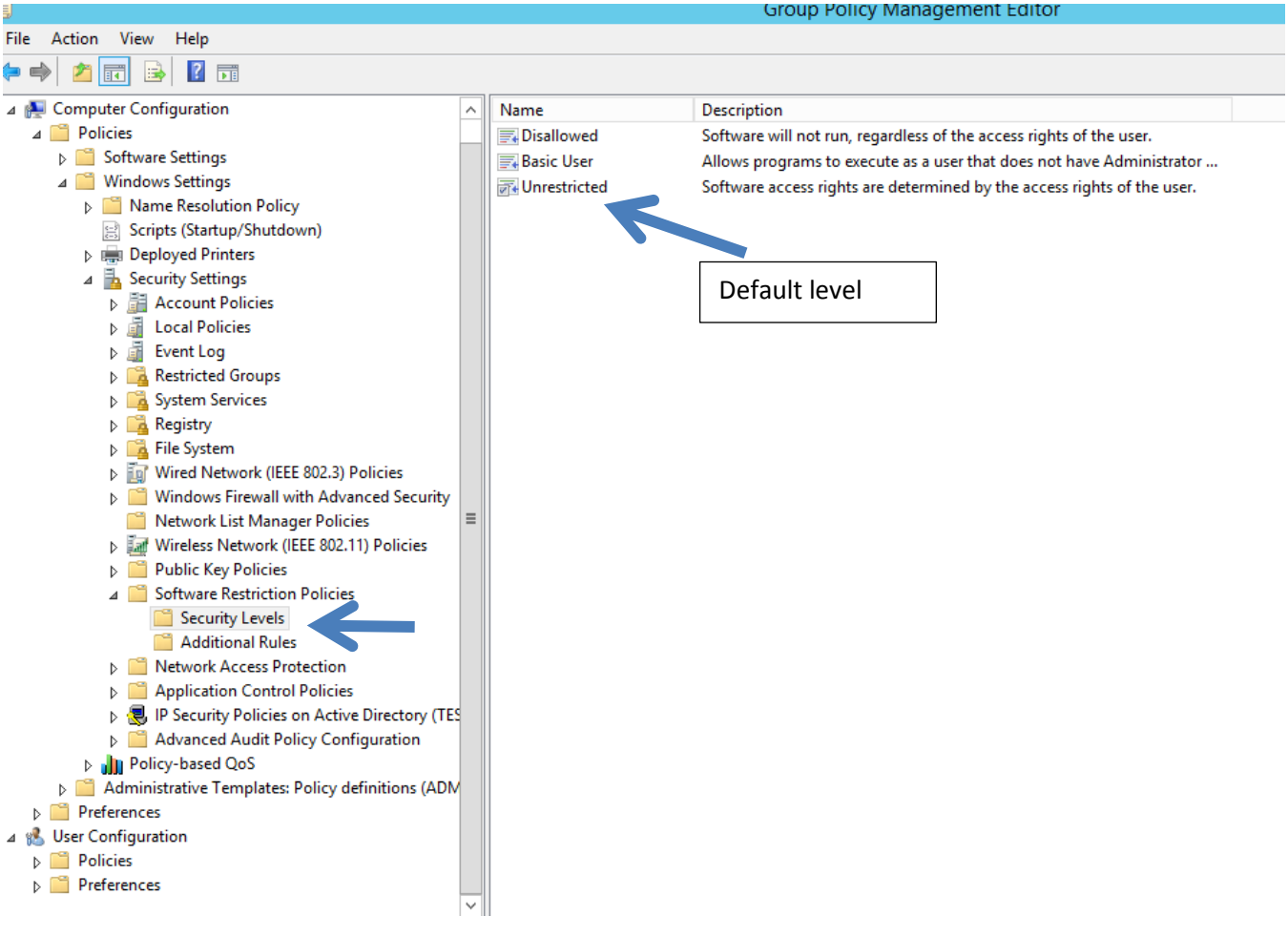
Software Restriction Policies: Software restriction policies can help organizations protect themselves because they provide another layer of defense against viruses, Trojan horses, and other types of malicious software. You can configure the Software Restriction Policies settings in the following location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

