



Fixing Windows XP

Chapter 2

Making Windows XP Boot Like New

Objectives

- Learn how to apply quick fixes to solve some drastic startup problems
- Learn how to remove unwanted startup processes to help optimize a system
- Learn about some complex solutions for difficult startup problems
- Learn how to keep the startup process clean

Introduction

- Chapter 2 organized as a how-to chapter
- You will learn:
 - Quick-and-dirty solutions to startup problems
 - Ways to clean up the startup process
 - Solutions needed for the most difficult situations
 - How to keep the problem from coming back

Quick Fixes for Drastic Startup Problems

- What to do for an immediate Windows XP startup problem, e.g.,
 - An error message
 - A device not working
- Tools covered in this section:
 - Last Known Good Configuration
 - Safe Mode
 - System Restore
 - System Configuration

Last Known Good Configuration

- Try when Windows XP will not boot to the Windows desktop
- Revert to the Last Known Good Configuration
 - Configuration on last startup saved in the registry
 - This method will work if:
 - Last Known Good is taken after the problem first started
 - Problem is caused by an error in the Windows XP configuration that has corrupted the registry

Safe Mode on the Advanced Options Menu

- If Last Known Good Configuration doesn't work, start in Safe Mode
- Once in Safe Mode:
 - Scan for viruses, clean, and reboot
 - Scan the hard drive for errors
 - Open Explorer and right-click logical drive C
 - Select the Tools tab in the Properties box
 - Click Check Now to scan for bad sectors

Windows XP in Safe Mode

The screenshot shows the Windows XP desktop in Safe Mode. The Windows Task Manager window is open, displaying the 'Processes' tab. The task manager window title is 'Windows Task Manager' and it has a menu bar with 'File', 'Options', 'View', 'Shut Down', and 'Help'. The 'Processes' tab is selected, showing a list of running processes with columns for 'Image Name', 'User Name', 'CPU', and 'Mem Usage'. The processes listed are:

Image Name	User Name	CPU	Mem Usage
taskmgr.exe	Jean Andrews	02	3,644 K
explorer.exe	Jean Andrews	00	12,404 K
svchost.exe	LOCAL SERVICE	00	1,808 K
svchost.exe	NETWORK SERVICE	00	1,628 K
svchost.exe	SYSTEM	00	10,400 K
MsmEng.exe	SYSTEM	00	7,640 K
svchost.exe	NETWORK SERVICE	00	2,884 K
svchost.exe	SYSTEM	01	2,860 K
lsass.exe	SYSTEM	00	1,100 K
services.exe	SYSTEM	00	3,092 K
winlogon.exe	SYSTEM	00	2,448 K
csrss.exe	SYSTEM	00	2,188 K
smss.exe	SYSTEM	00	324 K
System	SYSTEM	00	120 K
System Idle Process	SYSTEM	97	16 K

At the bottom of the task manager window, there is a checkbox labeled 'Show processes from all users' which is checked, and an 'End Process' button. The system tray at the bottom of the screen shows 'Processes: 15', 'CPU Usage: 4%', 'Commit Charge: 67840K / 314812K', and the time '11:07 AM'. The text 'Safe Mode' is visible in the bottom right corner of the desktop.

Figure 2-2 Windows XP in Safe Mode

Scan Logical Drive C for Errors



Figure 2-3 Scan logical drive C for errors

Safe Mode on the Advanced Options Menu (continued)

- Verify that drive has at least 318 MB of free space
- Make needed changes to Windows settings & reboot
- If System Restore has been configured to create restore points:
 - Use System Restore to bring the system back to a restore point and reboot
- If you have a current backup of the system state:
 - Use Ntbackup to restore system state

Safe Mode on the Advanced Options Menu (continued)

- How to try Safe Mode:
 - Try Safe Mode with Networking
 - Then try Safe Mode
 - Then try Safe Mode with Command Prompt
- Safe Mode won't help if core Windows components are corrupted
- If infected with viruses, boot into Safe Mode and run antivirus software there
- When booting into Safe Mode, choose between continuing to Safe Mode or using System Restore

System Restore

- Restores system to condition when snapshot taken
- Snapshot:
 - Taken of system settings and configuration
 - Called restore point
- Create restore point:
 - Automatically before any changes made to the system if System Restore is turned on
 - Manually at any time

System Restore (continued)

- Restoring a system to a previous restore point:
 - Will not alter user data on the hard drive
 - Can affect installed software and hardware, user settings, and OS configuration settings

