Take Control of Variables to Secure Your Windows Environment

With the information in this article you can:

- **Identify security holes caused by environment variables**
- **Automate common system tasks**
- **Fix problems with Windows environment variables**

These days, any discussion about the environment seems destined to include terrifying predictions about global warming and melting polar ice. However, just as we should be concerned about the environment that we live in, we should also take care of the environment that our PC operates in. The Windows environment is controlled by variables. This article will help you to understand what environmental variables are and how they work. You will then be prepared to handle any faults or security problems that might be caused by these variables. Throughout this article, new concepts are supported by practical examples, which will help you to keep your PC healthy.

Dr Steve North:

"Windows uses environment variables to describe and control its operational state. Accessing or modifying the values of these variables can dramatically impact the performance of Windows. Mastering a few simple concepts will help you to resolve Windows problems that would previously have seemed insurmountable."

%WINDIR% represents the folder where Windows is installed.

Getting to Grips with Environment Variables

Windows uses environment variables as placeholders for settings that can change. In conversation when we ask: "Will you deliver to my home address?", we are using 'address' as a variable that allows for a specific value to be added later. When a Windows program wants to store a file in the folder where Windows is installed, it uses a variable called %WINDIR% which stores the path to the Windows folder. In most cases, this will be set to C:\WINDOWS but it also allows for the fact that you might have Windows installed in E:\MY_WINDOWS

Before going into any more detail, it might be useful to try something practical. Let's find out which environment variables are currently set up on your PC:

Create a file that can be used to quickly check your environment variables.

1. Right-click on your desktop.
2. Click on **New** > **Text Document**.
3. Double-click on **NEW TEXT DOCUMENT.TXT** and Notepad should open.
4. Type **set** > **VARS.TXT** into the text file.
5. Click **File** > **Save** then click **File** > **Exit**.
6. Right-click on **NEW TEXT DOCUMENT.TXT**, choose **Rename** and give it the name ENVVAR.BAT.
7. Double-click on **ENVVAR.BAT**. You should now see a file called VARS.TXT on your desktop.
8. Double-click on **VARS.TXT** and you will see a list of currently set environment variables. The format is <variable>=<value>.

Keep the file ENVVAR.BAT and, in the future, you will be able to easily check your environment variable settings.

For the rest of this article, 'Command Prompt' is used to describe the different versions of MS-DOS style command window available in Windows 98SE/Me/2000/XP. Therefore, when asked to 'open Command Prompt', please proceed as follows:

Windows 98/Me

Click **Start** > **Run**, type: **command** and click **OK**.

Open the command prompt.

Windows 2000/XP

Click **Start** > **Run**, type: **cmd** and click **OK**.

The variable %WINDIR% was mentioned on the previous page. To check its current value follow these steps:

1. Open **Command Prompt**.
2. Type: **echo %WINDIR%**
3. Press Enter.

Echo is the MS-DOS command to display text on screen. You should now see the name of the folder where Windows is installed; this is likely to be C:\WINDOWS.

Where do environment variables come from?

There are three types of environment variables:

There are three types of environment variables: system, user and volatile.

System environment variables: these are accessible to all users. They will still be available after Windows has been restarted and so are termed 'persistent'. Windows loads these when it starts (either from the registry or a file, depending on the version of Windows). Some system variables are dynamically generated each time that Windows starts.

User environment variables: in Windows 2000/XP, individual users (and their applications) can store their own environment variables, which persist and cannot be accessed by other users. These are the same as system environment variables, but only apply to the user that is logged on.

Volatile environment variables: these are created by the current user or an application and only exist while the PC's RAM (volatile memory) has not been powered-down. Restarting Windows will delete these variables.

Standard Windows system environment variables

All versions of Windows make use of standard system environment variables. In Windows 98SE, there were only a few of these. They have increased with each Windows

System (auto) variables have their values set when Windows starts.

release. Windows XP has over twenty standard variables. To display the current value of any of the following:

1. Open **Command Prompt**.
2. Type: **echo *<variable name>*** where *<variable name>* is the name of the variable.
3. Press Enter.