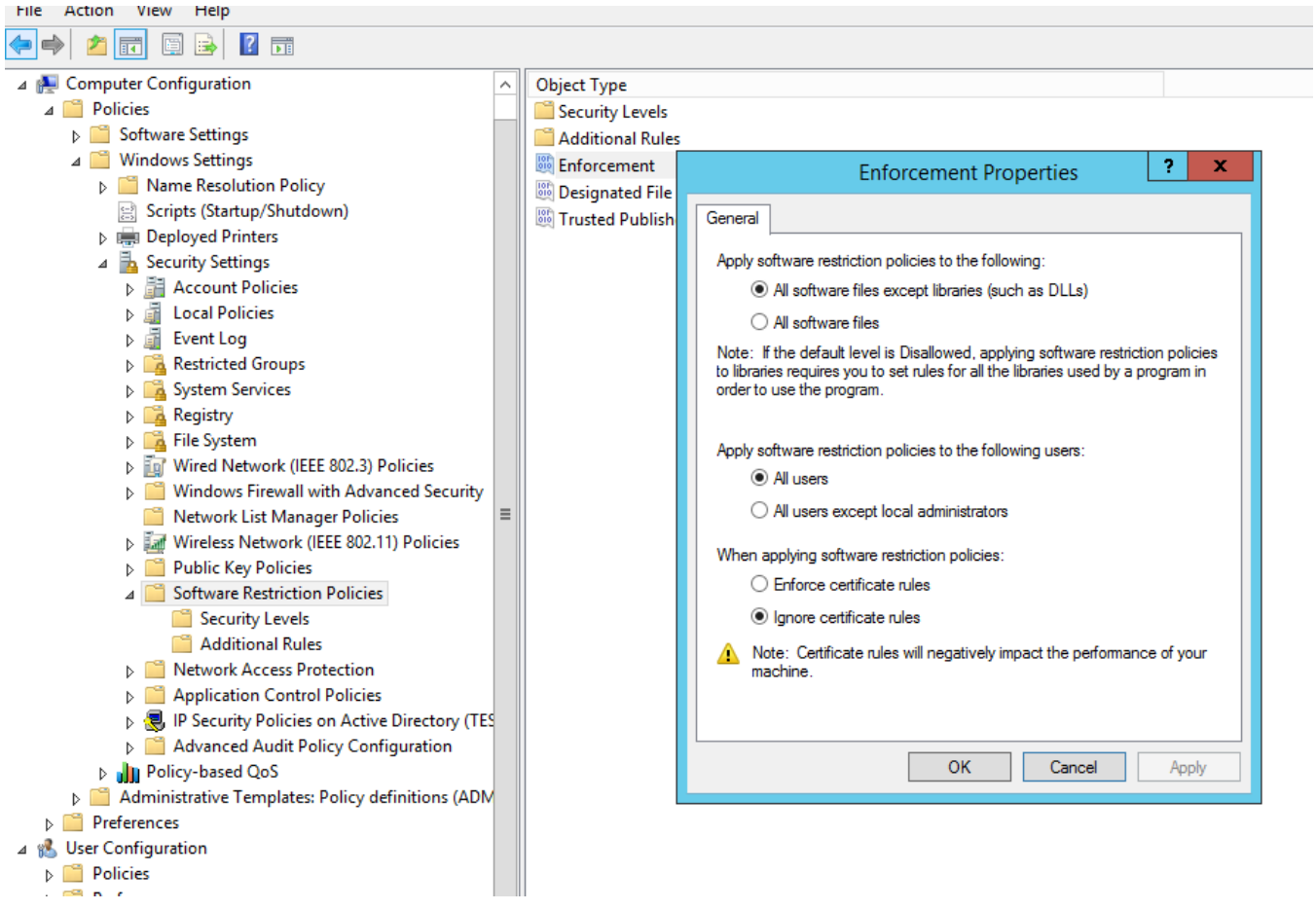
Software restriction policies do not prevent restricted processes that run under the System account. For example, if a malicious program has set up a malicious service that starts under the Local System account, it starts successfully even if there is a software restriction policy configured to restrict 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:

