

Windows XP System Restore

Melissa Wise

(Reprinted From WindowsItPro Magazine)

Microsoft OSs have typically included utilities that help you recover systems that become unstable or crash, but Windows XP's System Restore goes much further. System Restore reinstates the registry, local profiles, the COM+ database, the Windows File Protection (WFP) cache (wfp.dll), the Windows Management Instrumentation (WMI) database, the Microsoft IIS metabase, and files that the utility copies by default into a Restore archive. You can't specify what to restore: it's all or nothing.

Understanding System Restore

System Restore's purpose is to return your system to a workable state without requiring a complete reinstallation and without compromising your data files. The utility runs in the background and automatically creates a restore point when a trigger event occurs. Trigger events include application installations, AutoUpdate installations, Microsoft Backup Utility recoveries, unsigned-driver installations, and manual creations of restore points. The utility also creates restore points once a day by default.

System Restore requires 200MB of free hard disk space, which the utility uses to create a data store. If you don't have 200MB of free space, System Restore remains disabled until the space becomes available, at which point the utility enables itself. System Restore uses a first in/first out (FIFO) storage scheme: The utility purges old archives to make room for new ones when the data store reaches a set limit.

The file types that System Restore monitors are many but include most of the extensions that you typically see when you install new software (e.g., .cat, .com, .dll, .exe, .inf, .ini, .msi, .ole, .sys). Note that only application installations that use a System Restore restorept.api-compliant installer will trigger the creation of a restore point.

Typically, system recoveries are easiest when you know *or think you know* what caused the problem (e.g., a recently installed device driver). In some cases, System Restore might not be the best choice for correcting a problem you're experiencing. System Restore changes many different files and registry entries, and in some cases might replace too much and actually cause more problems than it solves. For example, say you install Office XP, which triggers System Restore to create a restore point, and the software suite works great. Later in the day, you download and install an updated video driver, and because the driver is signed, the installation doesn't trigger System Restore to create a restore point. Now your system hangs on occasion, and you believe that the video driver is the culprit. In this case, you should use the Device Driver Rollback utility because it will address the device-driver problem only and not change anything else on your system. System Restore would roll your computer back to a preOffice XP state, and you would have to reinstall the entire software suite after you resolved the driver problem.

Creating a Restore Point

Windows XP automatically creates restore points when you would typically need them most. However, occasions arise when you might want to create restore points manually*for example, if you're installing an application that you're not sure will be stable on Windows XP, if you're unsure whether an application is System Restore restorept.api-compliant, or if you're making system changes that could affect the system's stability.

For example, I wanted to install Crystal Decisions' Crystal Reports Professional 7, but because that version is several years old, I wasn't sure how well it would run on Windows XP. I decided to create a restore point before installing the software. I clicked Start, All Programs, Accessories, System Tools, System Restore. A Welcome screen appeared, and System Restore asked whether I wanted to

Windows XP System Restore

Melissa Wise
(Reprinted From WindowsItPro Magazine)

restore or create a restore point. I chose Create a restore point and clicked Next. I named my restore point Before Crystal Reports, as Figure 1 shows, and clicked Create.

