

# Wiping swap files

[lus mentis](#)

**ABSTRACT:** On many multi-tasking systems, a swap file is used to emulate RAM. The swapfile contains data from programs that are currently running. This data may include personal files as well as passwords. To avoid leaking this data, wiping the swapfile is a good idea. However, this is difficult because the swapfile is constantly being used. Special programs are available for this purpose.

## Paging and swapfiles

Although computers today have large amounts of RAM (working memory), today's programs are even bigger and still like to use more memory than available. A swapfile temporarily holds pieces of working memory that aren't needed at a particular moment. The operating system exchanges 'pages' of data between the swapfile and the working memory. This process allows a computer to run more programs than it can fit in the available memory. It simply writes data from memory to disk when it isn't needed, and reads it back when it is.

This practice is useful, but it has some serious consequences. The most important is that *anything* in your computer's memory can be written to disk. If it doesn't get overwritten before your computer is turned off, then someone else can examine your swapfile to get at this data. And this data may include things like your [PGP](#) passphrase and copies of personal files you are editing.

The best solution to this problem is to have a very large amount of RAM and to disable swapping to disk altogether.

## Wiping your swapfile

If having a swapfile is unavoidable, then the next best thing is to wipe its contents periodically. It's not possible to wipe the swapfile while the computer is working. This would be almost identical to removing a hard disk while the computer is on. But once the system is finished with it, the swapfile can be wiped like any other file.

There are a few pitfalls, though. The OS might expect the swapfile to be in a certain format, or at least to be *present* on the disk. If it can't find the file, it might refuse to boot or it might complain about this. Below you will find instructions on how to safely wipe your swapfile depending on your platform.

## Swapfile wiping utilities

- [Windows XP](#)
- [Windows '95](#)
- [Windows 3.1](#)
- [Linux](#)

## Windows NT, 2000 and XP

### Built-in swapfile wiping feature

Windows NT, 2000 and XP have a built-in feature which can wipe the swapfile when the system shuts down. Every page that is not in use at the time of shutdown is overwritten with zeroes. The following text is taken from the NT Resource kit:

This feature is enabled by changing a key in the registry. Go to:

```
HKEY_LOCAL_MACHINE\System
    \CurrentControlSet
        \Control
            \Session Manager
                \Memory Management
```

**Note:** Do not change the size of the paging file by editing the Registry. To create a new paging file or to change the size of a paging file, double-click the System option in Control Panel, click the Performance tab, then click the Change button in the Virtual Memory box.

#### ClearPageFileAtShutdown REG\_DWORD

Range: 0 or 1  
Default: 0

Specifies whether inactive pages in the paging file are filled with zeros when the system stops. If this value is set to 1, as the system stops, Windows NT fills all inactive pages in the paging file with zeros so that they cannot be read by another process. It cannot fill all pages with zeros because some are being used by the system or other remaining active processes. This is a Windows NT security feature.

### Third-party tools

Alternatively third-party tools are available. These usually offer more features and customizability than the above built-in feature. One popular tool is [BCWipe](#).

## Windows '95

There are three things you need to do.

1. Alter your virtual memory (swap file) settings
2. Change the boot sequence to boot into DOS
3. Run Windows via a DOS Batch file

### Alter your virtual memory (swap file) settings

The first thing you must do is go into Windows '95 and change your virtual memory settings. If you don't do this, the Windows swap file will have been insecurely "deleted" by the time that the file wiper gets to it, so the contents will still be on the disk. Also, the standard Windows '95 swap file grows and shrinks constantly, so any part of the disk could have contents of this file on it. To stop this, set the file to a constant size, and that stops it being shrunk to zero when we shut down Windows too.