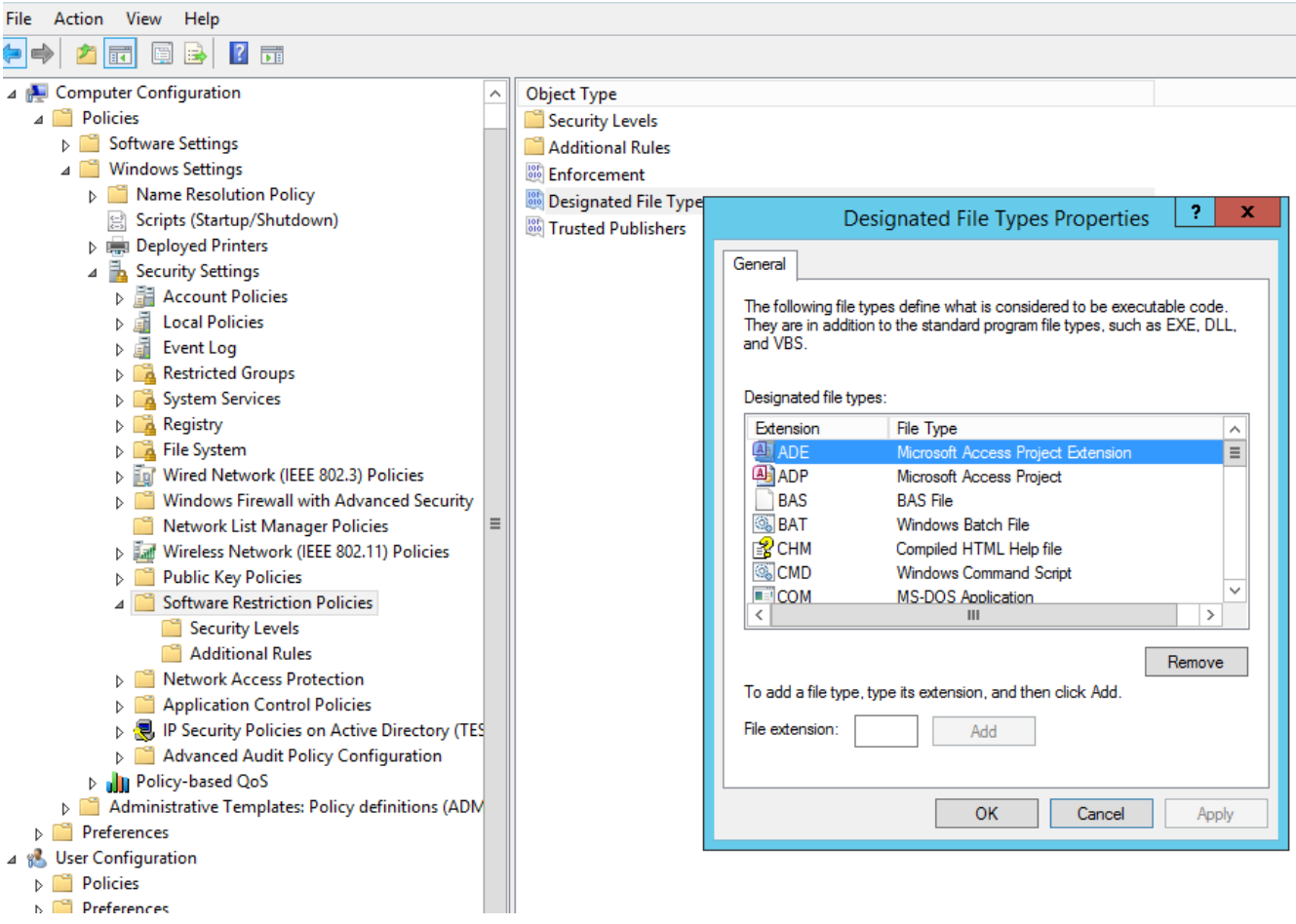
If an administrator knows all of the programs that should run, then a software restriction policy can be applied to allow only this list of trusted applications.