The first table contains environment variables that are common to Windows 98SE/Me/2000/XP:

Environment Variable name	Type	Details
%TEMP% and %TMP%	System and User	Folder where applications can store temporary files. Some applications require TEMP and others TMP.
%PROMPT%	System (auto)	Returns the MS-DOS or Command Prompt option settings (display, prompt type, etc.)
%PATH%	System	Specifies the search path where executable programs are found.
%COMSPEC%	System	Shows you where the actual main program for MS-DOS / Command Prompt is located.
%WINDIR%	System	Shows you the location of the Windows directory.

The following are some of the Environment Variables available only in Windows 2000/XP:

Environment Variable name	Type	Details
%APPDATA%	System (auto)	Contains the location where applications store data by default.
%COMPUTERNAME%	System (auto)	Contains the name of the computer.

Environment Variable name	Type	Details
%HOMEPATH%	System (auto)	Contains the full path of the user's home directory. Usually this is C:\Documents and Settings\<*username*> where <*username*> is the user's login name. The user's home directory is specified in Local Users and Groups.
%OS%	System	Contains the operating system name. Windows 2000/XP displays the operating system as NT.
%SYSTEMROOT%	System (auto)	Stores the folder name that contains the Windows system (or System32) folder.
%SYSTEMDRIVE%	System (auto)	Contains the drive letter containing %SYSTEMROOT%.
%USERNAME%	System (auto)	Contains the name of the user who is currently logged on.

Creating Your Own Environment Variables

Create an environment variable that, when called, will empty your temporary folder.

In order to fix problems with your environment variables, you need to understand how they are created. It will be helpful to work through a practical example to see how this is done. In this section, we will create an environment variable that clears out your Windows temporary folder, to help improve performance. This will start as a volatile variable that won't survive a Windows restart. It will then be converted into a persistent variable that can be used at any time.

The volatile environment variable

First, create the environment variables that will empty your temporary folder:

Windows 98SE/Me

1. Open **Command Prompt**.
2. Type: **set CLEAN=deltree /y %WINDIR%\temp*.***
3. Press Enter.

Windows 2000/XP

1. Open **Command Prompt**.
2. Type: **set CLEAN=rd %WINDIR%\TEMP /s /q**
3. Press Enter.
4. Type: **set REP=md %WINDIR%\TEMP**
5. Press Enter.

Windows 2000/XP does not support the MS-DOS 'deltree' command.

Note: it is necessary to use different MS-DOS commands for Windows 98SE/Me and 2000/XP because 'deltree' (which literally means delete the tree of files and folders) is not present in the 2000/XP version of MS-DOS. Instead, two commands are required. First the entire folder is deleted ('rd' means remove directory) and then an empty replacement is created ('md' means make directory).

The environment variables are now ready to test. It is a good idea to open Windows Explorer, so that you can watch the result as it happens:

1. Right-click **Start**, then choose **Explore**.
2. In the address bar, type: **%WINDIR%\TEMP**
3. Press Enter.

You can use environment variables in a Windows Explorer address.

Note the use of the environment variable %WINDIR%, which is likely to be set to: C:\WINDOWS. In addition, note how it is possible to use environment variables as an address in Windows Explorer. To empty your temporary folder, proceed as follows:

Windows 98SE/Me

1. Open **Command Prompt**.
2. Type: **%CLEAN%**
3. Press Enter.

Windows 2000/XP

1. Open **Command Prompt**.
2. Type: %CLEAN% then press Enter.
3. **Type:** %REP% **then press** Enter.

A volatile variable will only be available until Windows is restarted.