Using a Previous Restore Point

- To start System Restore:
 - Choose System Restore when booting into Safe Mode

System Restore Utility Opening Screen

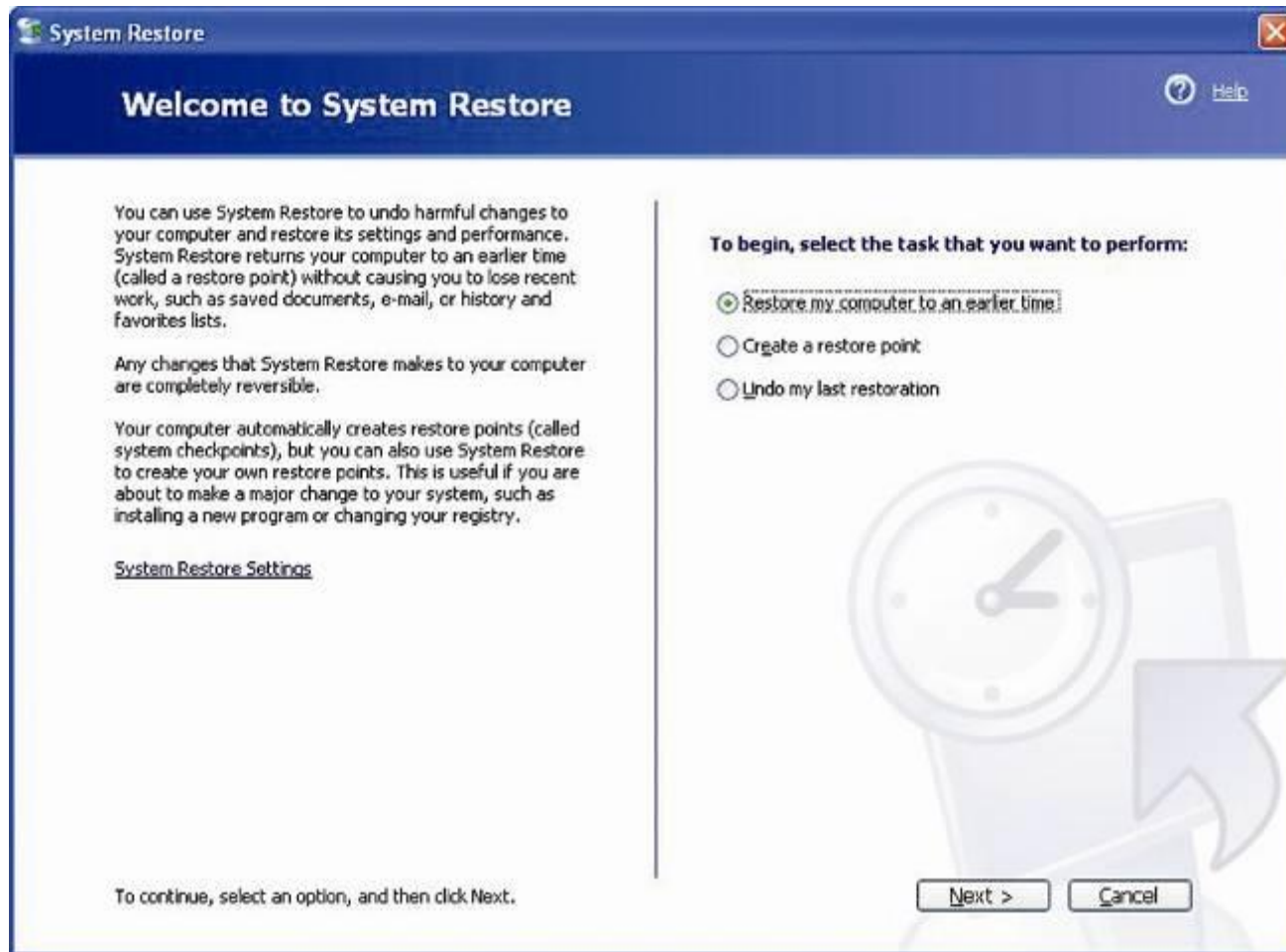


Figure 2-6 System Restore utility opening screen

Points to Remember about System Restore

- A great tool for:
 - Trying to fix a device that is not working
 - Restoring Windows settings with problems
 - Solving problems with applications

Points to Remember about System Restore (continued)

- System Restore limitations:
 - Must be able to boot normally or into Safe Mode
 - Only works if registry somewhat intact
 - Cannot help recover from a virus or worm unless infection launched at startup
 - Might create a new problem – use sparingly
 - For changes made to hardware devices, first try Driver Rollback
 - Must have restore points to use

System Configuration Utility (Msconfig)

- Use System Configuration Utility (Msconfig.exe) to disable processes that normally load at startup
 - Not a permanent fix
- Can use Msconfig to edit contents of initialization files using tabs for:
 - System.ini
 - Win.ini
 - Boot.ini

Use Msconfig to Temporarily Disable Processes

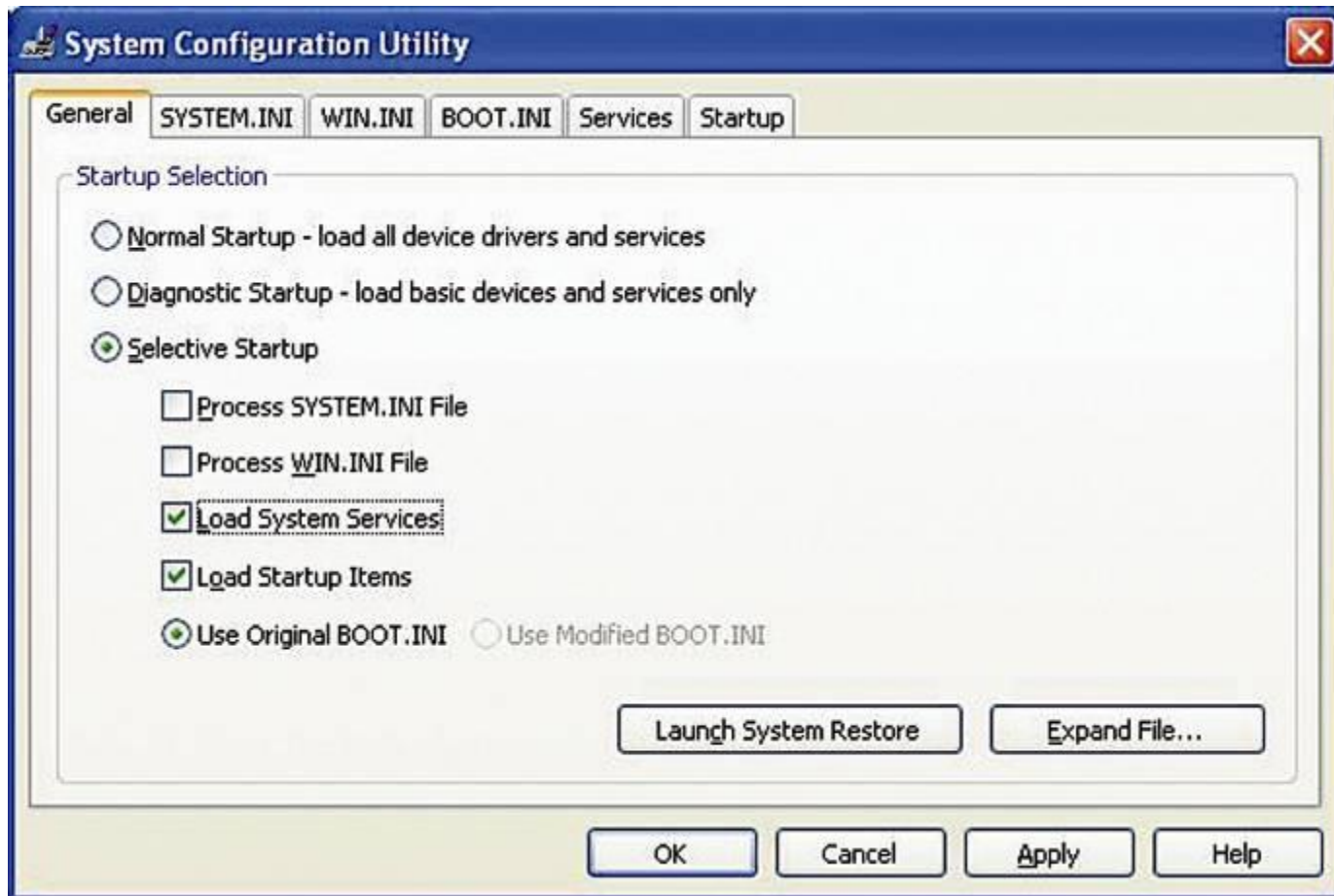


Figure 2-8 Use the Msconfig utility to temporarily disable processes from loading at startup