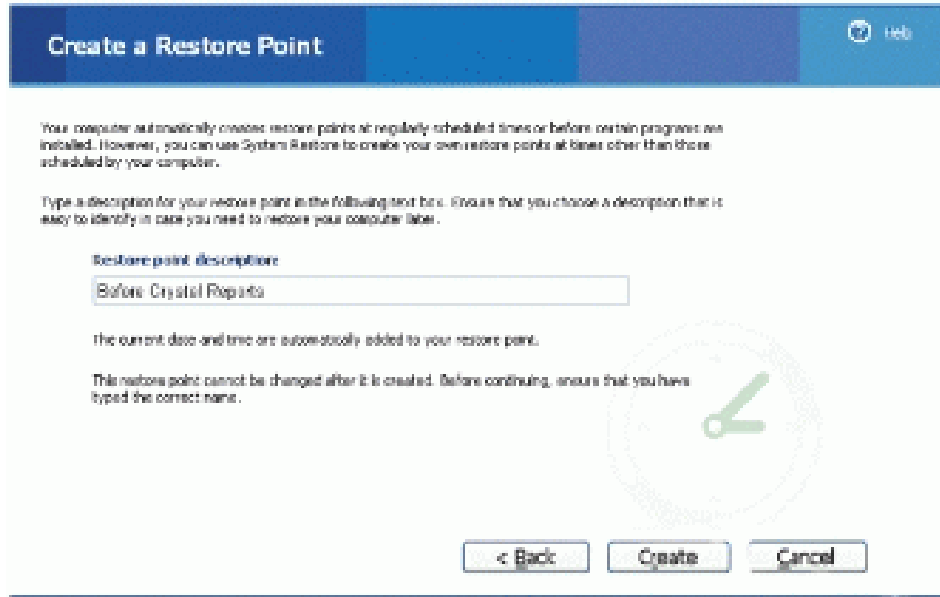


Figure 1

Name restore points so that you can easily identify them later. After the utility collected all the information it needed, it displayed the Restore Point Created screen, which Figure 2 shows. I closed the utility to end the process.

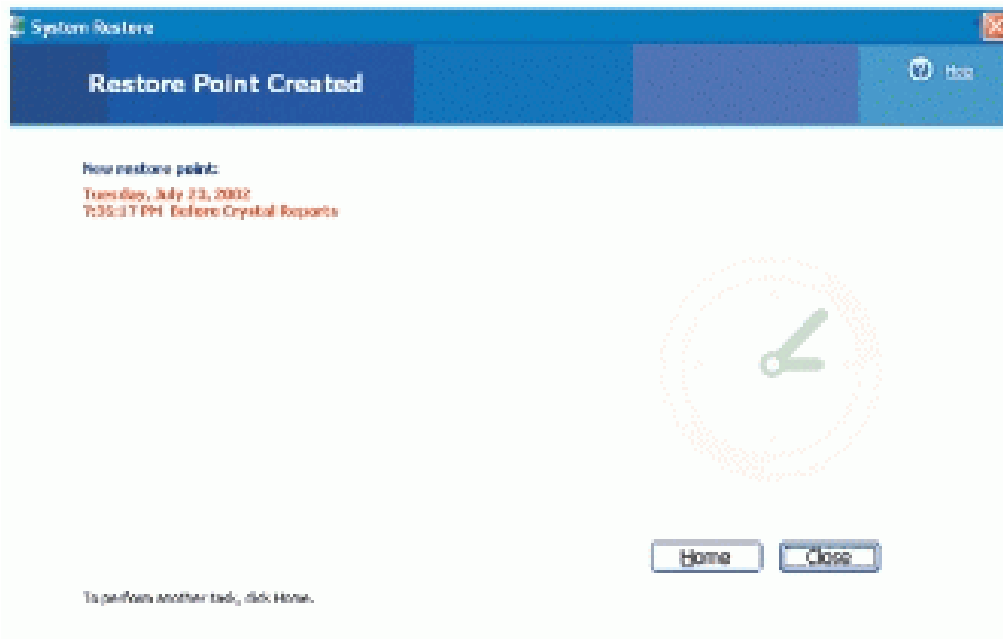


Figure 2

Windows XP System Restore

Melissa Wise
(Reprinted From WindowsItPro Magazine)

Restoring a System

Having created a restore point, I could install Crystal Reports on my Windows XP machine with the confidence of knowing that I could restore my system if anything went wrong. During the installation, several error messages reported that the system couldn't find a particular DLL. The installation finished, and Crystal Reports didn't start. I was immediately glad that I'd created the restore point.

Before performing a restore, I used the Crystal Reports uninstallation program to try to delete the application's program files and registry entries, but the procedure overlooked one registry entry. Instead of deleting the registry entry manually, which could destabilize the system, I decided to use System Restore to restore the registry safely.

