

Registry backup and restore

NOTE: On some systems these actions are only available to those with Administrator privileges. *These directions are intended for individuals with extensive experience and some obvious steps are left out.* This is intended as a quick reference for those who have a malware infection and can't access the usual system or online help sources.

Registry backup and restore

The Windows Registry is simply the configuration database. Malware alters the registry, but a mistake in editing it can destroy the system. Therefore, you should have a backup before editing the Registry. Even though this backup will contain the malware entries, the system will start if you have to use it. System State Data is essentially the same thing as Registry data.

Windows comes with Regedit.exe, an editor you can run from the command line:

- Go to Start | Run, type *regedit* , and press [Enter].
- Choose File, Export, and then check Export Range ALL and save the file.

This is a good reference backup, especially if you print a hard copy. However, you may not be able to import some long Registry Keys so it may not be suitable for restoring the Registry.

Windows 95

If you use Cfgback.exe, not all settings will be restored properly. These are Microsoft's directions for a full backup and restore:

1. Restart in Safe mode.
2. Go to the command line and enter these commands:

```
cd windows  
attrib -r -h -s system.dat  
attrib -r -h -s user.dat  
copy system.dat *.bu  
copy user.dat *.bu
```

To Restore:

1. Restart in Safe mode.
2. From the command line enter these commands:

```
cd windows  
attrib -r -h -s system.dat  
attrib -r -h -s system.da0  
attrib -r -h -s user.dat  
attrib -r -h -s user.da0  
ren system.dat system.daa  
ren system.da0 system.da1  
ren user.dat user.daa  
ren user.da0 user.da1  
copy system.bu system.dat  
copy user.bu user.dat
```

You can also use the Windows 95 Emergency Recovery Utility tool.

Windows 98, 98SE, and Me

Use the Windows Registry Checker utility, Scanregw.exe. This will not run in Safe mode because it runs in extended memory but restore will run in Safe mode. Go to Start | Run and type *scanregw*.

To restore, open an MS-DOS window and run *scanregw* with the */restore* switch. Remember, you can't open a CMD line like you can with later versions.

Windows NT

Registry backup and restore is very complicated: Go to Microsoft Knowledge Base Article 128731, "HOWTO: How to Back Up the Windows NT Registry" (<http://support.microsoft.com/default.aspx?scid=kb;en-us;128731>), and copy it.

Windows XP

To back up Registry (must be logged on as Administrator):

1. Go to Start | All Programs | Accessories | System Tools | Backup | Advanced Mode (unless it goes directly to Advanced Mode which happens if the Always Start In Wizard Mode box isn't checked).
2. Select Backup Wizard (Advanced), then Next.

3. Select Only Back Up The System State Data.
4. Select Browse to choose a destination and Cancel if you get an Insert Disk message.
5. Choose Desktop as the destination, choose a file name, and begin backup. To restore the Registry, use the Restore Wizard (Advanced) and select System State.

Windows 2000

Full Registry backup and restoration procedures are basically the same as XP: To back up Registry (must be logged on as Administrator):

1. Start, Programs, Accessories, System tools, Backup, then click on the Backup Wizard button.
2. Select Backup Wizard Advanced, then Next.

3. Select Only back up the System State Data
4. Select Browse to choose a destination and Cancel if you get an Insert Disk message.
5. Choose Desktop as the destination, choose a file name, and begin backup. To restore registry, use the Restore Wizard (Advanced) and select System State.