System Configuration Utility (Msconfig) (continued)

- To troubleshoot a startup problem:
 - Check the items to start
 - Uncheck the items to temporarily disable
 - Apply changes
 - Close utility
 - Reboot
- If problem solved, enable one service at a time in Msconfig until the problem reappears
- Investigate the problem service
- Verify that Normal Startup is selected on Msconfig window General tab

Clean Up Startup

- Learn step-by-step clean up procedures:
 - Start with easiest level of tools and methods
 - Then use more technical tools
- To remove unwanted applications or drivers, or change their startup parameters:
 - Perform a cold boot
 - Record number of seconds required to get to Windows desktop
 - Note items in system tray and windows that appear
- Assumption – Windows starts with no errors

Viewing Processes with Task Manager

- To view list of open applications:
 - Click Applications tab of Task Manager
- To view a program filename associated with an open application:
 - Right-click the application in the Applications tab in the Task Manager
 - Select Go To Process from the shortcut menu
 - The correct process on the Processes tab of Task Manager is highlighted
- To view the list of processes currently running:
 - Click the Processes tab

Viewing Processes with Task Manager (continued)

- Two modes in which OS programs and other programs can run:
 - User mode
 - Kernel mode
- Applications normally run in user mode
- Device drivers normally run in kernel mode
- A virus or worm can run in either mode
- Malicious processes running in kernel mode do not show up in Task Manager

Core Windows Processes

- To troubleshoot Windows, be familiar with:
 - All processes shown in Figure 2-11
 - The path to each program file
 - Most often C:\Windows\system32
 - The account under which the process normally runs

Processes Showing under Task Manager

Image Name	User Name	CPU	Mem Usage
taskmgr.exe	Administrator	01	3,300 K
mmsgs.exe	Administrator	00	372 K
svchost.exe	SYSTEM	00	2,192 K
explorer.exe	Administrator	00	9,760 K
spoolsv.exe	SYSTEM	00	3,604 K
svchost.exe	LOCAL SERVICE	00	3,144 K
svchost.exe	NETWORK SERVICE	00	2,444 K
svchost.exe	SYSTEM	00	11,196 K
svchost.exe	SYSTEM	00	3,132 K
lsass.exe	SYSTEM	00	4,688 K
services.exe	SYSTEM	00	2,356 K
winlogon.exe	SYSTEM	00	2,744 K
csrss.exe	SYSTEM	00	2,596 K
smss.exe	SYSTEM	00	348 K
System	SYSTEM	00	216 K
System Idle Process	SYSTEM	99	20 K

Show processes from all users

End Process

Processes: 16 CPU Usage: 1% Commit Charge: 57104K / 315221

Figure 2-11 Processes showing under Task Manager for a fresh installation of Windows XP

Core Windows Processes (continued)

- Investigate unknown processes on the Internet
 - Microsoft support site at support.microsoft.com
 - McAfee Security Web site
 - Answers That Work at www.answersthatwork.com
 - Jim Foley, The Elder Geek at www.theelderageek.com
 - Process Library by Jelsoft Enterprises, Ltd. At www.processlibrary.com
 - Uniblue at www.liutilities.com
 - Antivirus software sites listed in Table 1-1

Core Windows Processes (continued)

- Use Services console to close a service
- If process does not respond properly:
 - First try selecting the program on the Task Manager Applications tab and clicking End Task
 - Next try selecting the application on the Processes tab and clicking End Task
 - Can also try:
 - Closing the service (log in as administrator)
 - Using Tskill command in Command Prompt window

Do A General Cleanup

- To begin cleaning Windows startup:
 - Back up data
 - Boot into Safe Mode and run antivirus software
 - Respond to error messages
 - Uninstall software just installed
 - Disable new hardware devices just installed
 - Uninstall device if necessary
 - Rollback device drivers if just updated
 - Remove unwanted software
 - Clean up hard drive

Startup Folders

- To clean up startup:
 - Look in each startup folder
 - Move non-malicious programs or shortcuts to a different folder rather than deleting them
- Start up folders:
 - Current user startup folder
 - C:\Documents and Settings*username*\Start Menu\Programs\Startup
 - All users startup folder
 - C:\Documents and Settings\All Users\Start Menu\Programs\Startup

Startup Folders (continued)

- Upgrade from Windows NT:
 - C:\Windows\Profiles\All Users\Start Menu\Programs\Startup
 - C:\Windows\Profiles*username*\Start Menu\Programs\Startup
- Also check Scheduled Task folder