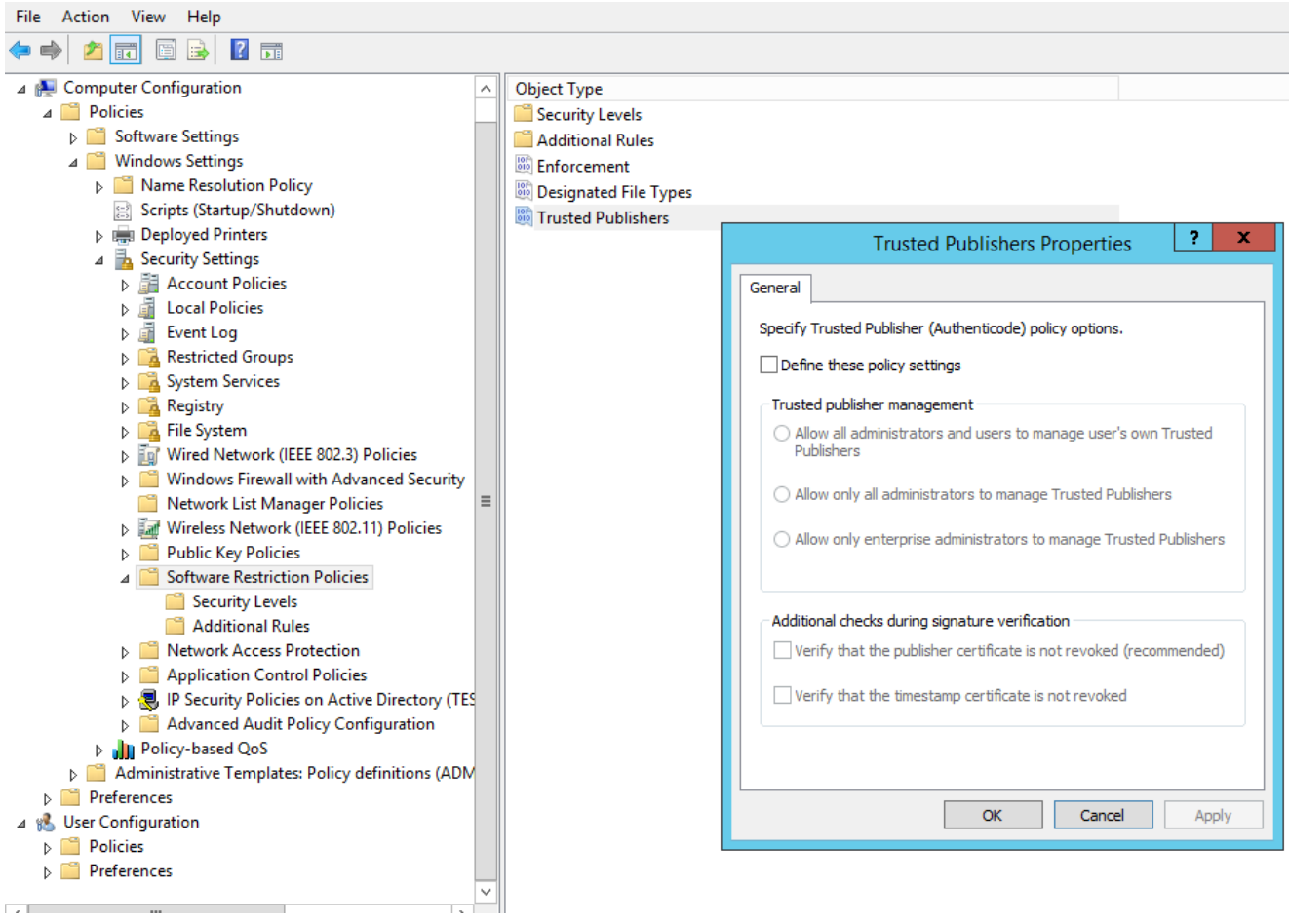
If all the applications that users might run are not known, then administrators can disallow undesired applications or file types as needed.

