Software Restriction Policy

Introduced in the Windows XP operating system and the Windows Server 2003 operating system, SRPs give administrators tools that they can use to identify and specify which applications can run on client computers. You configure and deploy SRP settings to clients by using Group Policy.

Windows Server 2012 uses SRPs to provide Windows Vista® compatibility. An SRP set is made up of rules and security levels.

Rules

Rules govern how SRP responds to an application that is being run or installed. Rules are the key constructs within an SRP, and a group of rules together determines how an SRP responds to applications that are being run. Rules can be based on one of the following criteria that apply to the primary executable file for the application in question:

- Hash. A cryptographic fingerprint of the file.
- Certificate. A software publisher certificate that is used to sign a file digitally.
- Path. The local or Universal Naming Convention (UNC) path to where the file is stored.
- Zone. The Internet zone.

Security Levels

Each applied SRP is assigned a security level that governs the way that the operating system reacts when the application that is specified in the rule is run. The three available security levels include:

- Disallowed. The software identified in the rule will not run, regardless of the access rights of the user.
- Basic User. Allows the software identified in the rule to run as a standard, nonadministrative user.
- Unrestricted. Allows the software identified in the rule to run unrestricted by SRP.

Using these three settings, there are two primary ways to use SRPs:

- If an administrator has a comprehensive list of all the software that is allowed to run on clients, the Default Security Level can be set to Disallowed. All applications that are allowed to run can be identified in SRP rules that apply either the Basic User or Unrestricted security level to each individual application, depending on the security requirements.
- If an administrator does not have a comprehensive list of the software that is allowed to run on clients, the Default Security Level can be set to Unrestricted or Basic User, depending on security requirements. All applications that are not allowed to run can then be identified in SRP

rules, which would use a security level setting of Disallowed.

You can configure settings for SRPs by accessing the following location from the GPMC:

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

AppLocker

AppLocker, which was introduced in the Windows 7 operating system and Windows Server 2008 R2, is a security setting feature that controls which applications users are allowed to run.

AppLocker provides administrators several methods with which they can quickly and concisely determine the identity of applications that they may want to restrict, or to which they may want to permit access. You apply AppLocker through Group Policy to computer objects within an OU. You also can apply Individual AppLocker rules to individual AD DS users or groups.

AppLocker also contains options for monitoring or auditing the application of rules. AppLocker can help organizations prevent unlicensed or malicious software from running, and can selectively restrict ActiveX® controls from being installed. It also can reduce the total cost of ownership by ensuring that workstations are standardized across the enterprise, and that users are running only the software and applications that are approved by the enterprise.

By using AppLocker technology, companies can reduce administrative overhead and help administrators control how users can access and use files, such as .exe files, scripts, Windows Installer files (.msi and .msp files), dynamic-link libraries (DLLs), and packaged applications, such as Windows Store apps.

You can use AppLocker to restrict software that:

- Is not allowed to be used in the company. For example, software that can disrupt employees' business productivity, such as social networking software, or software that streams video files or pictures that can use large amounts of network bandwidth and disk space.
- Is no longer used or it has been replaced with a newer version. For example, software that is no longer maintained, or for which licenses have expired.
- Is no longer supported in the company. Software that is not updated with security updates might pose a security risk.
- Should be used only by specific departments.

You can configure settings for AppLocker by accessing the following location from the GPMC:

Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies

- **Note:** AppLocker uses the Application Identity service to verify a file's attributes. You should configure this service to start automatically on each computer where AppLocker will be applied. If the Application Identity service is not running, then AppLocker policies are not enforced.

AppLocker defines rules based on file attributes that are derived from the digital signature of the file. File attributes in the digital signature include:

- Publisher name
- Product name
- File name
- File version

Default Configuration

By default, no AppLocker policies are defined. This means that no applications are blocked. However, you can configure default rules for each rule collection to ensure that applications in the Program Files and Windows directories are allowed to run, and all applications are allowed to run for the Administrators group. You should enable the default rules if you are going to implement AppLocker policies, because these applications are necessary for Windows operating systems to run and operate normally.

Allow and Deny Rule Actions

Allow and Deny are rule actions that allow or deny execution of applications based on a list of applications that you configure. The Allow action on rules limits execution of applications to an allowed list of applications, and blocks everything else. The Deny action on rules takes the opposite approach and allows the execution of any application except those on a list of denied applications. These actions also provide a means to identify exceptions to those actions