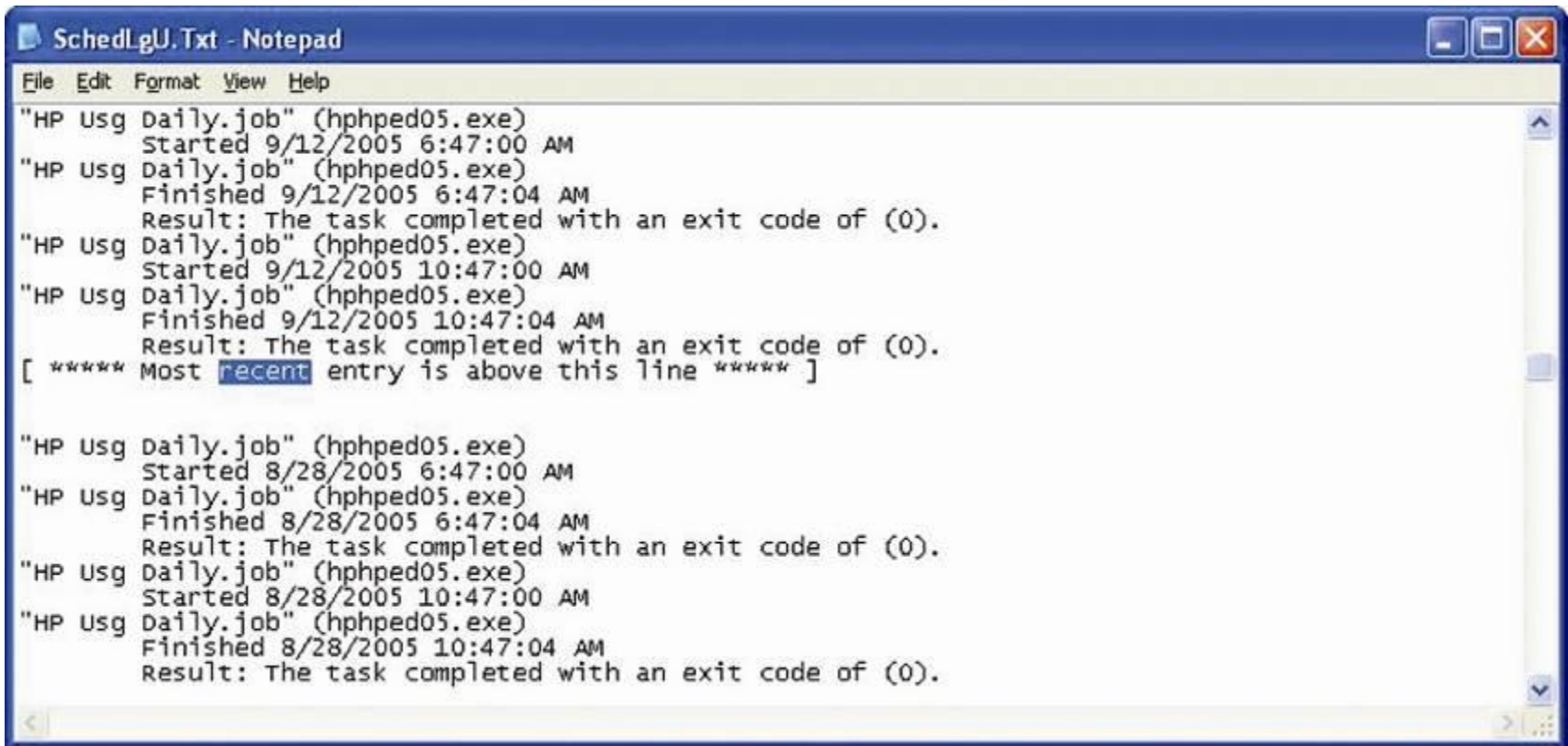
Scheduled Task Folder

- Windows Task Scheduler can be set to launch a task or program at a future time including startup
 - A file stored in C:\Windows\Tasks folder for each scheduled task
- To view list of scheduled tasks:
 - Open Scheduled Tasks applet in Control Panel
 - When the Scheduled Tasks folder appears:
 - Click View, Details, to see details of a task
- To add, delete, or change tasks, use:
 - Scheduled Tasks window
 - Schtasks command at the command line

Scheduled Task Folder (continued)

- Scheduled Task process generates log of activity
- Log file:
 - C:\Windows\SchedLgU.Txt
- To view log file:
 - Click Advanced, View Log, in the Scheduled Tasks window
- To find most recent entry:
 - Use Notepad search feature
 - Search for “recent”

Log of Activities of Scheduled Tasks



The screenshot shows a Notepad window titled "SchedLgU.Txt - Notepad". The menu bar includes "File", "Edit", "Format", "View", and "Help". The text content is as follows:

```
"HP Usq Daily.job" (hphped05.exe)
Started 9/12/2005 6:47:00 AM
"HP Usq Daily.job" (hphped05.exe)
Finished 9/12/2005 6:47:04 AM
Result: The task completed with an exit code of (0).
"HP Usq Daily.job" (hphped05.exe)
Started 9/12/2005 10:47:00 AM
"HP Usq Daily.job" (hphped05.exe)
Finished 9/12/2005 10:47:04 AM
Result: The task completed with an exit code of (0).
[ ***** Most recent entry is above this line ***** ]

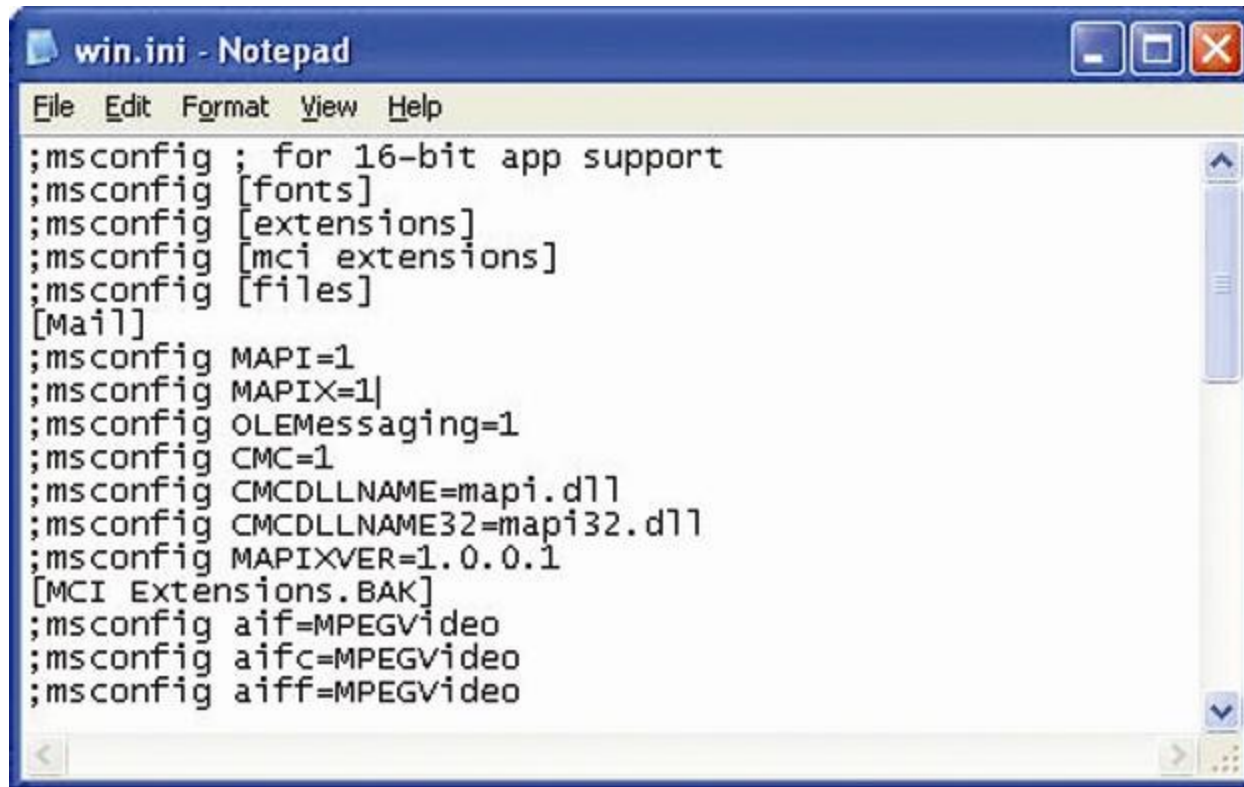
"HP Usq Daily.job" (hphped05.exe)
Started 8/28/2005 6:47:00 AM
"HP Usq Daily.job" (hphped05.exe)
Finished 8/28/2005 6:47:04 AM
Result: The task completed with an exit code of (0).
"HP Usq Daily.job" (hphped05.exe)
Started 8/28/2005 10:47:00 AM
"HP Usq Daily.job" (hphped05.exe)
Finished 8/28/2005 10:47:04 AM
Result: The task completed with an exit code of (0).
```

