Software Restriction Policies

Article • 01/16/2023 • 3 minutes to read

> 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.

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)

Content type	References
Community resources	Application Lockdown with Software Restriction Policies

Software Restriction Policies Technical Overview

Article • 07/29/2021 • 12 minutes to read

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic describes software restriction policies, when and how to use the feature, what changes have been implemented in past releases, and provides links to additional resources to help you create and deploy software restriction policies beginning with Windows Server 2008 and Windows Vista.

Introduction

Software restriction policies provide administrators with a Group Policy-driven mechanism to identify software and control its ability to run on the local computer. These policies can be used to protect computers running Microsoft Windows operating systems (beginning with Windows Server 2003 and Windows XP Professional) against known conflicts and safeguard the computers against security threats such as malicious viruses and Trojan horse programs. 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. The Software Restriction Policies extension to the Local Group Policy Editor provides a single user interface through which the settings for restricting the use of applications can be managed on the local computer or throughout a domain.

Procedures

- Administer Software Restriction Policies
    - Determine Allow-Deny List and Application Inventory for Software Restriction Policies
    - Work with Software Restriction Policies Rules

    - Use Software Restriction Policies to Help Protect Your Computer Against an Email Virus

- Troubleshoot Software Restriction Policies

Software restriction policy usage scenarios

Business users collaborate by using e-mail, instant messaging, and peer-to-peer applications. As these collaborations increase, especially with the use of the Internet in business computing, so do the threats from malicious code, such as worms, viruses, and malicious user or attacker threats.

Users might receive hostile code in many forms, ranging from native Windows executable files (.exe files), to macros in documents (such as .doc files), to scripts (such as .vbs files). Malicious users or attackers often use social engineering methods to get users to run code containing viruses and worms. (Social engineering is a term for tricking people into revealing their password or some form of security information.) If such code is activated, it can generate denial-of-service attacks on the network, send sensitive or private data to the Internet, put the security of the computer at risk, or damage the contents of the hard disk drive.

IT organizations and users must be able to determine which software is safe to run and which is not. With the large numbers and forms that hostile code can take, this becomes a difficult task.

To help protect their network computers from both hostile code and unknown or unsupported software, organizations can implement software restriction policies as part of their overall security strategy.

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 client computers

- Prevent users from running specific programs on shared computers
- Specify who can add trusted publishers to client computers
- Set the scope of the software restriction policies (specify whether policies affect all users or a subset of users on client computers)
- 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.

Differences and changes in functionality

There are no changes in functionality in SRP for Windows Server 2012 and Windows 8.

Supported versions

Software Restriction Policies can only be configured on and applied to computers running at least Windows Server 2003, including Windows Server 2012 , and at least Windows XP, including Windows 8.

> ⓘ Note
>
> Certain editions of the Windows client operating system beginning with Windows Vista do not have Software Restrictions Policies. Computers not administered in a domain by Group Policy might not receive distributed policies.

Comparing application control functions in Software Restriction Policies and AppLocker

The following table compares the features and functions of the Software Restriction Policies (SRP) feature and AppLocker.

Application control function	SRP	AppLocker
Scope	SRP policies can be applied to all Windows operating systems beginning with Windows XP and Windows Server 2003.	AppLocker policies apply only to Windows Server 2008 R2, Windows Server 2012 , Windows 7, and Windows 8.

