Software Restriction Policies

Article • 01/16/2023 • 8 contributors

Feedback

In this article

> Applies to: Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic for the IT professional describes Software Restriction Policies (SRP) in Windows Server 2012 and 2016 and Windows 8, and provides links to technical information about SRP beginning with Windows Server 2003.

> ⓘ **Important**
>
> Software Restriction Policies were deprecated beginning with Windows 10 build 1803 and also applies to Windows Server 2019 and above. You should use Windows Defender Application Control (WDAC) or AppLocker to control what software runs.

For procedures and troubleshooting tips, see Administer Software Restriction Policies and Troubleshoot Software Restriction Policies.

Software Restriction Policies description

Software Restriction Policies (SRP) is Group Policy-based feature that identifies software programs running on computers in a domain, and controls the ability of those programs to run. Software restriction policies are part of the Microsoft security and management strategy to assist enterprises in increasing the reliability, integrity, and manageability of their computers.

You can also use software restriction policies to create a highly restricted configuration for computers, in which you allow only specifically identified applications to run. Software restriction policies are integrated with Microsoft Active Directory and Group Policy. You can also create software restriction policies on stand-alone computers. Software restriction policies are trust policies, which are regulations set by an administrator to restrict scripts and other code that is not fully trusted from running.

You can define these policies through the Software Restriction Policies extension of the Local Group Policy Editor or the Local Security Policies snap-in to the Microsoft Management Console (MMC).

For in-depth information about SRP, see the Software Restriction Policies Technical Overview.

Practical applications

Administrators can use software restriction policies for the following tasks:

- Define what is trusted code
- Design a flexible Group Policy for regulating scripts, executable files, and ActiveX controls

Software restriction policies are enforced by the operating system and by applications (such as scripting applications) that comply with software restriction policies.

Specifically, administrators can use software restriction policies for the following purposes:

- Specify which software (executable files) can run on clients
- Prevent users from running specific programs on shared computers
- Specify who can add trusted publishers to clients
- Set the scope of the software restriction policies (specify whether policies affect all users or a subset of users on clients)
- Prevent executable files from running on the local computer, organizational unit (OU), site, or domain. This would be appropriate in cases when you are not using software restriction policies to address potential issues with malicious users.

New and changed functionality

There are no changes in functionality for Software Restriction Policies.

Removed or deprecated functionality

There is no removed or deprecated functionality for Software Restriction Policies.

Software requirements

The Software Restriction Policies extension to the Local Group Policy Editor can be accessed through the MMC.

The following features are required to create and maintain software restriction policies on the local computer:

- Local Group Policy Editor
- Windows Installer
- Authenticode and WinVerifyTrust

If your design calls for domain deployment of these policies, in addition to the above list, the following features are required:

- Active Directory Domain Services
- Group Policy

Server Manager information

Software Restriction Policies is an extension of the Local Group Policy Editor and is not installed through Server Manager, Add Roles and Features.

See also

The following table provides links to relevant resources in understanding and using SRP.

⛶ Expand table

Content type	References
Product evaluation	Application Lockdown with Software Restriction Policies
Planning	Software Restriction Policies Technical Overview (Windows Server 2012) Software Restriction Policies Technical Reference (Windows Server 2003)
Deployment	No resources available.
Operations	Administer Software Restriction Policies (Windows Server 2012) Software Restriction Policies Product Help (Windows Server 2003)
Troubleshooting	Troubleshoot Software Restriction Policies (Windows Server 2012) Software Restriction Policies Troubleshooting (Windows Server 2003)
Security	Threats and Countermeasures for Software Restriction Polices (Windows Server 2008) Threats and Countermeasures for Software Restriction Polices (Windows Server 2008 R2)
Tools and settings	Software Restriction Policies Tools and Settings (Windows Server 2003)
Community resources	Application Lockdown with Software Restriction Policies

Feedback

Was this page helpful? Yes No

English (United States) Your Privacy Choices Theme

Manage cookies Previous Versions Blog Contribute Privacy Terms of Use Trademarks