Figure 2-19 View a log of activities of scheduled tasks

Legacy System Files Used for Startup

- Four legacy system files used to control startup process:
 - Autoexec.bat
 - Config.sys
 - System.ini
 - Win.ini
- System.ini and Win.ini located in the C:\Windows folder
- To check legacy files use Msconfig or Notepad:
 - Right-click filename and select Open from the shortcut menu

Harmless and Unused Win.ini file



```
win.ini - Notepad
File Edit Format View Help
;msconfig ; for 16-bit app support
;msconfig [fonts]
;msconfig [extensions]
;msconfig [mci extensions]
;msconfig [files]
[Mail]
;msconfig MAPI=1
;msconfig MAPIX=1
;msconfig OLEMessaging=1
;msconfig CMC=1
;msconfig CMCDLLNAME=mapi.dll
;msconfig CMCDLLNAME32=mapi32.dll
;msconfig MAPIXVER=1.0.0.1
[MCI Extensions.BAK]
;msconfig aif=MPEGvideo
;msconfig aifc=MPEGvideo
;msconfig aiff=MPEGvideo
```

Figure 2-20 A harmless and unused Win.ini file

Services

- Use Services console to view services set to automatically start when Windows loads
- To launch Services console:
 - Type Services.msc in Run dialog box and press Enter
- To learn about a service:
 - Right-click and select Properties from shortcut menu
- When permanently disabling a service:
 - Reboot and make sure everything works

