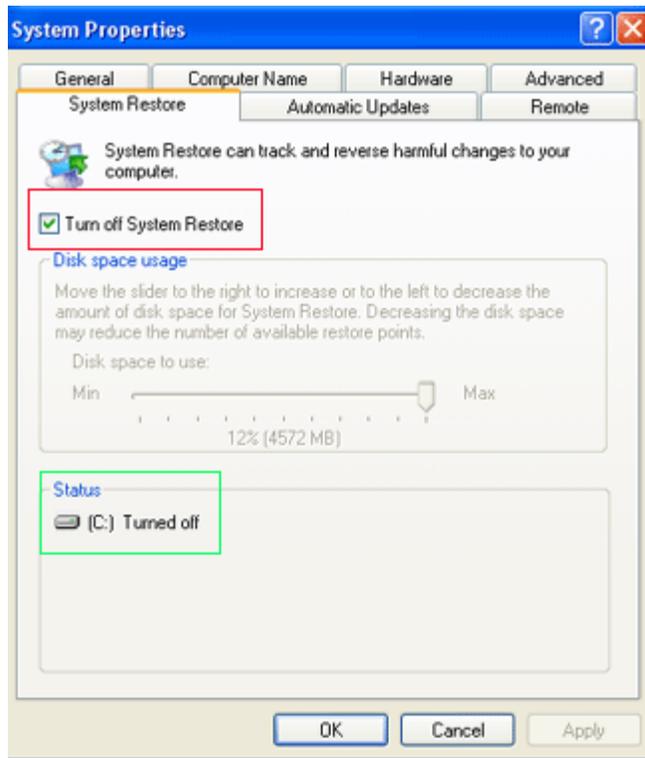


Enabling System Restore

NOTE: You need to be logged in as an Administrator to administer System Restore. If you are not logged in as an administrator you will not be able to follow these steps.

To enable system restore you should follow these steps.

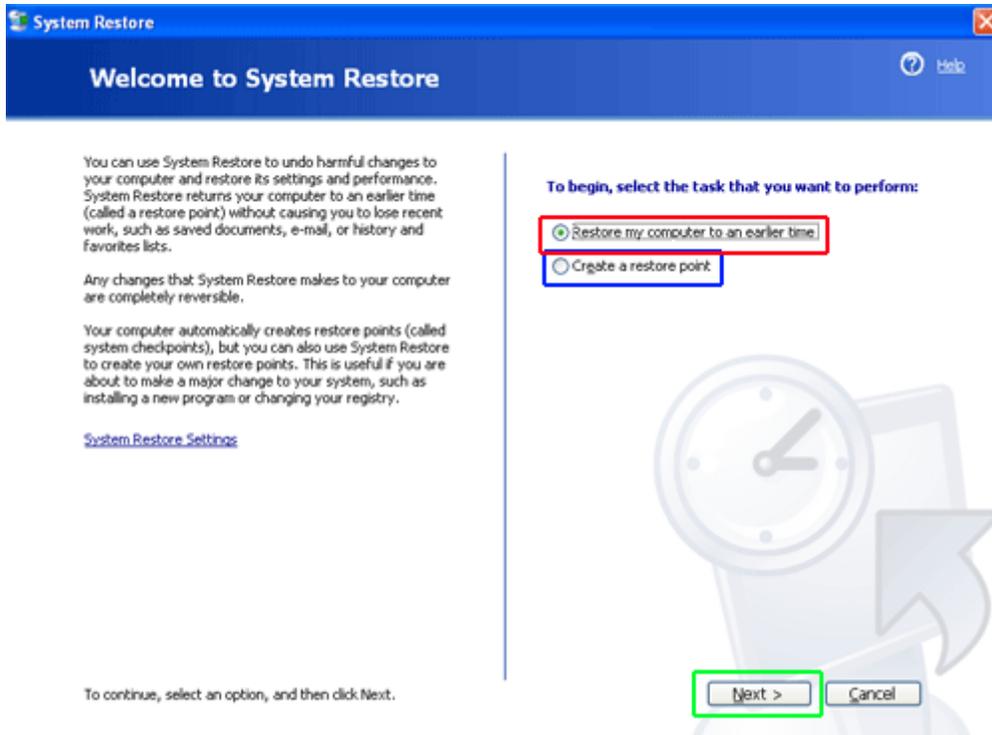
By default system restore is enabled on Windows XP machines, so there is a good chance that it is already enabled if this is your first time working with system restore. You should first go into the Control Panel and then double click on the System icon. If you are in the control panel and do not see the System icon, then click on the link that says "Switch to classic view" in the upper left hand side of the window. Now you should be able to see the System icon. After you double click on it you should then click on the System Restore tab.