I started the System Restore utility. At the Welcome screen, I chose Restore my computer to an earlier time, then clicked Next. To prompt me to select a restore point, the utility presented the various options in a calendar format, which Figure 3 shows. The calendar format lets you click through dates and see the existing restore points. Restore points that System Restore creates appear as System Checkpoint.

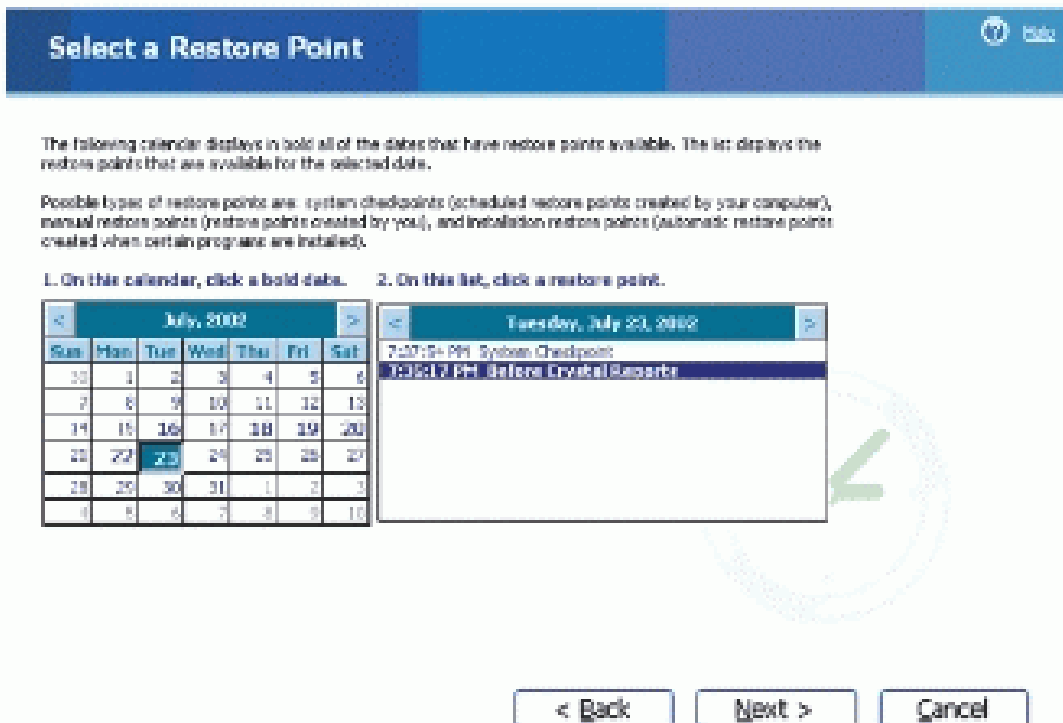


Figure 3

I clicked July 23 and saw the Before Crystal Reports restore point that I had created earlier. I selected that restore point and clicked Next, then confirmed the restore point selection and clicked Next again. System Restore closed all programs and proceeded with the restoration. The computer then rebooted. I logged back on, and the Restoration Complete screen appeared to let me know the restore was finished and had succeeded, as Figure 4 shows.

Windows XP System Restore

Melissa Wise
(Reprinted From WindowsItPro Magazine)