Services Console

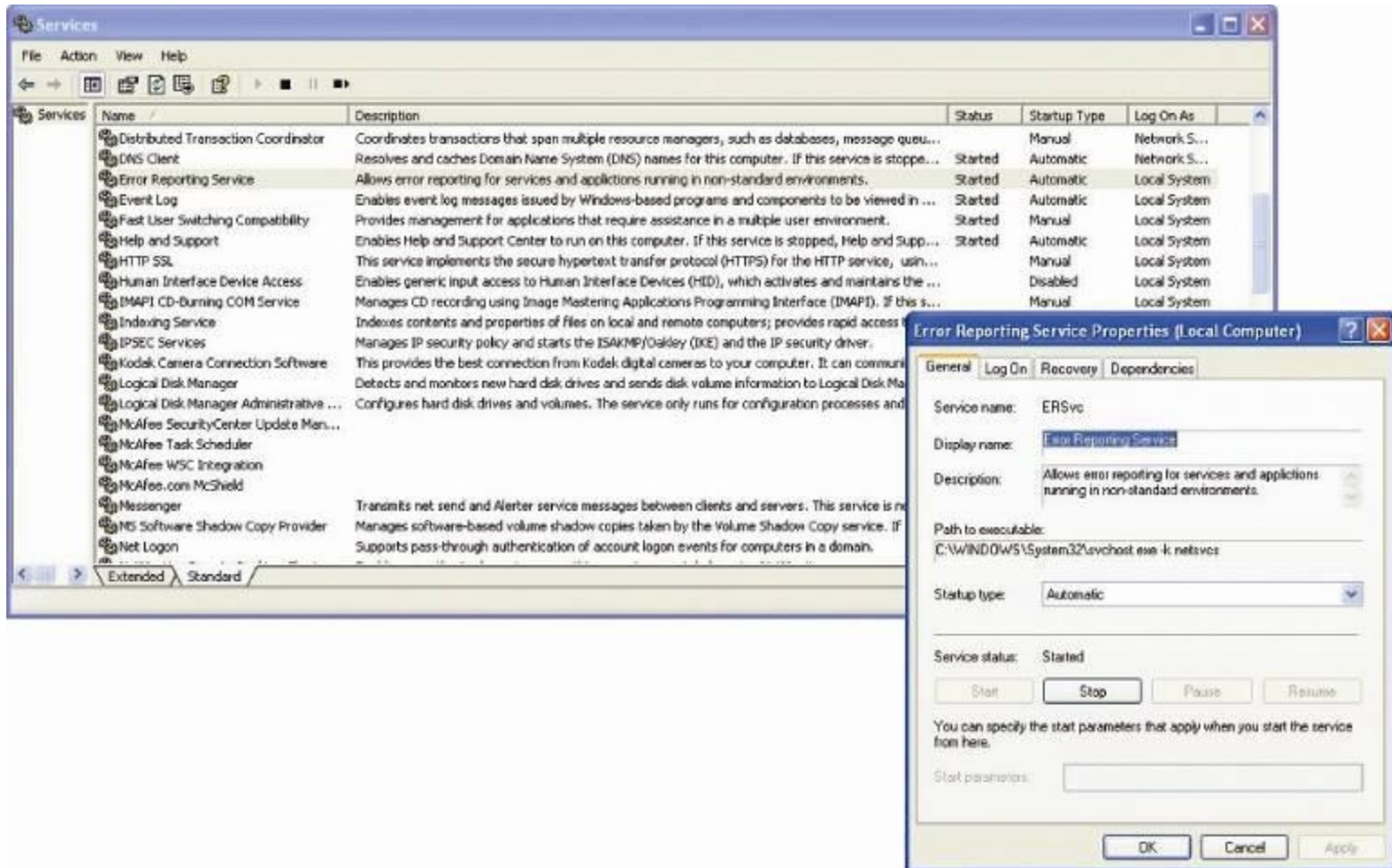


Figure 2-21 The Services console is used to start, stop, and schedule services

Group Policy

- For Windows XP Professional, use Group Policy console (Gpedit.msc) to:
 - Manage many computers on a network
 - Limit how users can use Windows and applications
 - Control Windows settings and features
- Group Policy can also be used to:
 - Manage a single standalone computer
 - Launch programs at startup
- To access Group Policy console:
 - Enter gpedit.msc in Run dialog box

Group Policy (continued)

- Two main groups of policies:
 - Computer Configuration
 - User Configuration
- Four ways to launch a script using Group Policy:
 - Startup
 - Shutdown
 - When a user logs on
 - When a user logs off

Group Policy (continued)

- Scripts for launching a program stored in:
 - 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
- To see currently applied Group Policies use Windows XP Help and Support Center

Group Policy Console

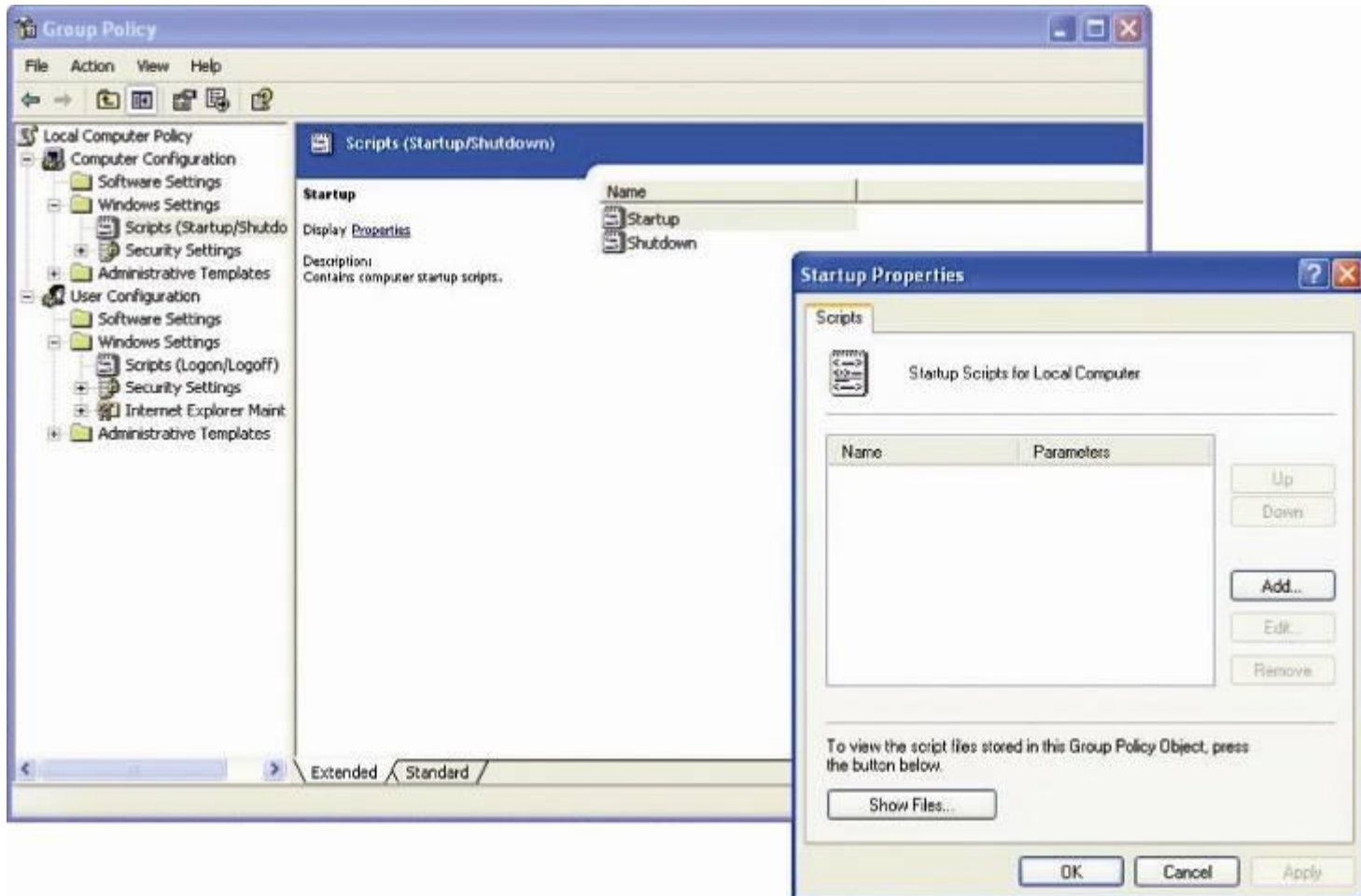


Figure 2-22 Using the Group Policy console, you can control many Windows events and settings, including the startup process

Uninstall Unused Fonts

- All installed fonts loaded at startup
- Unused fonts can slow down startup
- To install or uninstall a font:
 - Move font in or out of C:\Windows\Fonts folder

Digging Deeper into Startup Processes

- Learn to:
 - Search the registry and remove startup tasks left there by software
 - Remove software that won't politely uninstall using Add or Remove Programs
 - Use third-party utilities

Editing the Registry

- Many actions result in changes to the registry that can:
 - Create new keys
 - Add new values to existing keys
 - Change existing values
- May need to edit or remove a registry key for difficult problems
- Will learn:
 - How registry is organized
 - Which keys might hold entries causing problems
 - How to back up and edit the registry