In Windows Explorer, you should now see the TEMP folder empty itself. In Windows 2000/XP, you may find that your location has changed to %WINDIR% and you will need to open the TEMP folder again. As this is a volatile example, these environment variables will only remain available in RAM until Windows is restarted or the command prompt is closed.

The system environment variable

We will now convert the variable we have just created from a volatile variable (which will be lost when Windows is restarted) to a persistent variable which will be available after a restart.

Convert your variable, so that you can empty your temporary folder at any time.

1. Start Windows Explorer.
2. In the address bar, type: %WINDIR%
3. Press Enter.
4. Right-click on an empty space in the right-hand pane of Windows Explorer.
5. Click on **New** > **Text Document**.
6. Double-click on **NEW TEXT DOCUMENT.TXT** and Notepad should open.
7. Windows 98SE/Me
   type: **deltree /y %WINDIR%\temp*.***
   Windows 2000/XP
   type: **rd %WINDIR%\TEMP /s /q** on one line and then **md %WINDIR%\TEMP** on the line below.
8. Click **File** > **Save** then click **File** > **Exit**.
9. Right-click on **NEW TEXT DOCUMENT.TXT** choose **Rename** and call it **CLEAN.BAT**.

Create a Windows batch file that will empty the temporary folder.

Use the delete commands with great care!

We now have a file with commands that will empty the TEMP folder. Next we need to create a persistent system environment variable that will execute CLEAN.BAT.

Windows 98SE/Me

Early versions of Windows store persistent variables in a file.

Persistent system environment variables in Windows 98SE/Me are set in a file called AUTOEXEC.BAT. The commands that this contains (including those for environment variable settings) run at Windows startup, before control of the PC is turned over to the user.

Make sure that Notepad's Word Wrap feature (**Format** menu) is turned off.

1. Right-click **Start** then choose **Explore**.
2. Browse to **C:** (or the root of the drive that you have Windows installed on).
3. Right-click on the file **AUTOEXEC.BAT** and choose **Edit**.
4. After any other lines in the file, type the line: **set CLEAN=%WINDIR%\CLEAN.BAT**
5. Click **File** > **Save** then click **File** > **Exit**.
6. Restart Windows.

Windows 2000/XP

Persistent environment variables in Windows 2000/XP are set from within the operating system. Although AUTOEXEC.BAT may still be found in 2000/XP, it is only present in case older applications require it. Windows no longer uses it for environment variables. To set the variable:

1. Click on **Start** > **Settings** > **Control Panel** (**Start** > **Control Panel** in Windows XP).
2. Double-click on **System** then click on the **Advanced** tab.
3. Click on the **Environment Variables** button.
4. Under **System Variables**, click on the **New** button.
5. On the **New System Variable** screen, in the **Variable name** field type: **CLEAN**

6. In the **Variable value** field type: %WINDIR%\CLEAN.BAT
7. Click **OK** > **OK** > **OK**.
8. Restart Windows.

Open Windows Explorer, so that you can check that the temporary directory has emptied, and then test the variable:

1. Right-click **Start** then choose **Explore**.
2. In the address bar, type: %WINDIR%\TEMP
3. Press Enter.
4. Open Command Prompt.
5. Type: %CLEAN % then press Enter.

Assuming that this is all working correctly, you can now empty your temporary folder at any time, by repeating the last two steps.

Identify Security Problems Caused by Environment Variables

Now that you have an understanding of variables and their function within the Windows environment, the rest of this article will consider the possible problems that they may cause. In this section, we will consider an example of a security issue, which you need to know about.

The %PATH% variable allows programs to be started by name, without a full path.

There is a Windows environment variable called %PATH%. This contains a list of the paths to important files used by Windows and installed programs. Its purpose is to allow a program to be started just by name, without using its full location (or path) on the hard drive. For example, in Windows XP the application Notepad (NOTEPAD.EXE) can be found in C:\WINDOWS\system32\. This location varies between versions of Windows, but this does not affect the point of this illustration.