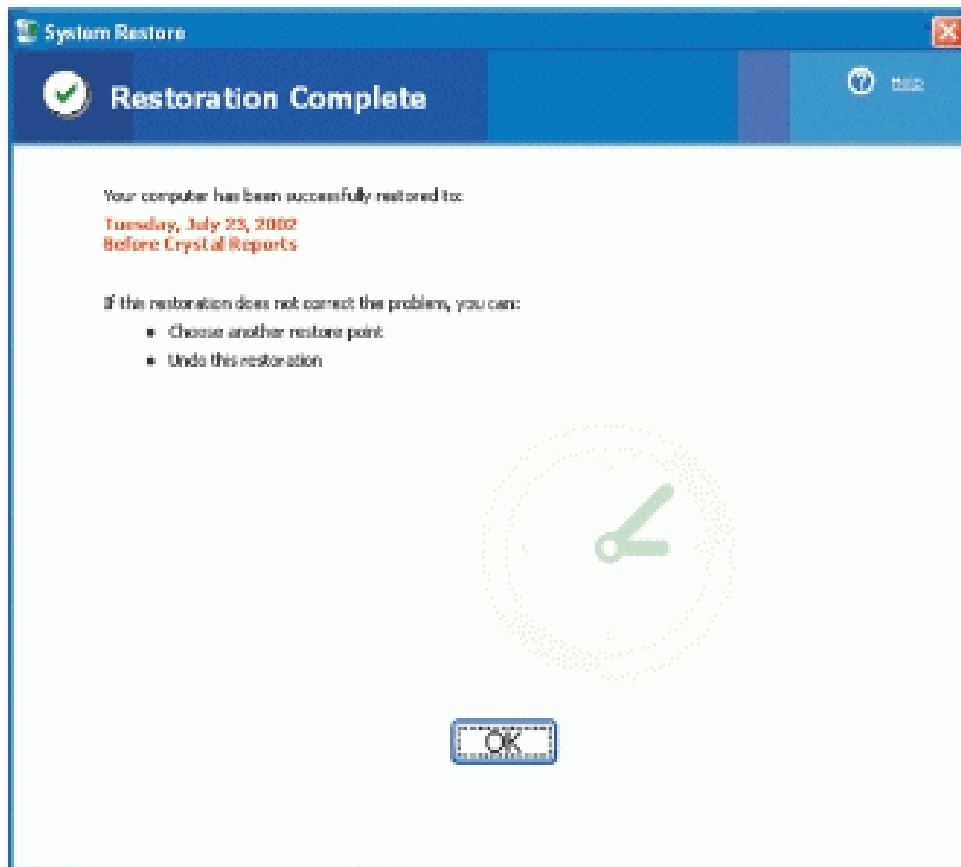


Figure 4

I then checked the hard disk and the registry and found no sign of Crystal Reports. In addition, the files I created between installing and restoring my system remained on my system. My data files were safe, and the system was stable.

If your system no longer boots to the OS, start the computer and press the F8 key as Windows begins to run. When the Windows Advanced Options menu appears, choose Last Known Good Configuration and press Enter. If the damage isn't too bad, a boot menu will appear, and you can select Microsoft Windows XP, then press Enter. Windows XP will restore the computer to the most recent restore point. If a restoration fails to resolve a problem, System Restore lets you try to select another restore point or undo the restoration. So, if you chose the wrong restore point earlier, you get a chance to correct your mistake. Remember, performing a restore is one of the events that triggers the system to create a restore point. Now you know why.

Troubleshooting

I've found System Restore to be stable and reliable. However, as with most programs, you might occasionally experience problems with System Restore. Should you need to disable it, you can do so (for details, see the sidebar "Disabling System Restore"). But first, try troubleshooting:

- Read any error messages and address any issues that the messages identify.

Windows XP System Restore

Melissa Wise

(Reprinted From WindowsItPro Magazine)

- Check your hard disks for free space. You must have at least 200MB of free space on each disk on which you've enabled System Restore. You can use the Disk Cleanup utility to reclaim space. If necessary, you can also use this utility to delete all but the most recent restore point.
- Confirm that the System Restore service is running.
- Try to run the utility in Safe mode.
- Check the System log for any errors that relate to sr or srservice.

If these steps don't help, run srdiag.exe to troubleshoot further. Srdiag creates a .cab file, which it places in the \%windir%\system32\restore folder by default. You can double-click the file or right-click it and choose Extract. You can then examine the 14 extracted files to troubleshoot your problem.

System Restore's scope, ease of use, and reliability are impressive. It's a useful utility that power users, technical support staff, and administrators should familiarize themselves with. System Restore has the potential to significantly reduce administrator work and user downtime.