Editing the Registry (continued)

- Registry:
 - A hierarchical database
 - Contains configuration information for:
 - Windows
 - Users
 - Software applications
 - Installed hardware devices
 - Built during startup
 - Organized into five tree-like structures called keys:
 - HKEY_CURRENT_USER (HKCU)
 - Contains configuration information for current user

Editing the Registry (continued)

- HKEY_USERS (HKU)
 - Stores information for every user
- HKEY_LOCAL_MACHINE (HKLM)
 - Contains configuration information for all software, hardware, and security settings
- HKEY_CLASSES_ROOT (HKCR)
 - Stores information that determines which application opens when user double-clicks a file
- HKEY_CURRENT_CONFIG (HKCC)
 - Contains Plug and Play information about the hardware configuration

Editing the Registry (continued)

- Two ways to back up the registry:
 - Back up entire system state and registry
 - Back up keys in the registry expected to change
- To restore system state:
 - Open Backup Utility window, select Restore Wizard (Advanced)
- To restore registry:
 - Copy all files in C:\Windows\System32\config
 - Copy Default, Sam, Security, Software, and System files from C:\Windows\Repair to C:\Windows\System32\config

Editing the Registry (continued)

- To back up a particular key and its subkeys:
 - Use registry editor and Export feature
- Changes to the registry:
 - Are immediate
 - No undo feature

Registry Editor

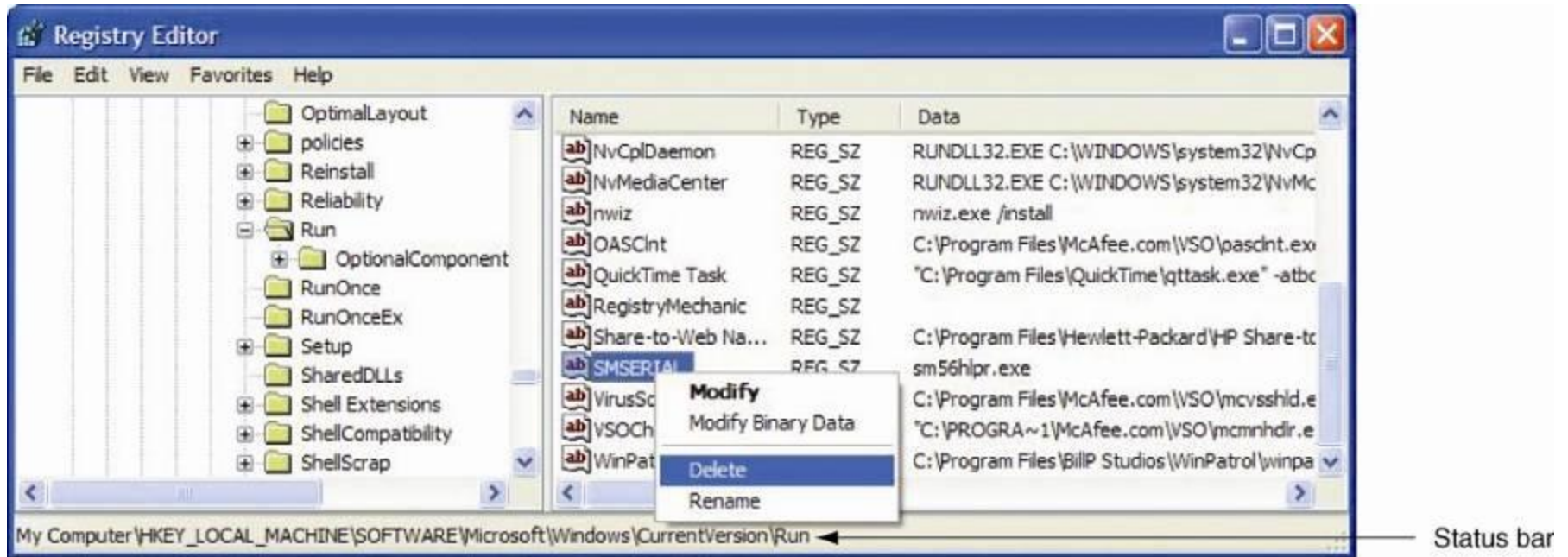


Figure 2-30 Right-click a value to modify, delete, or rename it

Manually Removing Software

- Typical result of installing and uninstalling software:
 - More files and folders
 - Larger registry
- To uninstall software:
 - Use uninstall routine (All Programs), if available
 - Next, click Remove in Add or Remove Programs window if software still visible
 - Finally, try manually deleting software

Manually Removing Software (continued)

- To manually remove software:
 - Locate folder that contains the software
 - Delete the folder
- Delete registry entries for programs in Add or Remove Programs window:
 - Locate and backup key:
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall
 - Locate software to be deleted
 - Delete the key