Application control function	SRP	AppLocker
Policy creation	SRP policies are maintained through Group Policy and only the administrator of the GPO can update the SRP policy. The administrator on the local computer can modify the SRP policies defined in the local GPO.	AppLocker policies are maintained through Group Policy and only the administrator of the GPO can update the policy. The administrator on the local computer can modify the AppLocker policies defined in the local GPO. AppLocker permits customization of error messages to direct users to a Web page for help.
Policy maintenance	SRP policies must be updated by using the Local Security Policy snap-in (if the policies are created locally) or the Group Policy Management Console (GPMC).	AppLocker policies can be updated by using the Local Security Policy snap-in (if the policies are created locally), or the GPMC, or the Windows PowerShell AppLocker cmdlets.
Policy application	SRP policies are distributed through Group Policy.	AppLocker policies are distributed through Group Policy.
Enforcement mode	SRP works in the "deny list mode" where administrators can create rules for files that they do not want to allow in this Enterprise whereas the rest of the file are allowed to run by default. SRP can also be configured in the "allow list mode" such that the by default all files are blocked and administrators need to create allow rules for files that they want to allow.	AppLocker by default works in the "allow list mode" where only those files are allowed to run for which there is a matching allow rule.
File types that can be controlled	SRP can control the following file types: - Executables - Dlls - Scripts - Windows Installers SRP cannot control each file type separately. All SRP rules are in a single rule collection.	AppLocker can control the following file types: - Executables - Dlls - Scripts - Windows Installers - Packaged apps and installers (Windows Server 2012 and Windows 8) AppLocker maintains a separate rule collection for each of the five file types.

Application control function	SRP	AppLocker
Designated file types	SRP supports an extensible list of file types that are considered executable. Administrators can add extensions for files that should be considered executable.	AppLocker does not support this. AppLocker currently supports the following file extensions: - Executables (.exe, .com) - Dlls (.ocx, .dll) - Scripts (.vbs, .js, .ps1, .cmd, .bat) - Windows Installers (.msi, .mst, .msp) - Packaged app installers (.appx)
Rule types	SRP supports four types of rules: - Hash - Path - Signature - Internet zone	AppLocker supports three types of rules: - Hash - Path - Publisher
Editing the hash value	SRP allows administrators to provide custom hash values.	AppLocker computes the hash value itself. Internally it uses the SHA1 Authenticode hash for Portable Executables (Exe and Dll) and Windows Installers and a SHA1 flat file hash for the rest.
Support for different security levels	With SRP administrators can specify the permissions with which an app can run. So, an administrator can configure a rule such that notepad always runs with restricted permissions and never with administrative privileges. SRP on Windows Vista and earlier supported multiple security levels. On Windows 7 that list was restricted to just two levels: Disallowed and Unrestricted (Basic User translates to Disallowed).	AppLocker does not support security levels.
Manage Packaged apps and Packaged app installers	Unable	.appx is a valid file type which AppLocker can manage.

Application control function	SRP	AppLocker
Targeting a rule to a user or a group of users	SRP rules apply to all users on a particular computer.	AppLocker rules can be targeted to a specific user or a group of users.
Support for rule exceptions	SRP does not support rule exceptions	AppLocker rules can have exceptions which allow administrators to create rules such as "Allow everything from Windows except for Regedit.exe".
Support for audit mode	SRP does not support audit mode. The only way to test SRP policies is to set up a test environment and run a few experiments.	AppLocker supports audit mode which allows administrators to test the effect of their policy in the real production environment without impacting the user experience. Once you are satisfied with the results, you can start enforcing the policy.
Support for exporting and importing policies	SRP does not support policy import/export.	AppLocker supports the importing and exporting of policies. This allows you to create AppLocker policy on a sample computer, test it out and then export that policy and import it back into the desired GPO.
Rule enforcement	Internally, SRP rules enforcement happens in the user-mode which is less secure.	Internally, AppLocker rules for Exes and Dlls are enforced in the kernel-mode which is more secure than enforcing them in the user-mode.

System requirements

Software restriction policies can only be configured on and applied to computers running at least Windows Server 2003, and at least Windows XP. Group Policy is required to distribute Group Policy Objects that contain software restriction policies.

Software restriction policies components and architecture

Software restriction policies provide a mechanism for the operating system and applications compliant with software restriction policies to restrict the runtime execution of software programs.