The path to Notepad will be found, along with several others, in the environment variable %PATH%.

As an executable file (one which ends in .exe), Notepad can be started just by typing its name into Command Prompt. Without the entry C:\WINDOWS\system32\ in the environment variable %PATH%, you would need to type: C:\WINDOWS\system32\notepad. As there are lots of other programs in the same location, adding this entry to %PATH% allows any of them to be run by name. You can try this out as follows:

1. Open Command Prompt.
2. Type **Notepad** then press Enter.

If Windows finds a file called EXPLORER in a location specified in %PATH%, it will start it.

This feature can be exploited to allow malware to be started, instead of the intended program. EXPLORER.EXE is an essential process in Windows. It controls the Windows Program Manager or Windows Explorer (depending on your Windows version) and also manages the Windows Graphical Shell including the Start menu, taskbar and desktop. Without this process the graphical interface for Windows would disappear. The program can be found in the path stored in the environment variable %WINDIR%. In Windows XP, this is C:\WINDOWS\. When Windows starts up, an entry in the registry is used to call EXPLORER.EXE. Due to the path in %WINDIR% being contained in %PATH%, EXPLORER.EXE can be started just by name (as with the Notepad example).

At startup, Windows looks in C:\ before checking the paths in the %PATH% variable.

When Windows tries to start EXPLORER.EXE by name, it first looks in the root of your hard drive (usually C:\) and then sequentially searches the paths in %PATH% looking for a program called EXPLORER.EXE. If it finds something with the same name before it reaches the real copy in %WINDIR%, it will start this program instead. This is obviously very dangerous, as a virus can copy a compromised version of EXPLORER.EXE into C:\ and it will take control of vital Windows display functions. Also, once the real EXPLORER.EXE is no longer running and protected by Windows, the virus can also modify the real version.

A virus can be named EXPLORER and placed in C:\ and this impostor will start instead of the real version.

The key thing to understand here is that the %PATH% environment variable allows Windows to keep things simple.

EXPLORER.EXE can be started just by Windows calling EXPLORER, rather than having to call C:\WINDOWS\EXPLORER. This can make life much simpler when Windows is dealing with hundreds of components and the user has changed a path (by installing Windows in C:\MY_WINDOWS\, for example). However, its weakness is that %PATH% is searched sequentially for copies of EXPLORER.EXE and it is possible to put a fake program in a location that occurs earlier in the list of paths.

Put C:\WINDOWS at the start of your %PATH% variable.

You can avoid this by editing %PATH% so that C:\WINDOWS appears first in the list. As C:\ is searched before %PATH% (whether or not it is listed in this variable), there is unfortunately no way to put C:\WINDOWS before C:\

To change the order in Windows 98SE/Me:

In Windows 98/Me %PATH% is edited in AUTOEXEC.

1. Right-click **Start** and choose **Explore**.
2. Browse to **C:** (or the root of the drive that you have Windows installed on).
3. Right-click on the file **AUTOEXEC.BAT** and choose **Edit**.
4. Make sure that C:\WINDOWS occurs first in the line starting **PATH=** (it should read SET PATH=C:\WINDOWS...).
5. Click **File** > **Save** then **File** > **Exit**.
6. Restart Windows.

To change the order in Windows 2000/XP:

In Windows 2000/XP %PATH% is edited in Control Panel.

1. Click **Start** > **Settings** > **Control Panel** (**Start** > **Control Panel** Windows XP).
2. Double-click on **System** then click on the **Advanced** tab.
3. Click on the **Environment Variables** button.
4. Under **System Variables**, double-click on **Path**.
5. In the **Variable value** field, make sure that C:\WINDOWS (or %SYSTEMROOT%) occurs first in the list of paths. Edit it if necessary.

6. Click **OK** > **OK** > **OK**.
7. Restart Windows.

Search for extra copies of EXPLORER, they may be intruders.