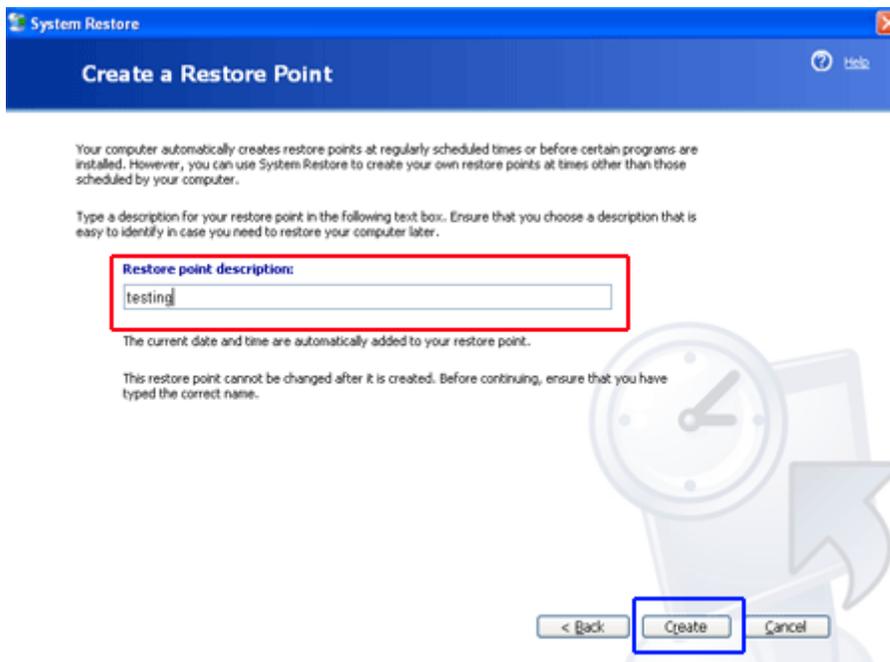
Manually Creating Restore Points

It is possible to manually make restore points when you wish by using the System Restore utility. Common reasons to do this are because you feel you have your computer set up perfectly and would like to save that state in case something goes wrong in the future.

To open the utility, go to your System Tools group under Accessories in your Programs menu. Then click on the System Restore icon



To create a manual restore point select the radio dial labeled "Create a restore point", designated by the blue box, and press the Next button.



At this point you should type the name you would like this restore point to be referred as in the field designated by the red box. The current date and time will automatically be appended to the name you choose. When you are done, press the Create button designated by the blue box. System restore will create the restore point .

Restore Point Created

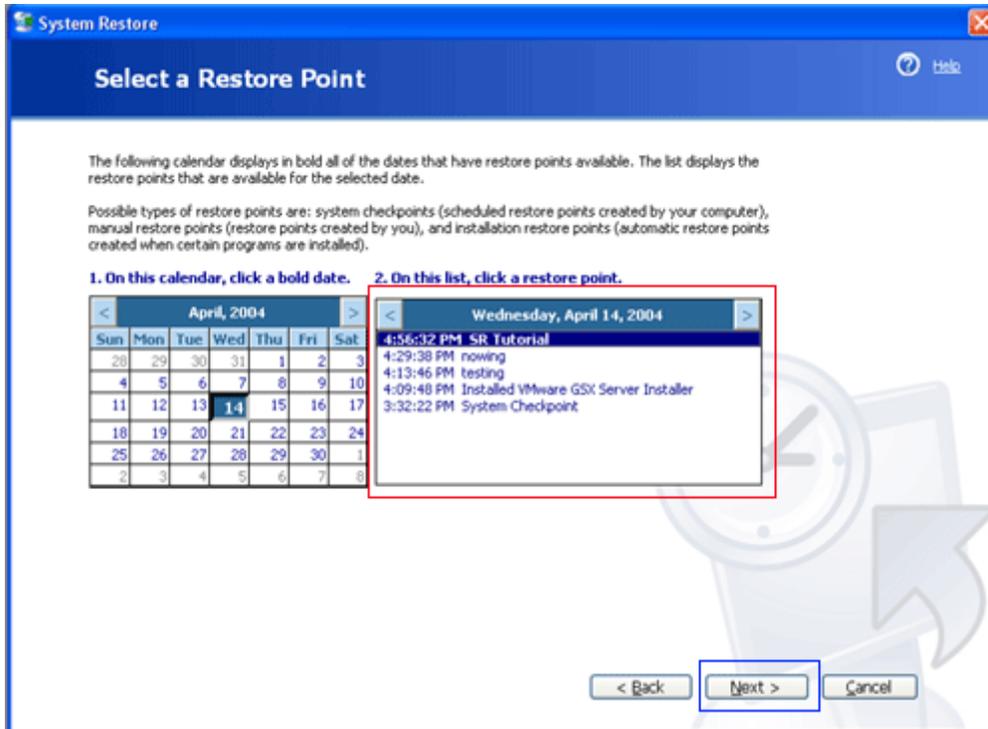
New restore point:

**Wednesday, April 14, 2004
4:13:46 PM testing**

Restoring Windows XP to a previous State

To restore Windows XP to a previous restore point you need to open the System Restore Utility. To open the utility, go to your System Tools group under Accessories in your Programs menu. Then click on the System Restore icon. You will be presented with a screen similar to Figure 3 above.

