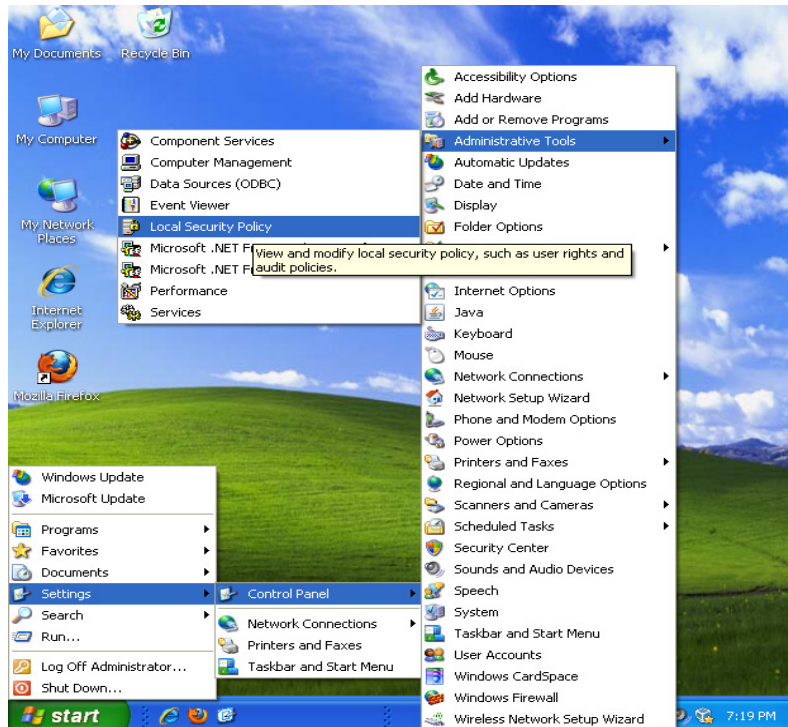


Implementing Software Restriction Policies

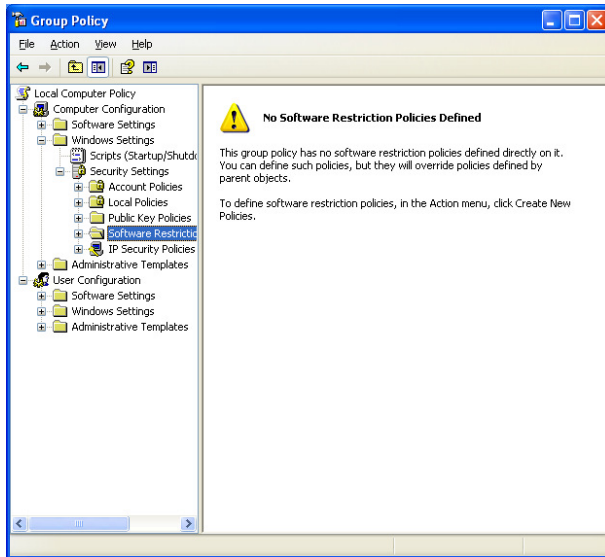
This is one of the options for implementing Software Restriction Policies using the built-in Microsoft tools. This is one way to protect systems in a workgroup. Local users should be users, not local administrators. For additional information, consult this page from the Microsoft site.

<http://technet.microsoft.com/en-us/windows/cc507878.aspx>

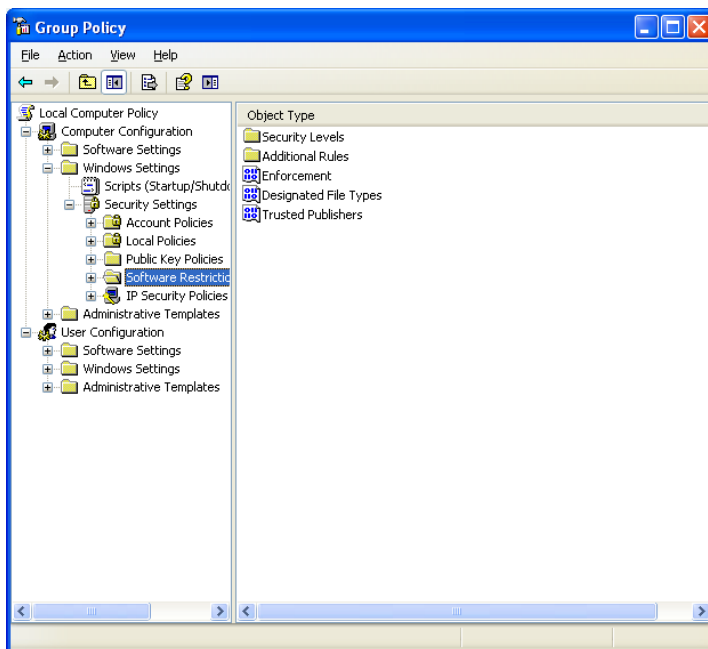
Open Local Software Security Settings Applet by either (Start/Run/gpedit.msc) or (Start/Settings/Control Panel/Administative Tools/Local Security Settings