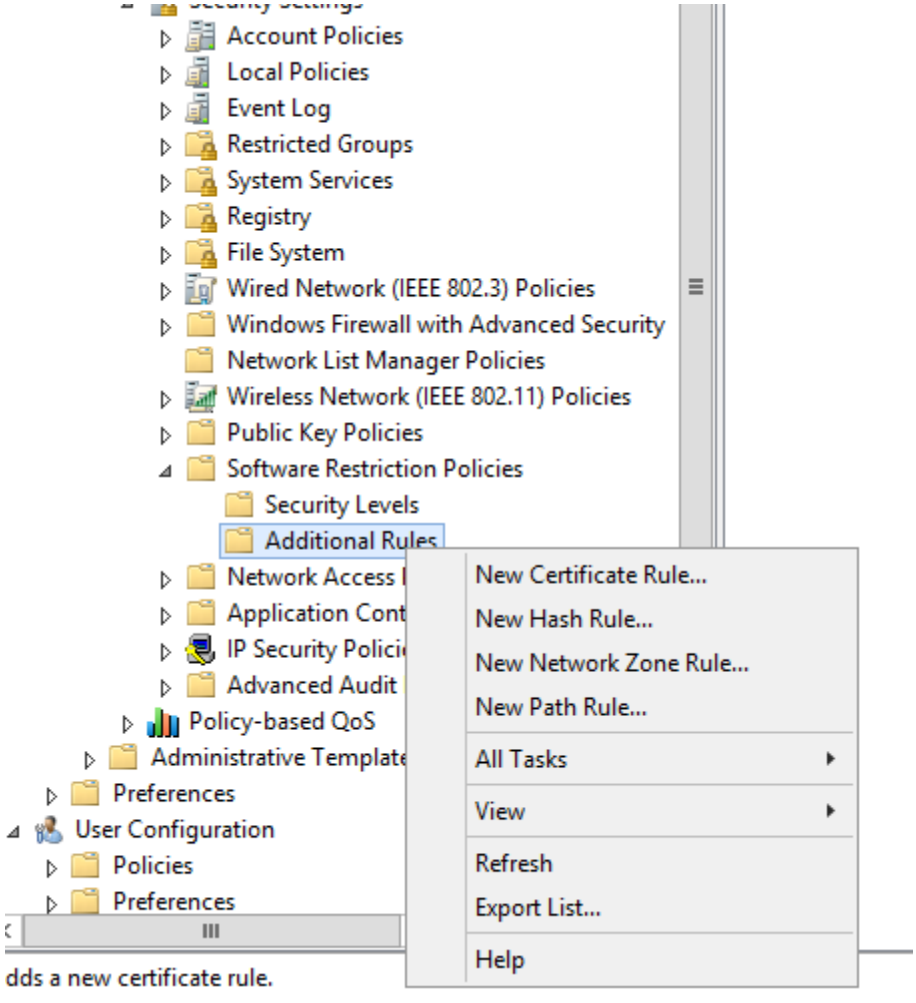
Software Restriction Policies has four rules with which to identify software. The purpose of a rule is to identify one or more software applications, and specify whether or not they are allowed to run. Creating rules largely consists of identifying software that is an exception to the default rule. Each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