Subkey under the Uninstall Key

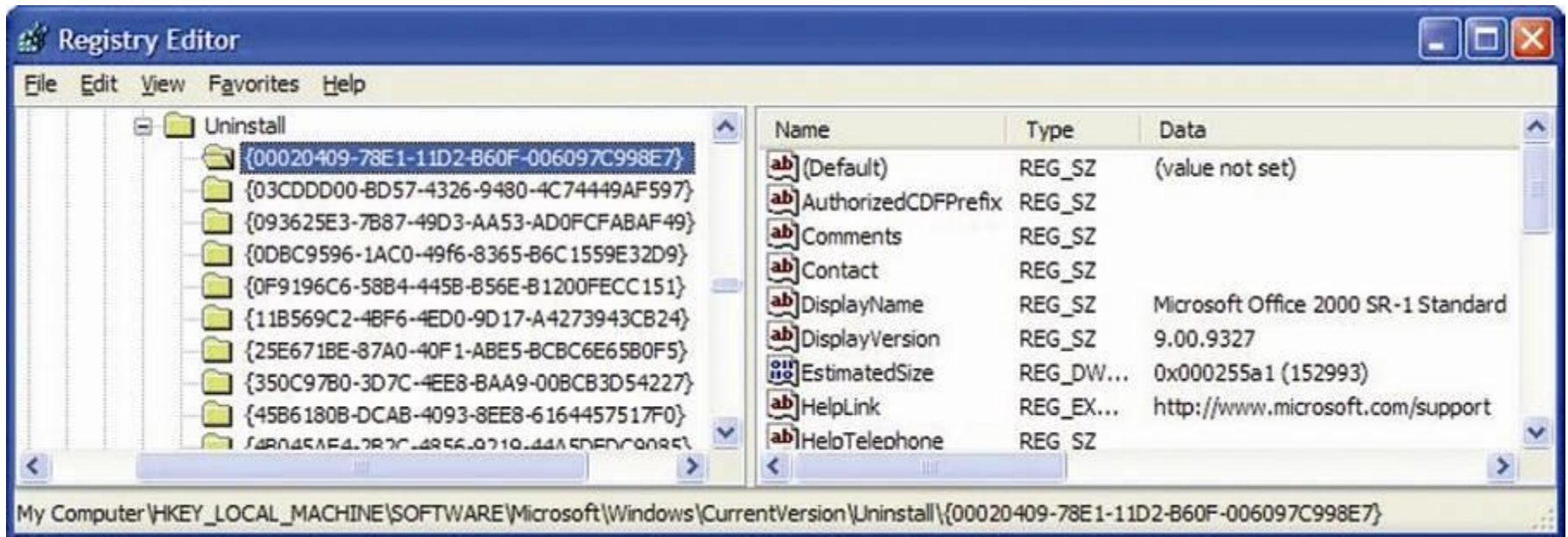


Figure 2-33 Select a subkey under the Uninstall key to display its values and data in the right pane

Manually Removing Software (continued)

- Some registry keys:
 - Affect startup and logon events
 - Cause an entry to run once and only once at startup
 - HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
 - HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
 - HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
 - HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

Manually Removing Software (continued)

- Group Policy places entries in:
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
 - HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- Windows loads DLL programs from:
 - HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
- Windows XP Tweak UI places entries in:
 - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
 - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

Manually Removing Software (continued)

- Entries in the following keys apply to all users:
 - HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows
 - HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
 - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
 - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Contains entries that pertain to background services sometimes launched at startup:
 - HKLM\System\CurrentControlSet\Control\Services

Manually Removing Software (continued)

- The following contains BootExecute, normally set to autochk
 - HKLM\System\CurrentControlSet\Control\Session Manager
- Keys known to cause problems at startup:
 - 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

Manually Removing Software (continued)

- 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

Third-party Tools

- Process Manager by Sysinternals
- WinTasks Pro by Uniblue
- Autoruns by Sysinternals
- Startup Control Panel by Mike Lin

Third-party Tools (continued)

- Process Manager by Sysinternals
 - *www.sysinternals.com*
 - Use to smoke out processes, DLLs, and registry keys that elude Task Manager
 - Terminology:
 - Handle – a relationship between a process and a resource it has called into action
 - Open handle – a relationship that has not yet completed

Third-party Tools (continued)

- WinTasks Pro by Uniblue
 - *www.liutilities.com*
 - Displays information about running processes
 - Use to temporarily or permanently stop and start processes
 - Useful for researching unknown processes
 - Can measure memory and CPU usage

Third-party Tools (continued)

- Autoruns by Sysinternals
 - *www.sysinternals.com*
 - Finds startup and login programs not found by Msconfig and other third-party programs
 - Gives more information than Msconfig
 - Can view information while using Windows
 - Helps search for the way a listed item was started
 - Can save Autoruns information to a text file to keep a record of a current state

Third-party Tools (continued)

- Startup Control Panel by Mike Lin
 - www.mlin.net/StartupCPL.shtml
 - Can determine the source of a program more easily than Msconfig

Microsoft BootVis for Windows XP

- Used to evaluate startup performance problems for developers
- Initiates some optimization processes
 - May see a performance increase
 - Record time in seconds for Windows startup before and after running BootVis

Keep XP Startup Clean and Prepare for Disaster

- Learn:
 - What you can do to protect startup
 - Prepare in advance for problems

Back Up the System State

- Should back up system state as a routine task
- Can't restore system state from backup unless you can boot into Windows desktop

Make Sure System Restore Is Turned on and Use It

- Verify System Restore has not been turned off:
 - Go to System Restore tab in Properties in My Computer
 - Ensure Turn off System Restore unchecked
- Restore points:
 - Normally kept in C:\System Volume Information, which is not accessible to the user.
 - Are taken at least every 24 hours
 - Can use up to 12 percent of disk space

Make Sure System Restore Is Turned on and Use It (continued)

- If just after a Windows installation free hard drive space is less than 200 MB:
 - System Restore suspended until 200 MB available
- If hard drive free space less than 80 MB:
 - System Restore gives up some of its storage area
 - Fewer restore points kept
- If free drive less than 50 MB:
 - System Restore suspended until 200 MB available
- Can create a restore point manually

Monitor the Startup Process

- Use third-party tools to monitor any changes to startup process
 - WinPatrol by BillP Studios
 - Install to run in the background to monitor:
 - Changes to the registry
 - Startup processes
 - Internet Explorer settings
 - System files

WinPatrol by BillP Studios Alert



Figure 2-46 WinPatrol by BillP Studios alerts you when the startup process has been altered

Monitor the Startup Process (continued)

- Can catch malicious software by monitoring changes to the registry
- Regmon by Sysinternals
 - *www.sysinternals.com*
 - Useful for tweaking when and how an application accesses the registry

Summary

- Use Last Known Good Configuration to return configuration to its settings at last successful boot
- Windows XP Safe Mode:
 - Boots with a minimum of drivers and options installed
 - Can troubleshoot a failed boot or run antivirus software
- Use System Restore to return system settings to a time when a snapshot of the system was taken
- Use System Configuration Utility (Msconfig) to limit startup processes and services

Summary (continued)

- Use Task Manager to monitor, start, and stop programs running in Windows
- Folders containing startup programs and shortcuts:
 - All Users startup folder
 - Current User startup folder
 - Scheduled Task folder
- Launch service at startup by making an entry into the registry using the Services console
- Group Policy can affect:
 - Startup or logon
 - Launching scripts that can contain programs to run

Summary (continued)

- Too many loaded fonts can slow down startup
- Manually delete an application by deleting:
 - Its folder in the C:\Program Files folder
 - Its entries in the registry
- Use the Backup tool to back up the system state
- Use the Export command to back up an individual key and its subkeys
- Use third-party software to monitor Windows events