

Description of the Software Restriction Policies in Windows XP

This article was previously published under Q310791

Article ID	: 310791
Last Review	: July 26, 2002
Revision	: 1.0

SUMMARY

This article describes software restriction policies in Windows XP.

Administrators can use software restriction policies to allow software to run. By using a software restriction policy, an administrator can prevent unwanted programs from running. This includes viruses and Trojan horse software, or other software that is known to cause problems.

MORE INFORMATION

You can use the Group Policy tool in Windows XP to implement software restriction policies. To enable a software restriction policy, use either of the following methods:

- Using Group Policy
 1. Click **Start**, and then click **Run**.
 2. Type **gpedit.msc**, and then click **OK**.
 3. Expand the following items:
 - Computer Configuration**
 - Windows Settings**
 - Security Settings**
 - Software Restriction Policies**
- Using the Local Security Policy
 1. Click **Start**, and then click **Run**.
 2. Type **secpol.msc**, and then click **OK**.
 3. Follow the instructions to enable a policy.

The Default Security Level and Exceptions

You can configure the default security level and define additional rules that form exceptions to the default rules. The default security level determines the behavior for all programs. Additional rules provide exceptions to the default security level. The two security levels are:

- **Disallowed** - If you set **Disallowed** as the default rule, no programs are permitted. You must create additional rules that enable particular programs to run.

Using **Disallowed** as the default is not a good idea unless the administrator has a complete list of permitted programs.

- **Unrestricted** - If you set **Unrestricted** as the default rule, all programs are allowed to run. You must create additional rules if you want to restrict individual programs.

Unrestricted is best if the administrator does not have a complete list of permitted programs, but needs to prevent certain programs from running.

Additional Rules

You can configure several types of additional rules:

- Hash - With a Hash rule, the administrator lists the program file to be blocked or explicitly permitted. It is hashed, resulting in a cryptographic fingerprint that remains the same regardless of the file name or location. You can use this method to prevent a particular version of a program from running, or to prevent a program from running no matter where it is located.
- Certificate - You can build Certificate rules by providing a code-signing software publisher certificate. Like Hash rules, Certificate rules apply no matter where the program file is located or what it is named.
- Path - Path rules apply to all programs that run from the specified local or network path, or from subfolders that are in the path.
- Internet Zone - You can use Internet Zone rules to apply software restriction policy rules based on the Microsoft Internet Explorer security zone in which the program is run. Currently, these rules apply only to Microsoft Windows Installer packages that are run from the zone. Internet Zone rules do not apply to programs that are downloaded by Internet Explorer.

General Configuration Rules

In addition to the default security and additional rules, you can also define general configuration rules to determine how software restriction policies are applied on the computer. These include:

- Enforcement - You can use the Enforcement settings to determine which files are enforced, and which users are subject to the security restriction policy configuration. By default, all software files except libraries (such as dynamic-link libraries, or DLLs) are subject to the security restriction policy settings. You can configure the security restriction policies to apply to all software files. Note that this may require that you add rules for each library file that is required by a program.

By default, all users are subject to the security restriction policy settings on the computer. You can configure enforcement for all users except local administrators, which allows local administrators to run disallowed programs.

- Designated Files Types - You can use this policy to configure the file types to which the security restriction policy settings apply.
- Trusted Providers - You can use the Trusted Providers properties to configure which users can select trusted publishers. You can also determine which, if any, certificate revocation checks are performed before trusting a publisher.

APPLIES TO

- [Microsoft Windows XP Professional](#)

© 2006 Microsoft Corporation. All rights reserved.