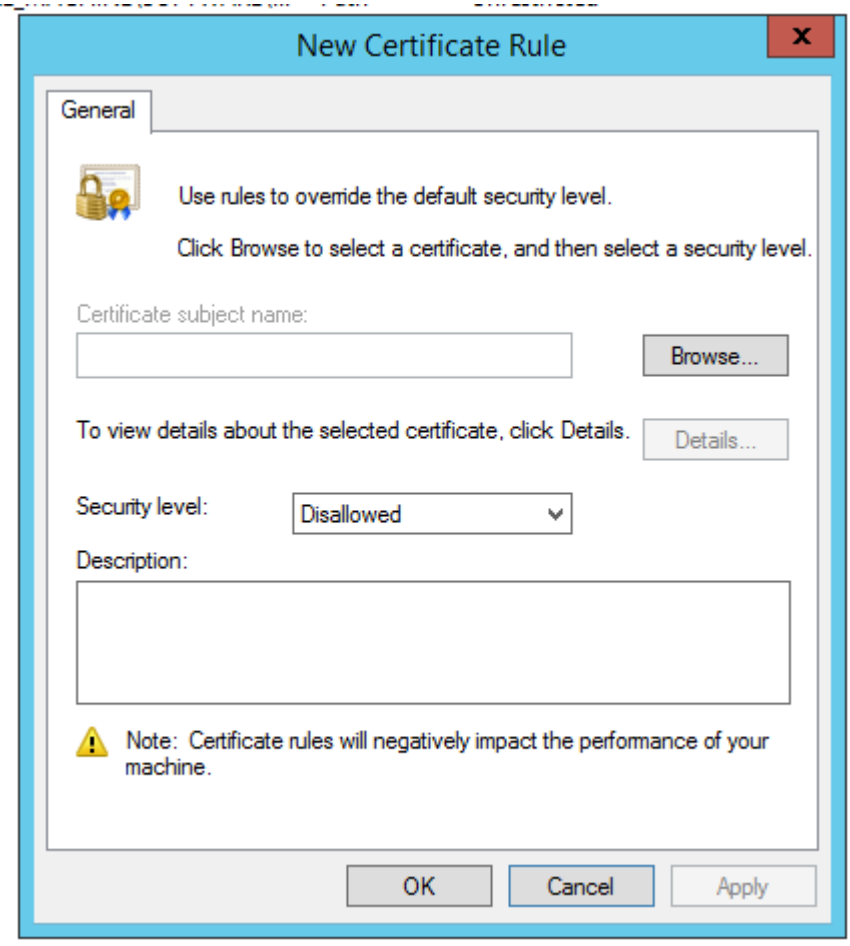


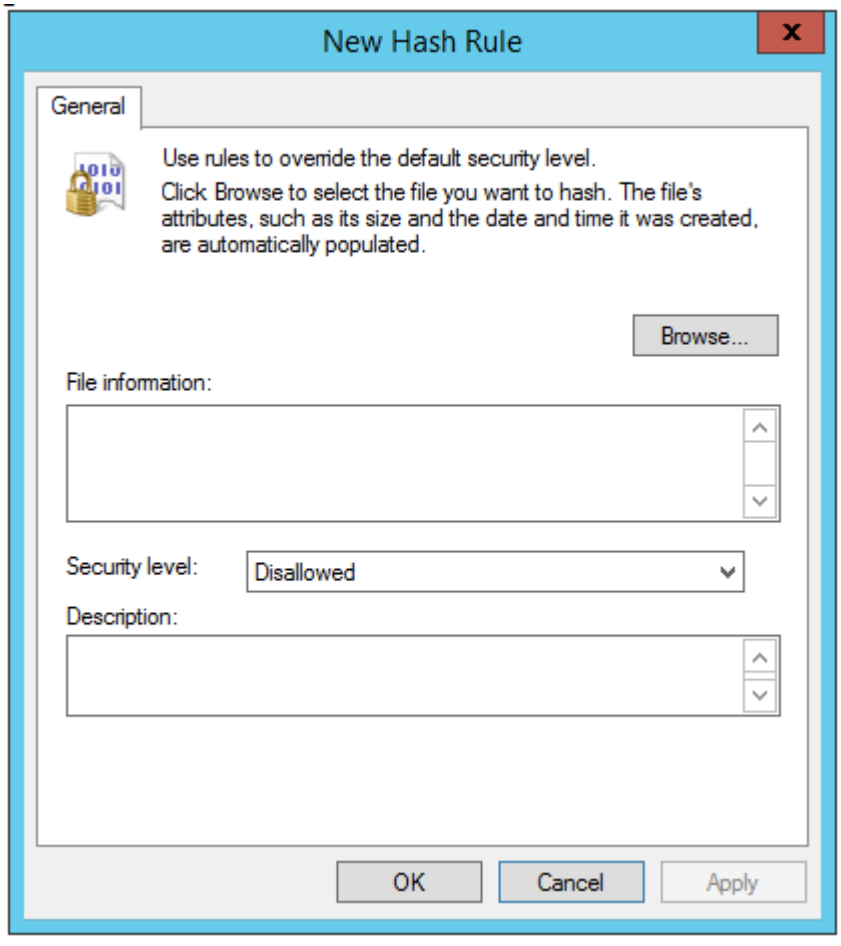

File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (TES
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADM
Preferences
User Configuration
Policies
Object Type
Security Levels
Additional Rules
Enforcement
Designated File
Trusted Publish
Enforcement Properties
General
Apply software restriction policies to the following:
All software files except libraries (such as DLLs)
All software files
Note: If the default level is Disallowed, applying software restriction policies to libraries requires you to set rules for all the libraries used by a program in order to use the program.
Apply software restriction policies to the following users:
All users
All users except local administrators
When applying software restriction policies:
Enforce certificate rules
Ignore certificate rules
Note: Certificate rules will negatively impact the performance of your machine.
OK
Cancel
Apply

