

## Local Machine – Hardening and Customization Handout

Listed below are some common settings that one can use through registry edits to secure the default local machine on a Windows XP machine. Please note that many of these settings can be more easily modified if you have a directory service running where you can push out group policy items.

---

Windows Registry Editor Version 5.00

### **; Disables Simple File Sharing**

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]

"forceguest"=dword:00000000

### **; Disable File and Print Sharing on the machine itself**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Network]

"NoFileSharing"=dword:00000001

"NoPrintSharing"=dword:00000001

### **; Opt to not save the temp files from internet explorer**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache]

"Persistent"=dword:00000000

### **; Hide Share Passwords with Asterisks**

[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Network]

"HideSharePwds"="1"

### **; Disable dump file creation**

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]

"CrashDumpEnabled"=dword:00000000

### **; Disable Dr. Watson dump file creation**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug]

"Auto"="0"

### **; Enable Restrict Anonymous**

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]

"restrictanonymous"=dword:00000002

"restrictanonymoussam"=dword:00000001

### **; Disable default admin shares**

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]

; "AutoShareWks"=dword:00000000

**; Dissociate "Anonymous" from "Everyone"**

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]  
"everyoneincludesanonymous"=dword:00000000

**; Disable searching for Task Scheduled events and printers on network shares**

[-HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RemoteComputer\NameSpace\{D6277990-4C6A-11CF-8D87-00AA0060F5BF}]  
@="Scheduled Tasks"

**; Disable Language Bar**

[-HKEY\_CLASSES\_ROOT\CLSID\{540D8A8B-1C3F-4E32-8132-530F6A502090}]  
@="Language bar"  
"MenuTextPUI"="@%SystemRoot%\System32\msutb.dll,-325"

**; Disable Storage of .Net Passwords**

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa]  
"DisableDomainCreds"=dword:00000001

**; Enable NumLock On at Boot**

[HKEY\_USERS\.Default\Control Panel\Keyboard]  
"InitialKeyboardIndicators"="2"

**; Enable Windows Firewall**

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile]  
"EnableFirewall"=dword:00000001

**; Disable Messenger in Outlook Express**

[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Outlook Express]  
"Hide Messenger"=dword:00000002

**; Disable Error Reporting**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting]  
"DoReport"=dword:00000000

**; Disable Fast User Switching**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]  
"AllowMultipleTSSessions"=dword:00000000

**; Auto Restart Explorer After Crash**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]  
"AutoRestartShell"=dword:00000001

**; Run 16-bit applications in their own process**

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\WOW]  
"DefaultSeparateVDM"="Yes"

**; Prevent windows messenger from being run**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Messenger\Client]  
"PreventAutoRun"=dword:00000001  
"PreventRun"=dword:00000001

**; Make Windows Media Player Behave by disabling auto updates**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\MediaPlayer]  
"EnableAutoUpgrade"="no"

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsMediaPlayer]  
"DisableAutoUpdate"=dword:00000001

**; Modifying the Disk Check Autochk.exe Time-out (Scandisk Delay) Value from 10 seconds to 3 Seconds**

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager]  
"AutoChkTimeOut"=dword:00000003

**; Disable Automatic Restart in the event of a System Crash / BSOD**

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl]  
"AutoReboot"=dword:00000000

**; Disable sending error reports in Internet Explorer**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main]  
"IEWatsonEnabled"=dword:00000000  
"IEWatsonDisabled"=dword:00000001

**; Sets percentage of drive space to use for system restore**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRestore]  
"DiskPercent"=dword:00000010

**; Sets the login screen theme to the purple metallic theme**

[HKEY\_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\ThemeManager]  
"DllName"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,00,\  
74,00,25,00,5c,00,52,00,65,00,73,00,6f,00,75,00,72,00,63,00,65,00,73,00,5c,\  
00,74,00,68,00,65,00,6d,00,65,00,73,00,5c,00,4d,00,65,00,74,00,61,00,6c,00,\  
00

6c,00,69,00,63,00,53,00,68,00,61,00,64,00,65,00,73,00,5c,00,4d,00,65,00,74,\  
00,61,00,6c,00,6c,00,69,00,63,00,53,00,68,00,61,00,64,00,65,00,73,00,2e,00,\  
6d,00,73,00,73,00,74,00,79,00,6c,00,65,00,73,00,00,00  
"ColorName"="Purple"

**; Sets the login screen background to our custom splash**

[HKEY\_USERS\DEFAULT\Control Panel\Desktop]  
"Wallpaper"="C:\\Documents and Settings\\All Users\\Documents\\My  
Pictures\\HDS\_LoginWallpaper.bmp"

**; Completely disables autorun**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\IniFileMapping\Autorun.inf]  
@"@SYS:DoesNotExist"

[HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]  
"HonorAutorunSetting"=dword:00000001  
"NoDriveAutoRun"=dword:03ffffff  
"NoDriveTypeAutoRun"=dword:000000ff

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom]  
"AutoRun"=dword:00000013

**; Enables viewing of CHM files on local intranet**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\HTMLHelp]  
[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\HHRestrictions]  
"MaxAllowedZone"=dword:00000001  
"EnableFrameNavigationInSafeMode"=dword:00000001

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\HTMLHelp\1.x\ItssRestrictions]  
"MaxAllowedZone"=dword:00000001

**; Enables Automatic Updates to use the KSU WSUS server**

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]  
"WUServer"="http://susupdate.lan.ksu.edu"  
"WUStatusServer"="http://susupdate.lan.ksu.edu"

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]  
"RescheduleWaitTime"=dword:00000014  
"NoAutoRebootWithLoggedOnUsers"=dword:00000001  
"NoAutoUpdate"=dword:00000000  
"AUOptions"=dword:00000004

```
"ScheduledInstallDay"=dword:00000000  
"ScheduledInstallTime"=dword:00000002  
"UseWUserver"=dword:00000001
```

**; Configures Windows Time Server to synchronize the time for the computer with the KSU NTP server  
first before checking other outside sources**

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime\Servers]  
@="1"  
"1"="ntp.ksu.edu"  
"2"="time.windows.com"  
"3"="time.nist.gov"
```