

Prblm: Can't get Software Restrictions Policies to work as expected

Source:

http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.group_policy/2004-10/0032.html

From: Ola Theander (*ola.theander_at_otssystem.com*)

Date: 09/30/04

Date: Fri, 1 Oct 2004 01:43:44 +0200

Dear subscribers

I have a problem to get Software Restriction Policies (SRP) to work as expected. I'm administering a number of computers at a school and I use SRP to prevent use of disallowed software. My problem is that I find SRP to behave very peculiar; the way that I think would be the obvious way for it to work doesn't at all give the expected result. Of course I may have totally misunderstood things but in that case I hope for a clarification here.

Our environment is:

- Windows 2000 Server with AD, US version
- Windows XP Pro, Swedish version

I've read a lot of postings in the Microsoft Usenet groups and it seems like there might exist a bug in Windows XP that was fixed in sp2 that's concerning Netware shares (Q815471). We don't have any such shares, at least not as long as they aren't shared as such by default, so I'm not sure whether this bug applies to us.

Now to a description of the problem; the problem is that the user can't run applications that should be runnable, i.e. the user gets a message stating that the application was prevented to start due to software restrictions policies.

Our default policy configuration is to disallow running of applications, then we specify exactly which applications and in which paths applications are allowed to run. Our policy list is as follows:

Name	Type	Security level
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%	Path	Unlimited
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SystemRoot%*.exe	Path	Unlimited
%HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows		

microsoft.public.win2000.group_policy: Prblm: Can't get Software Restrictions Policies to work as expected

NT\CurrentVersion\SystemRoot%\System32*.exe Path Unlimited
*.js Path Not allowed
*.jse Path Not allowed
*.vbe Path Not allowed
*.vbs Path Not allowed
*.wsf Path Not allowed
*.wsh Path Not allowed
\\c0047\software\$* Path Unlimited
\\domain.se\SysVol* Path Unlimited
C:\Documents and Settings\%USERNAME%\Local Settings\Temp* Path Unlimited
C:\Documents and Settings\All Users\Desktop Path Unlimited
C:\Program Files* Path Unlimited
C:\WINDOWS* Path Unlimited

The polices are distributed using GPO in the Active Directory.

The strange thing is that some applications installed in "Program Files" runs perfectly e.g. Office but other third party applications can't start and I can't figure out why. There are some MS applications, e.g. Notepad, that doesn't start either.

I've studied the document "Using Software Restriction Policies to Protect Against Unauthorized Software"

<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx>

to configure SRP and in the Troubleshooting section it says that a denied SRP should be logged in the system event log but this doesn't occur so I can't get any information here, at least I can't find any log records. Do I need to do anything special to enable this logging?

Any help with this matter would be greatly appreciated.

Kind regards, Ola Theander