soundtraining.net
short-form training for IT professionals
PO Box 1321 Seahurst, Washington 9802-1321 USA Voice: 206.988.5858 Fax: 206.892.0499

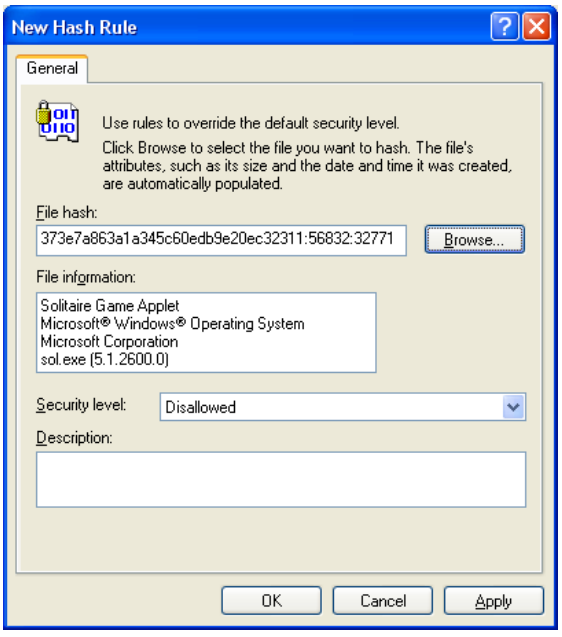
How-to Guide

Software Restriction through Group Policies

Group Policies include the ability to restrict the software applications that are allowed to run on systems configured with Windows 2000 or later. Although domain membership simplifies the application of Group Policies involving large numbers of systems, it is not required. Perhaps you want to prevent users from running games, peer-to-peer file swapping programs, or an instant messaging client. Perhaps you simply want to ensure that only authorized software is allowed to run on workplace computers. In either of these scenarios, Group Policy Software Restriction may be your solution.

In a domain environment, use the Microsoft Group Policy Management Console (if you haven't downloaded it yet, we recommend downloading it from the Microsoft web site). In a standalone workstation or peer-to-peer environment, use the Local Security Policies Microsoft Management Console.

Enable Group Policy Software Restriction by opening the Group Policy editor and navigating to either Computer Configuration or User Configuration>Windows Settings>Security Settings>Software Restrictions. Right-click on Software Restrictions and choose Create New Policies. (If software restriction policies have already been created, the "Create New Policies" option will not be available.) Expand Additional Rules and right-click in the white area. There are several options, all of which you should evaluate as solutions for software restriction. For the purpose of this guide, however, we'll consider only the New Hash Rule option. A hash is a numerical representation of a file created by a bit-by-bit analysis of that file. Using a hash allows you to apply restrictions to a file even if it's been renamed (the actual 1s and 0s of the file remain the same, so the hash remains the same). Choose New Hash Rule from the available options. In the dialog box that appears, you can browse for the software application you wish to restrict (you might want to use sol.exe for testing your policy settings--it's in c:\windows\system32). When you select the file you wish to restrict, the New Hash Rule applet will generate a hash



based on that file. Note that the default setting for the Security level is Disallowed, meaning that the application upon which the hash is based will not be allowed to run. Computers or users in the container where the policy is applied will receive a console message stating that the application has been restricted by a policy setting and will not be allowed to run that application.

Get more info here:

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

soundtraining.net's 2-day Windows Server 2003 workshop includes excellent coverage of Group Policies as part of its coverage of installing, configuring, optimizing, and troubleshooting. Offered in various locations as a public seminar and also in onsite training, available at the time and location of your choosing, this outstanding training program is a great solution for busy IT professionals who need to get up-to-speed quickly on Windows Server 2003.

More info including dates, locations, and a course outline is available at http://www.soundtraining.net

soundtraining.net is a privately-held Seattle, Washington-based firm specializing in short-form training for Information Technology professionals. We specialize in training on Microsoft, Cisco, and Linux products. Our one, two, and three-day seminars and workshops are specially designed for busy IT professionals who need the skills to work effectively with modern technology, but can't take the time to attend week-long (or longer) training sessions.

More information about soundtraining.net, including course listings, how-to guides, and other training resources is available online at www.soundtraining.net.