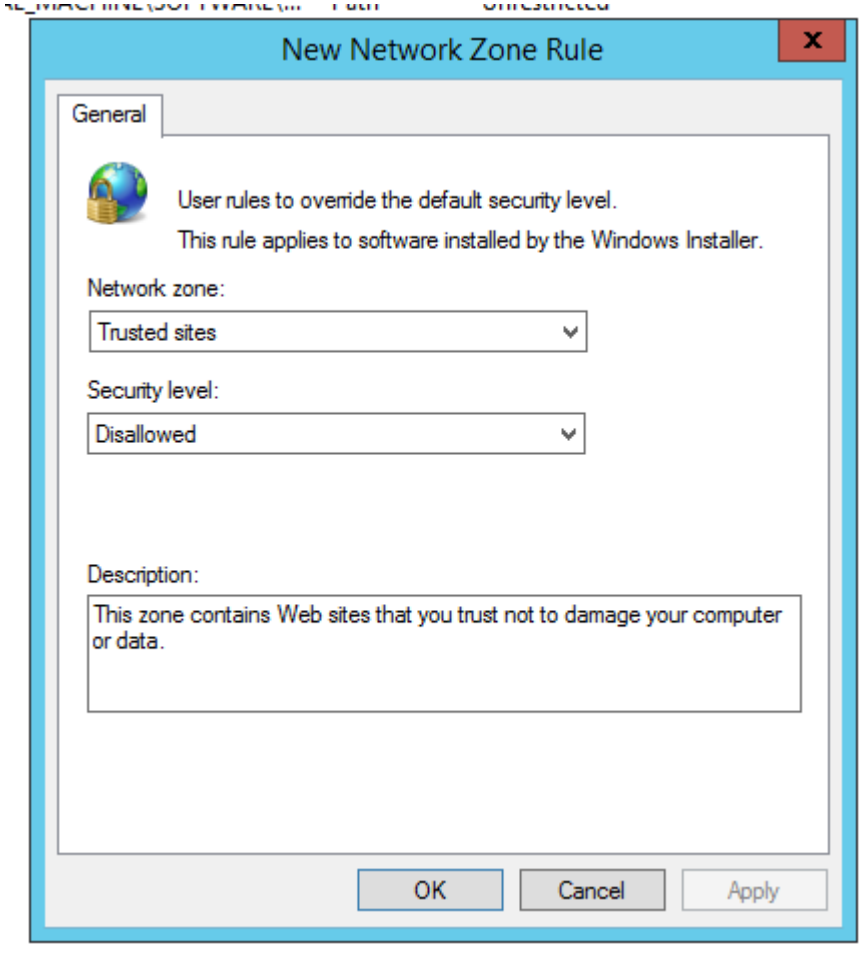

File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (TES
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADM
Preferences
User Configuration
Policies
Preferences
Object Type
Security Levels
Additional Rules
Enforcement
Designated File Type
Trusted Publishers
Designated File Types Properties
General
The following file types define what is considered to be executable code. They are in addition to the standard program file types, such as EXE, DLL, and VBS.
Designated file types:
Extension
File Type
ADE
Microsoft Access Project Extension
ADP
Microsoft Access Project
BAS
BAS File
BAT
Windows Batch File
CHM
Compiled HTML Help file
CMD
Windows Command Script
COM
MS-DOS Application
Remove
To add a file type, type its extension, and then click Add.
File extension:
Add
OK
Cancel
Apply