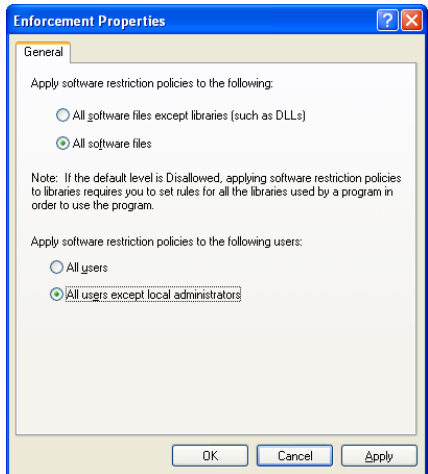
When you first open the applet there will be no policies. Expand the Computer Configuration/Windows Settings/Security Settings option.



Right Click on the Software Restriction Policies menu option and select Create New Policies. A blank set of policies will be created like the following image.



Double click the Enforcement option in the right pane under Object Type. Select All software files in the top radio button and All users except local administrators in the bottom section.



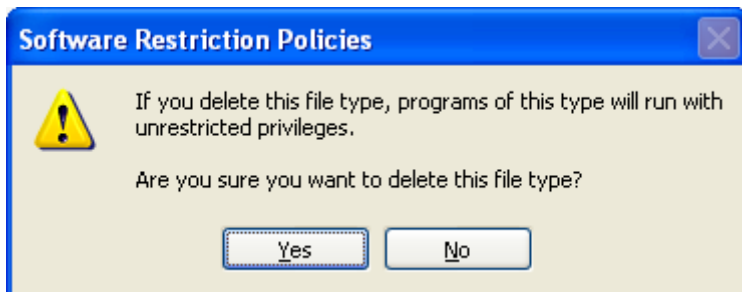
We recommend All software files, unless there becomes a performance issue as this is the most secure setting. From the MS technet site:

“DLL checking results in performance degradation. If a user runs 10 programs during a logon session, the software restriction policy is evaluated 10 times. If DLL checking is turned on, the software restriction policy is evaluated for each DLL load within each program. If each program uses 20 DLLs, this results in 10 executable program checks plus 200 DLL checks, so the software restriction policy is evaluated 210 times.”

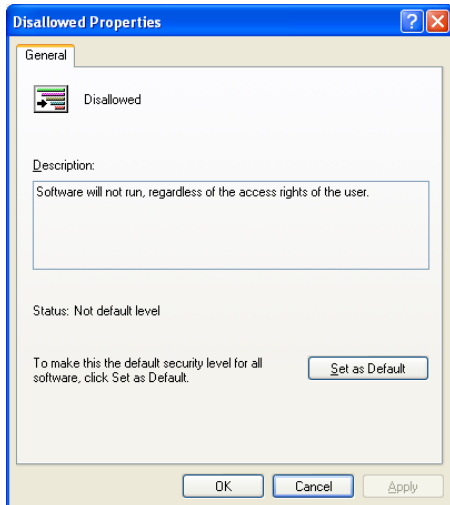
“ If the default security level is set to Disallowed, not only does the main executable file have to be identified to allow it to run, but all of its constituent DLLs must also be identified, which can be burdensome.”

Local users should NOT be running as local Administrators. If local users are in the local Administrators group, it might be better to select All users. Testing in each environment is recommended.

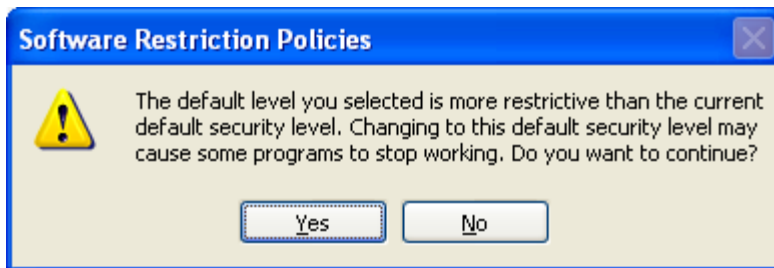
This SRP will be applied as a default policy. Open the Designated File Types option and remove the LNK option, otherwise shortcuts on the Start Menu will not function properly. The following dialog box appears



Select Yes and then Apply. The default policy is now created and needs to be applied. To apply the default Software Restriction Policy, expand the Security Levels option and select the Disallowed option. Double-click to open the Disallowed Properties dialog box as show below.



Select the Set as Default button and this applies the SRP for the computer. The following dialog box appears explaining you are creating a more restrictive policy.



