**Entry Points for Startup Processes**

This appendix contains a summary of the entry points that can affect Windows 10/8/7 startup. The entry points include startup folders, Group Policy folders, the Scheduled Tasks folder, and registry keys. To see all the subfolders listed in this appendix, use File Explorer Options or Folder Options in Control Panel to unhide folders that don’t normally display in File Explorer or Windows Explorer.

Programs and shortcuts to programs are stored in these startup folders:

* C:\Users\*username*\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
* C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

Startup and shutdown scripts used by Group Policy are stored in these folders:

* C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup
* C:\Windows\System32\GroupPolicy\Machine\Scripts\Shutdown
* C:\Windows\System32\GroupPolicy\User\Scripts\Logon
* C:\Windows\System32\GroupPolicy\User\Scripts\Logoff

Scheduled tasks are stored in this folder:

* C:\Windows\System32\Tasks

To see a list of scheduled tasks, enter the schtasks command in a command prompt window.

These keys cause an entry to run once and only once at startup:

* HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
* HKLM\Software\Microsoft\Windows\CurrentVersion\RunServiceOnce
* HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
* HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

Group Policy places entries in the following keys to affect startup:

* HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
* HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

Windows loads many DLL programs from the following key, which is sometimes used by malicious software. Don’t delete one unless you know it’s causing a problem:

* HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

Entries in the keys listed next apply to all users and hold legitimate startup entries. Don’t delete an entry unless you suspect it to be bad:

* HKLM\Software\Microsoft\Windows\CurrentVersion\Run
* HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows
* HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
* HKCU\Software\Microsoft\Windows\CurrentVersion\Run

These keys and their subkeys contain entries pertaining to background services that are sometimes launched at startup:

* HKLM\Software\Microsoft\Windows\CurrentVersion\RunService
* HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices

The following key contains a value named BootExecute, which is normally set to autochk. It causes the system to run a type of Chkdsk program to check for hard drive integrity if it was previously shut down improperly. Sometimes another program adds itself to this value, causing a problem. The Chkntfs utility can be used to exclude volumes from being checked by autochk. For more information about this situation, search for “CHKNTFS.EXE: What You Can Use It For” at *support.microsoft.com.*

* HKLM\System\CurrentControlSet\Control\Session Manager

Here is an assorted list of registry keys that have all been known to cause various problems at startup. Remember, before you delete a program entry from one of these keys, research the program file name so that you won’t accidentally delete something you want to keep:

* HKCU\Software\Microsoft\Command
* HKCU\Software\Microsoft\Command Processor\AutoRun
* HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup
* HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\load
* HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit\_DLLs
* HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\System
* HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Us
* HKCR\batfile\shell\open\command
* HKCR\comfile\shell\open\command
* HKCR\exefile\shell\open\command
* HKCR\htafile\shell\open\command
* HKCR\piffile\shell\open\command
* HKCR\scrfile\shell\open\command

Finally, check out the subkeys in the following key; they apply to 32-bit programs installed in a 64-bit version of Windows:

* HKLM\Software\Wow6432Node

Other ways in which processes can be launched at startup:

* Services can be set to launch at startup. To manage services, use the Services console (services.msc).
* Device drivers are launched at startup. For a listing of installed devices, use Device Manager (devmgmt.msc) or the System Information utility (msinfo32.exe).