A second precaution is to search for additional copies of EXPLORER.EXE. If you find any instances of this file that are not located in %WINDIR%, temporarily rename them (EXPLORER.EXE.OLD for example), so that they are disabled.

Fix Problems Caused by Environment Variables

Keep a back up list of your environment variables.

Many viruses will add new environment variables or make changes to your existing ones. For example, %PATH% may be modified to load an infected version of a program. If you suspect that your computer has become infected, it is a good idea to have a copy of your variables as they were before your PC was compromised.

1. Double-click on the **ENVVAR.BAT** file that you created earlier in the article. You should now see a file called VARS.TXT on your desktop.
2. Double-click on **VARS.TXT** and you will see the list of environment variables.
3. In Notepad, click **File** > **Save As...** Name the file: **VARS *<DATE>*.TXT**
4. Where *<DATE>* is today's date.
5. Click **File** > **Exit**.
6. **Keep the file that you have just created in a safe place and then if your PC becomes infected, you can run ENVVAR.BAT again and compare the two text file lists of environment variables.**

Examine the %PATH% variable for suspicious paths.

When you have generated VARS.TXT after a possible infection, you should first examine the %PATH% variable for suspicious folders that you don't recognise. Using Windows Explorer, see what's inside the suspicious folder. Search on the Internet for both the suspicious path and the names of

any files that it contains. Also look for suspicious environment variables that are not present in the older copy of VARS.TXT. Search for these, by name, on the Internet.

Problems installing new software

A common cause of software installation failure is a missing or incorrect %TEMP% environment variable. Microsoft Office is particularly prone to failing on installation when this variable is either missing or pointing to a non-existent folder. You must determine the location of your Windows %TEMP% folder and verify the validity of your %TEMP% environment variable. To check this follow these steps:

Many software installation routines expect to find %TEMP% or %TMP%.

1. Open Command Prompt.
2. Type: **echo %TEMP%**
3. Press Enter.

If the %TEMP% variable exists, make a note of the folder and use Windows Explorer to check that the folder itself exists. If necessary, create a folder with the correct name. If %TEMP% does not exist, create a new environment variable with this name:

Does %TEMP% exist and is it pointing at a folder that exists?

Windows 98/Me

1. Start Windows Explorer.
2. Browse to C:\ (or the root of the drive that you have Windows installed on).
3. Right-click on the file **AUTOEXEC.BAT** and choose **Edit**.
4. Add the line **set TEMP=C:\WINDOWS\TEMP**. Note: amend this if Windows is not installed in a folder called WINDOWS.
5. Click **File** > **Save** then click **File** > **Exit**.
6. Restart Windows.

In Windows 98SE/Me add %TEMP% to AUTOEXEC.

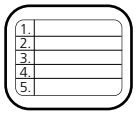
Windows 2000/XP

1. Click on **Start** > **Settings** > **Control Panel** (**Start** > **Control Panel** in Windows XP).

In Windows 2000/XP add %TEMP% via the Control Panel.

2. Double-click on **System** then click on the **Advanced tab**.
3. Click on **Environment Variables**.
4. Under **System Variables** click **New**.
5. In the **New System Variable** screen, in the **Variable name** field type: **TEMP**.
6. In the **Variable value** field type: **C:\WINDOWS\TEMP**
   Note: amend this if Windows is not installed in a folder called WINDOWS.
7. Click **OK > OK > OK**.
8. Restart Windows.

Now reattempt the software installation that previously failed.



This article has shown you what environment variables are and how they are generated at Windows startup. It has also shown you how to write a batch file that generates a file listing all of your environment variable and how to create your own environment variable that can run a batch file to empty your temporary folder.

We have also looked at the security problems caused by variables and how you can protect Windows processes (such as EXPLORER.EXE) from being hijacked via the %PATH% environment variable, as well as how to examine changes to your environment variables looking for virus intrusion and how to diagnose software installation problems relating to environment variables.