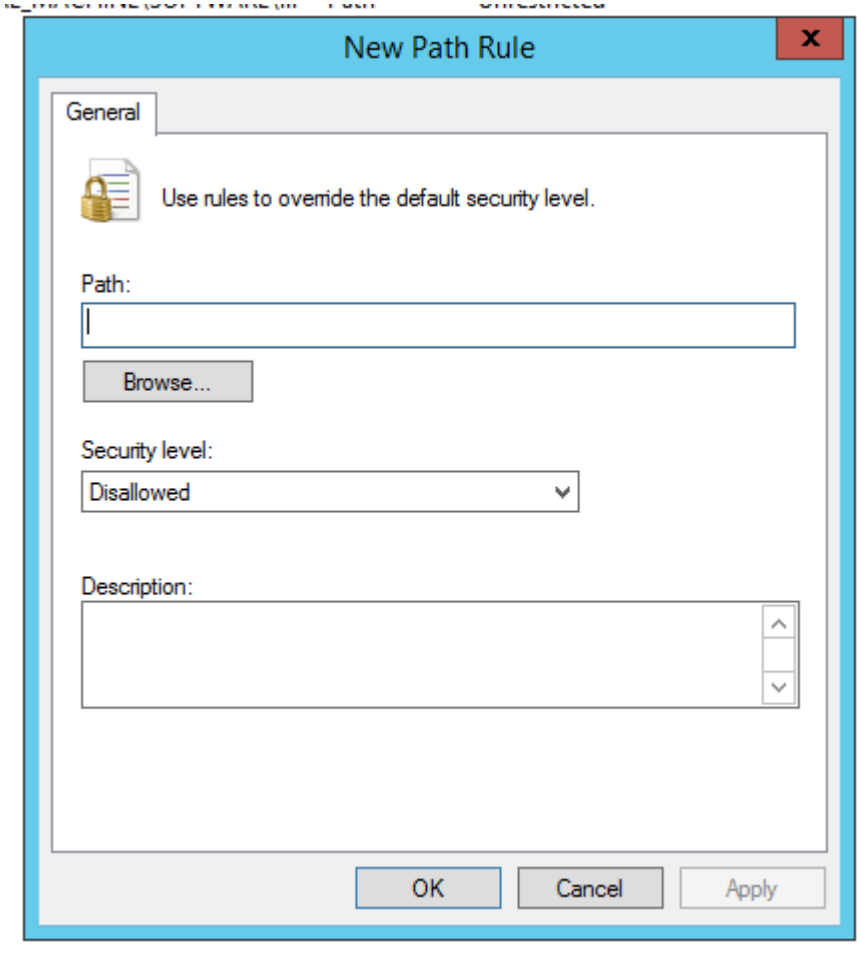

File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (TES
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADM
Preferences
User Configuration
Policies
Preferences
Object Type
Security Levels
Additional Rules
Enforcement
Designated File Types
Trusted Publishers
Trusted Publishers Properties
General
Specify Trusted Publisher (Authenticode) policy options.
Define these policy settings
Trusted publisher management
Allow all administrators and users to manage user's own Trusted Publishers
Allow only all administrators to manage Trusted Publishers
Allow only enterprise administrators to manage Trusted Publishers
Additional checks during signature verification
Verify that the publisher certificate is not revoked (recommended)
Verify that the timestamp certificate is not revoked
OK
Cancel
Apply


Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Security Levels
Additional Rules
Network Access
Application Cont
IP Security Polici
Advanced Audit
Policy-based QoS
Administrative Templat
Preferences
User Configuration
Policies
Preferences
New Certificate Rule...
New Hash Rule...
New Network Zone Rule...
New Path Rule...
All Tasks
View
Refresh
Export List...
Help
dds a new certificate rule.


New Certificate Rule
General
Use rules to override the default security level.
Click Browse to select a certificate, and then select a security level.
Certificate subject name:
Browse...
To view details about the selected certificate, click Details.
Details...
Security level:
Disallowed
Description:
Note: Certificate rules will negatively impact the performance of your machine.
OK
Cancel
Apply


New Hash Rule
General
Use rules to override the default security level.
Click Browse to select the file you want to hash. The file's attributes, such as its size and the date and time it was created, are automatically populated.
Browse...
File information:
Security level:
Disallowed
Description:
OK
Cancel
Apply


New Network Zone Rule
General
User rules to override the default security level.
This rule applies to software installed by the Windows Installer.
Network zone:
Trusted sites
Security level:
Disallowed
Description:
This zone contains Web sites that you trust not to damage your computer or data.
OK
Cancel
Apply


New Path Rule
General
Use rules to override the default security level.
Path:
Browse...
Security level:
Disallowed
Description:
OK
Cancel
Apply