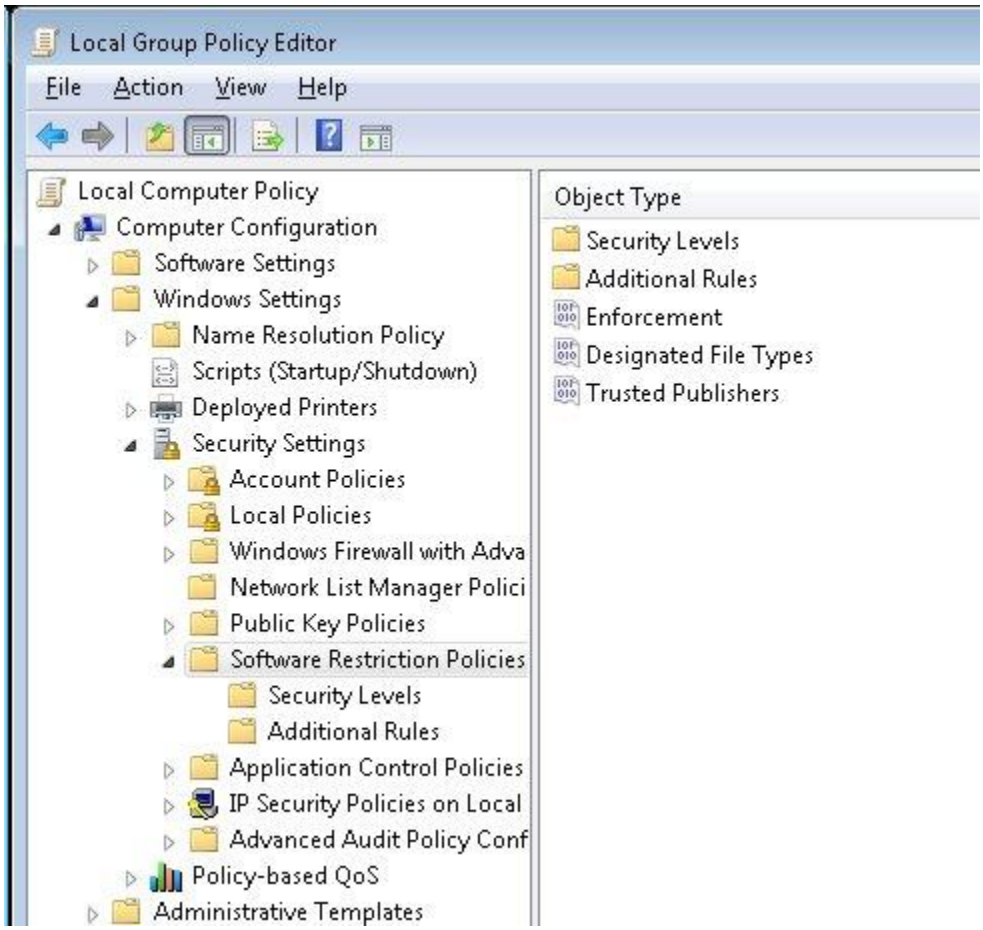
Software Restriction Policies:

Software restriction policies can help organizations protect themselves because they provide another layer of defense against viruses, Trojan horses, and other types of malicious software. You can configure the Software Restriction Policies settings in the following location within the Group Policy Management Console:

Computer Configuration\Windows Settings\Security Settings\Software Restriction Policies



Software restriction policies do not prevent restricted processes that run under the System account. For example, if a malicious program has set up a malicious service that starts under the Local System account, it starts successfully even if there is a software restriction policy configured to restrict it. A flawed software restriction policy implementation can disable necessary applications or allow malicious software to run.

A policy consists of a default rule that specifies whether programs are allowed to run and exceptions to that rule. The default rule can be set to *Unrestricted* (the program is allowed to run) or *Disallowed* (the program is not allowed to run). Setting the default rule to *Unrestricted* allows an administrator to define exceptions (programs that are not allowed to run). A more secure approach is to set the default rule to *Disallowed*, and specify only the programs that are known and trusted to run.

There are two ways to use software restriction policies:

- If an administrator knows all of the programs that should run, then a software restriction policy can be applied to allow only this list of trusted applications.

- If all the applications that users might run are not known, then administrators can disallow undesired applications or file types as needed.

Software Restriction Policies has four rules with which to identify software. The purpose of a rule is to identify one or more software applications, and specify whether or not they are allowed to run. Creating rules largely consists of identifying software that is an exception to the default rule. Each rule can include descriptive text to help communicate why the rule was created.

A software restriction policy supports the following four ways to identify software:

- Hash: A cryptographic fingerprint of the file.
- Certificate: A software publisher certificate that is used to digitally sign a file.
- Path: The local or universal naming convention (UNC) path of where the file is stored.
- Zone: The Internet zone as specified through Internet Explorer.