At a high level, software restriction policies consist of the following components:

- Software restriction policies API. The Application Programming Interfaces (APIs) are used to create and configure the rules that constitute the software restriction policy. There also are software restriction policies APIs for querying, processing, and enforcing software restriction policies.
- A software restriction policies management tool. This consists of the **Software Restriction Policies** extension of the **Local Group Policy Object Editor** snap-in, which administrators use to create and edit the software restriction policies.
- A set of operating system APIs and applications that call the software restriction policies APIs to provide enforcement of the software restriction policies at runtime.
- Active Directory and Group Policy. Software restriction policies depend on the Group Policy infrastructure to propagate the software restriction policies from the Active Directory to the appropriate clients, and for scoping and filtering the application of these policies to the appropriate target computers.
- Authenticode and WinVerify Trust APIs which are used to process signed executable files.
- Event Viewer. The functions used by software restriction policies log events to the Event Viewer logs.
- Resultant Set of Policies (RSoP), which can aid in the diagnosing of the effective policy that will be applied to a client.

For more information about SRP architecture, how SRP manages rules, processes and interactions, see How Software Restriction Policies Work in the Windows Server 2003 Technical Library.

Best practices

Do not modify the default domain policy.

- If you do not edit the default domain policy, you always have the option of reapplying the default domain policy if something goes wrong with your customized domain policy.

Create a separate Group Policy Object for software restriction policies.

- If you create a separate Group Policy Object (GPO) for software restriction policies, you can disable software restriction policies in an emergency without disabling the rest of your domain policy.

If you experience problems with applied policy settings, restart Windows in Safe Mode.

- Software restriction policies do not apply when Windows is started in Safe Mode. If you accidentally lock down a workstation with software restriction policies, restart the computer in Safe Mode, log on as a local administrator, modify the policy, run **gpupdate**, restart the computer, and then log on normally.

Use caution when defining a default setting of Disallowed.

- When you define a default setting of **Disallowed**, all software is disallowed except for software that has been explicitly allowed. Any file that you want to open has to have a software restriction policies rule that allows it to open.

- To protect administrators from locking themselves out of the system, when the default security level is set to **Disallowed**, four registry path rules are automatically created. You can delete or modify these registry path rules; however, this is not recommended.

For best security, use access control lists in conjunction with software restriction policies.

- Users might try to circumvent software restriction policies by renaming or moving disallowed files or by overwriting unrestricted files. As a result, it is recommended that you use access control lists (ACLs) to deny users the access necessary to perform these tasks.

Test new policy settings thoroughly in test environments before applying the policy settings to your domain.

- New policy settings might act differently than originally expected. Testing diminishes the chance of encountering a problem when you deploy policy settings across your network.

- You can set up a test domain, separate from your organization's domain, in which to test new policy settings. You can also test the policy settings by creating a test GPO and linking it to a test organizational unit. When you have thoroughly tested the policy settings with test users, you can link the test GPO to your domain.
- Do not set programs or files to **Disallowed** without testing to see what the effect may be. Restrictions on certain files can seriously affect the operation of your computer or network.
- Information that is entered incorrectly or typing mistakes can result in a policy setting that does not perform as expected. Testing new policy settings before applying them can prevent unexpected behavior.

Filter user policy settings based on membership in security groups.

- You can specify users or groups for which you do not want a policy setting to apply by clearing the **Apply Group Policy** and **Read** check boxes, which are located on the **Security** tab of the properties dialog box for the GPO.
- When the Read permission is denied, the policy setting is not downloaded by the computer. As a result, less bandwidth is consumed by downloading unnecessary policy settings, which enables the network to function more quickly. To deny the Read permission, select **Deny** for the **Read** check box, which is located on the **Security** tab of the properties dialog box for the GPO.

Do not link to a GPO in another domain or site.

- Linking to a GPO in another domain or site can result in poor performance.

Additional resources

Content type	References
Planning	Software Restriction Policies Technical Reference
Operations	Administer Software Restriction Policies
Troubleshooting	Software Restriction Policies Troubleshooting (2003)

Content type	References
Security	Threats and Countermeasures for Software Restriction Polices (2008) Threats and Countermeasures for Software Restriction Polices (2008 R2)
Tools and settings	Software Restriction Policies Tools and Settings (2003)
Community resources	Application Lockdown with Software Restriction Policies

Administer Software Restriction Policies

Article • 07/29/2021 • 8 minutes to read

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic for the IT professional contains procedures how to administer application control policies using Software Restriction Policies (SRP) beginning with Windows Server 2008 and Windows Vista.