Here is how to proceed:

1. Select "My Computer" from the desktop
2. Select the "Control Panel" folder
3. Select the "System" icon
4. Select the "Performance" tab
5. Press the "Virtual Memory" button

That gets you to the Virtual Memory settings. Now:

1. Click the switch for "Let me specify my own virtual memory settings".
2. Set both "Minimum" and "Maximum" boxes to the same number (this will be the number of megabytes in your swap file, I use 32).
3. Click "OK".
4. Shutdown and restart Windows (there will be a prompt inviting this).
5. After the restart, close all the open folders, panels, etc.
6. Shut down Windows from the task bar, selecting "Restart the computer in MSDOS mode" from the panel when it appears. This is in preparation for the next part of the task.

### Change the boot sequence to boot into DOS

Next, you have to stop your computer booting straight into Windows '95. There are two different ways to do this:

- Put `C:\WINDOWS\COMMAND` as the last line in your `AUTOEXEC.BAT`. That will run the Windows '95 version of `COMMAND.COM` when you boot instead of automatically going into the Windows GUI, or
- Edit the `C:\MSDOS.SYS` file to change `BootGUI=1` to `BootGUI=0`. You can also add a line saying `Logo=0` so you don't get the initial graphic screen. Essentially this restores the way that Windows used to work in version 3.x. `MSDOS.SYS` is a hidden file, so you must enter `attrib -h -r -s \msdos.sys` in order to make it accessible for editing. Use a plain ASCII DOS editor to edit the file, not a word processor.

Windows '95 may not let you do these things in a Windows DOS box, which is why you were advised above to exit Windows '95 via the shut down command and restart in MSDOS mode.

## Run Windows via a DOS Batch file

Lastly, you must write a DOS batch file to use when you want to run Windows '95. This is so that when you shut Windows down in future, execution will return to the batch file, and further commands can be processed, in particular, a secure deletion of the swap file. The batch file should look like this:

```
cd \WINDOWS
win
mode co80
cd\
pgp -w win386.swp
```

It's advisable not to name this batch file WIN.BAT, as this name may conflict with the already-existing WIN.COM.

The mode co80 line makes the "it is OK to turn off your computer" Windows shut down screen go away and returns you to the command line prompt.

Note that the last line uses PGP to wipe the swap file. You can use another program, such as [Real Delete](#), which will work as a foreground file wiper if invoked using the command `realdeal [win386.swp] /per /garb`

The square brackets are required for wiping a specified file as a foreground task (prevents accidents) and the additional switches select personal security level (just one overwrite) and the random garbage overwrite pattern.

Note that it can take a long time to wipe a swap file, as it is a very large file.

## Windows 3.1

Since Windows 3.1 is basically just a DOS application, you can safely erase the swapfile once you have exited Windows. You should not erase it from within a DOS box, even though this *is* possible!

It is recommended that you use a permanent swapfile. A temporary file gets deleted when you exit Windows, which means that you have to take extra steps to make sure it is deleted safely. Windows expects that the first 1000 bytes of the swapfile contain a specific pattern. In this location no data is stored, so you could start wiping at location 1001 or restore these bytes afterwards.

To wipe the swapfile, a tool such as [Real Delete](#) or PGP can be used.

## Linux

Linux (and other Unix-like operating systems) do not use a file but rather a separate partition on the hard disk to swap data. This partition can be wiped by simply overwriting it with zeroes or random data, or with a special tool such as [BCWipe for Unix-like systems](#).

The swap partitions are listed in `/etc/fstab`. Another way to list them is to issue the command `swapon -a`. You can add extra swap files (or partitions) with this command.

To wipe the partition, first turn it off so it is no longer in use. Then fill the partition with zeroes or random data. For example:

1. `swapon /dev/hda1`
2. `dd if=/dev/zero of=/dev/hda1`

The above commands fill the partition `/dev/hda1` with zeroes. If you use `/dev/urandom` as input instead, the partition is wiped with random data. Repeat the command multiple times for extra security.

**Warning:** Check that your swap partition is in fact `/dev/hda1` before issuing this command! The command will happily wipe whatever partition you specify, even if it's the root partition or the partition with your home directory on it.

You may need to wipe the swap partitions one by one. If you disable all swap at once, the system might not operate normally anymore.