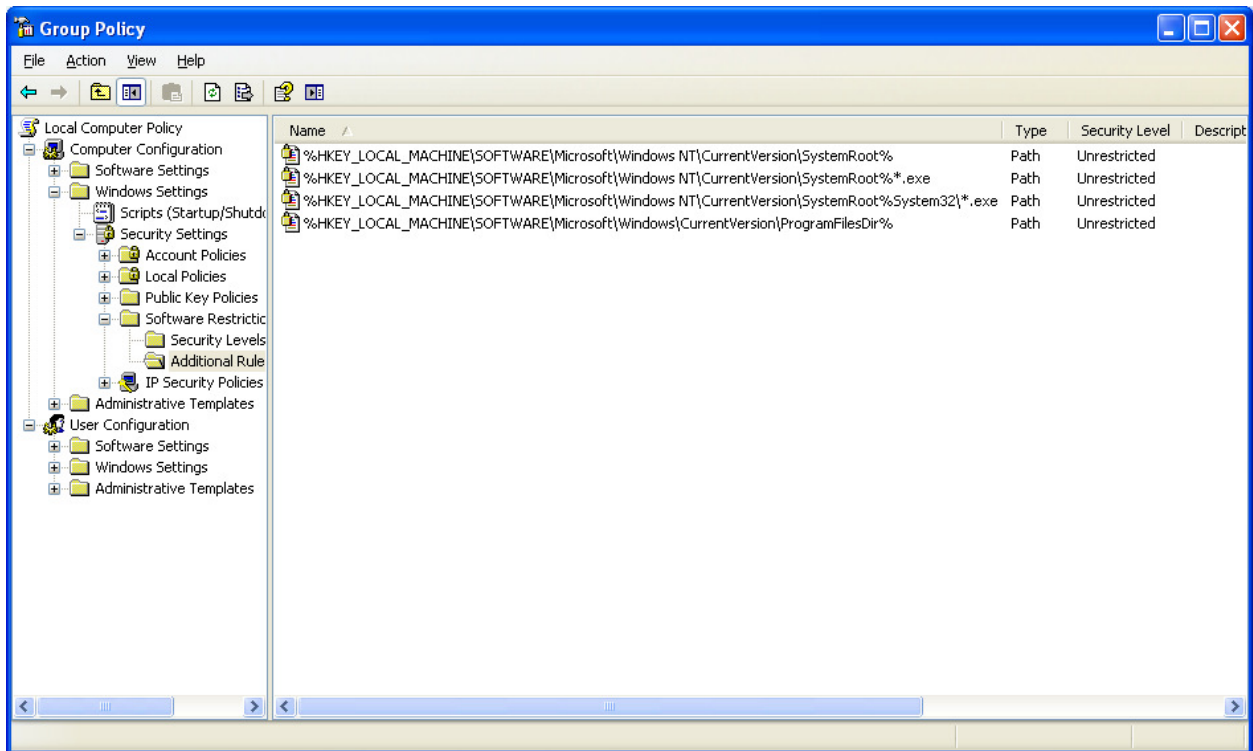
Click Yes and then OK in the resulting dialog box. Your system is now configured to disallow applications from running unless they are running from known directories. Select the Additional Rules menu option from the left menu tree and you can examine the default directories. The default rules allow unrestricted execution of applications from specific directories of the file system. While these are actually Registry Entries, they point to file system locations.

SystemRoot%

SystemRoot%*.exe

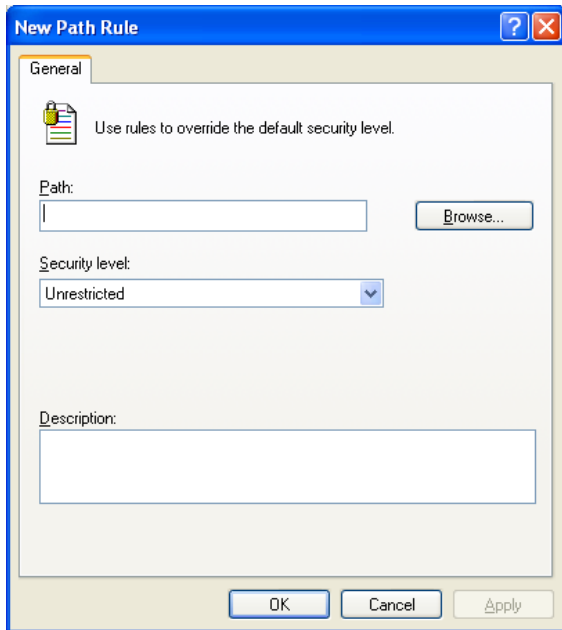
SystemRoot%System32*.exe

ProgramFilesDir%



By applying these rules, only software located in these directories will be allowed to run. If used in conjunction with restricting local users to running as users, not administrators, most malware files are unable to run. Since local users cannot create files in the SystemRoot% (c:\windows in most cases) or ProgramFilesDir% ("c:\program files" in most cases), and the SRP only allows execution of the files found in those directories, most malware is now rendered useless.

If it is discovered that an application is installed in a directory other than these identified in the default policy, it is very simple to add another folder. Right click in the right window pane and select New Path Rule... Notice there are other options for creating Certificate, Hash and Internet Zone Rules.



Browse to the directory and select the path. The default Security Level is Unrestricted. Any application in the newly selected directory will be allowed to run.

Any disallowed application that a users tries to run will be blocked and logged in the Application Error log.

If it is found that the SRP is too restrictive, it is quick to remove the default restriction. Select Security Levels and Assign the Unrestricted option for all users. The policy is effectively disabled at that point.