Introduction

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. You use software restriction policies to create a highly restricted configuration for computers, in which you allow only specifically identified applications to run. These are integrated with Microsoft Active Directory Domain Services and Group Policy but can also be configured on stand-alone computers. For more information about SRP, see the Software Restriction Policies.

Beginning with Windows Server 2008 R2 and Windows 7 , Windows AppLocker can be used instead of or in concert with SRP for a portion of your application control strategy.

This topic contains:

- To open Software Restriction Policies
- To create new software restriction policies
- To add or delete a designated file type
- To prevent software restriction policies from applying to local administrators
- To change the default security level of software restriction policies
- To apply software restriction policies to DLLs

For information about how to accomplish specific tasks using SRP, see the following:

- Determine Allow-Deny List and Application Inventory for Software Restriction Policies
- Work with Software Restriction Policies Rules

- Use Software Restriction Policies to Help Protect Your Computer Against an Email Virus

To open Software Restriction Policies

- For your local computer
- For a domain, site, or organizational unit, and you are on a member server or on a workstation that is joined to a domain
- For a domain or organizational unit, and you are on a domain controller or on a workstation that has the Remote Server Administration Tools installed
- For a site, and you are on a domain controller or on a workstation that has the Remote Server Administration Tools installed

For your local computer

1. Open Local Security Settings.
2. In the console tree, click **Software Restriction Policies**.

   Where?

   - Security Settings/Software Restriction Policies

> ⓘ **Note**
>
> To perform this procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority.

For a domain, site, or organizational unit, and you are on a member server or on a workstation that is joined to a domain

1. Open Microsoft Management Console (MMC).
2. On the **File** menu, click **Add/Remove Snap-in**, and then click **Add**.
3. Click **Local Group Policy Object Editor**, and then click **Add**.
4. In **Select Group Policy Object**, click **Browse**.

5. In **Browse for a Group Policy Object**, select a Group Policy Object (GPO) in the appropriate domain, site, or organizational unit-or create a new one, and then click **Finish**.

6. Click **Close**, and then click **OK**.

7. In the console tree, click **Software Restriction Policies**.

   Where?

   - *Group Policy Object* [*ComputerName*] Policy/Computer Configuration or

     User Configuration/Windows Settings/Security Settings/Software Restriction Policies

ⓘ **Note**

To perform this procedure, you must be a member of the Domain Admins group.

For a domain or organizational unit, and you are on a domain controller or on a workstation that has the Remote Server Administration Tools installed

1. Open Group Policy Management Console.

2. In the console tree, right-click the Group Policy Object (GPO) that you want to open software restriction policies for.

3. Click **Edit** to open the GPO that you want to edit. You can also click **New** to create a new GPO, and then click **Edit**.

4. In the console tree, click **Software Restriction Policies**.

   Where?

   - *Group Policy Object* [*ComputerName*] Policy/Computer Configuration or

     User Configuration/Windows Settings/Security Settings/Software Restriction Policies

ⓘ **Note**

To perform this procedure, you must be a member of the Domain Admins group.

For a site, and you are on a domain controller or on a workstation that has the Remote Server Administration Tools installed

1. Open Group Policy Management Console.
2. In the console tree, right-click the site that you want to set Group Policy for.

   Where?

   - Active Directory Sites and Services [*Domain_Controller_Name.Domain_Name*]/Sites/Site

3. Click an entry in **Group Policy Object Links** to select an existing Group Policy Object (GPO), and then click **Edit**. You can also click **New** to create a new GPO, and then click **Edit**.
4. In the console tree, click **Software Restriction Policies**.

   Where

   - *Group Policy Object* [*ComputerName*] Policy/Computer Configuration or

     User Configuration/Windows Settings/Security Settings/Software Restriction Policies

> ⓘ **Note**
>
> - To perform this procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.
> - To set policy settings that will be applied to computers, regardless of which users log on to them, click **Computer Configuration**.
> - To set policy settings that will be applied to users, regardless of which computer they log on to, click **User Configuration**.