You should select the radio button that is labeled "Restore my computer to an earlier time", which is designated by the red box. When that is selected press the Next button.



At this point you should select a restore point that you would like to restore. If a particular day has any restore points created on it the date will be in bold. You can then select the restore point by clicking once on its name, as designated by the red box in Figure 6 and then pressing the Next button.

At this point you will be prompted with a confirmation as to whether or not you want to continue. If you do want to continue, you should press the Next button again, otherwise press cancel. System restore will then shut down all open applications and reboot the computer.

After the computer is rebooted you will see a screen that contains information as shown below.



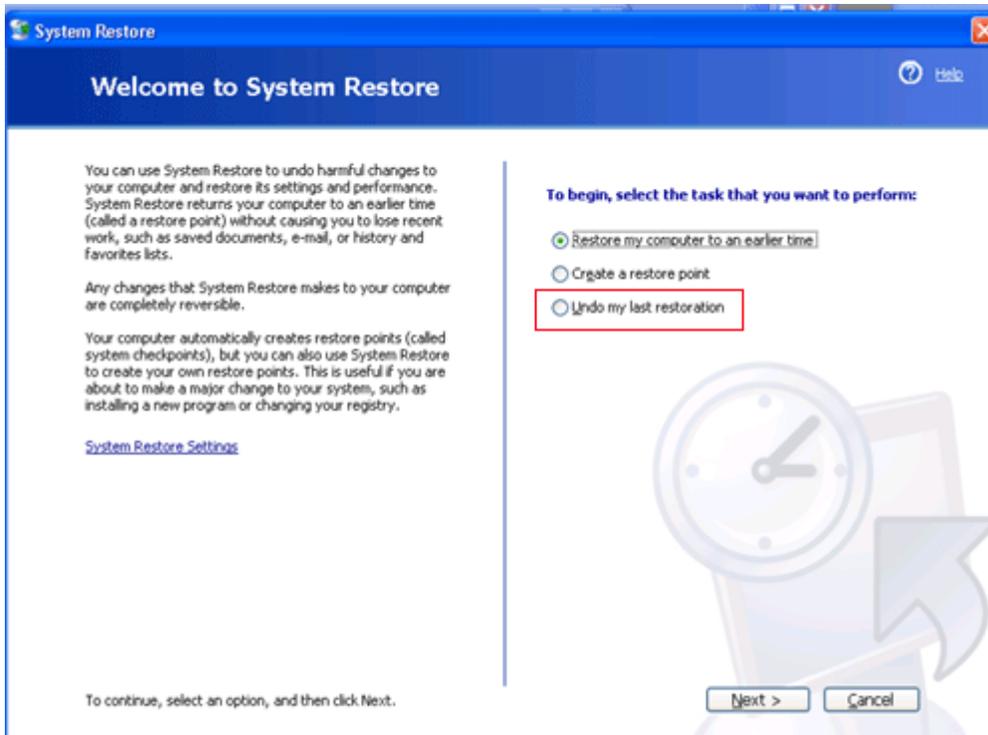
Your computer has been successfully restored to:

Wednesday, April 14, 2004
SR Tutorial

If this restoration does not correct the problem, you can:

- Choose another restore point
- Undo this restoration

If there are any problems with your computer since you restored to this restore point, you can revert back to your previous settings by going back into the System Restore Utility and selecting the "Undo my last restoration" radio button and pressing the Next button



[Deleting Restore Points](#)

There are three known safe ways to delete restore points stored on your computer. These ways are described below:

Disk Cleanup - Launch the Disk Cleanup tool and then select the more options tab. On this tab you will find a section for System Restore. If you press the Clean Up button for that section, Windows will delete all restore points except for the most recent one.

Turn off System Restore - Just by turning off System Restore all your restore points will be deleted. Unless you want this to happen, be careful that you don't mistakenly delete all your restore points by disabling system restore.

System Restore runs out of storage space - If system restore runs out of the storage space that has been allocated towards its use, it will delete the oldest restore point in order to create space for the new restore point.

[The Registry Keys and Values for the System Restore Utility](#)

You can also specify what registry keys should not be restored and what files should not be backed up by System Restore.

These registry keys are:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\BackupRestore\FilesNotToBackup
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\BackupRestore\KeysNotToRestore

The System Restore application is a powerful tool for keeping your Windows Installation running smoothly and safely. If you use this feature you will be guaranteed to have a valid restore point to revert to if any issues arise in the future. Care must be taken, though, when using this application so that damaged or infected files are not restored to your computer and cause you to be reinfected. With caution in mind when using System Restore you should not have these problems.