To create new software restriction policies

1. Open Software Restriction Policies.
2. On the **Action** menu, click **New Software Restriction Policies**.

⚠ Warning

- Different administrative credentials are required to perform this procedure, depending on your environment:
  - If you create new software restriction policies for your local computer: Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure.
  - If you create new software restriction policies for a computer that is joined to a domain, members of the Domain Admins group can perform this procedure.
- If software restriction policies have already been created for a Group Policy Object (GPO), the **New Software Restriction Policies** command does not appear on the **Action** menu. To delete the software restriction policies that are applied to a GPO, in the console tree, right-click **Software Restriction Policies**, and then click **Delete Software Restriction Policies**. When you delete software restriction policies for a GPO, you also delete all software restriction policies rules for that GPO. After you delete software restriction policies, you can create new software restriction policies for that GPO.

To add or delete a designated file type

1. Open Software Restriction Policies.
2. In the details pane, double-click **Designated File Types**.
3. Do one of the following:
   - To add a file type, in **File name extension**, type the file name extension, and then click **Add**.
   - To delete a file type, in **Designated file types**, click the file type, and then click **Remove**.

ⓘ Note

- Different administrative credentials are required to perform this procedure, depending on the environment in which you add or delete a designated file type:

  - If you add or delete a designated file type for your local computer: Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure.
  - If you create new software restriction policies for a computer that is joined to a domain, members of the Domain Admins group can perform this procedure.

- It may be necessary to create a new software restriction policy setting for the Group Policy Object (GPO) if you have not already done so.

- The list of designated file types is shared by all rules for both Computer Configuration and User Configuration for a GPO.

To prevent software restriction policies from applying to local administrators

1. Open Software Restriction Policies.

2. In the details pane, double-click **Enforcement**.

3. Under **Apply software restriction policies to the following users**, click **All users except local administrators**.

⚠ Warning

- Membership in the local **Administrators** group, or equivalent, is the minimum required to complete this procedure.
- It may be necessary to create a new software restriction policy setting for the Group Policy Object (GPO) if you have not already done so.
- If it is common for users to be members of the local Administrators group on their computers in your organization, you may not want to enable this option.
- If you are defining a software restriction policy setting for your local computer, use this procedure to prevent local administrators from having software restriction policies applied to them. If you are defining a software restriction policy setting for your network, filter user policy settings based on membership in security groups through Group Policy.

To change the default security level of software restriction policies

1. Open Software Restriction Policies.

2. In the details pane, double-click **Security Levels**.

3. Right-click the security level that you want to set as the default, and then click **Set as default**.

> ⊗ **Caution**
>
> In certain directories, setting the default security level to **Disallowed** can adversely affect your operating system.

> ⓘ **Note**
>
> - Different administrative credentials are required to perform this procedure, depending on the environment for which you change the default security level of software restriction policies.
> - It may be necessary to create a new software restriction policy setting for this Group Policy Object (GPO) if you have not already done so.
> - In the details pane, the current default security level is indicated by a black circle with a check mark in it. If you right-click the current default security level, the **Set as default** command does not appear in the menu.
> - Software restriction policies rules are created to specify exceptions to the default security level. When the default security level is set to **Unrestricted**, rules can specify software that is not allowed to run. When the default security level is set to **Disallowed**, rules can specify software that is allowed to run.
> - At installation, the default security level of software restriction policies on all files on your system is set to **Unrestricted**.

To apply software restriction policies to DLLs

1. Open Software Restriction Policies.

2. In the details pane, double-click **Enforcement**.

3. Under **Apply software restriction policies to the following**, click **All software files**.

ⓘ **Note**

- To perform this procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.
- By default, software restriction policies do not check dynamic-link libraries (DLLs). Checking DLLs can decrease system performance, because software restriction policies must be evaluated every time a DLL is loaded. However, you may decide to check DLLs if you are concerned about receiving a virus that targets DLLs. If the default security level is set to **Disallowed**, and you enable DLL checking, you must create software restriction policies rules that allow each DLL to run.

Determine Allow-Deny List and Application Inventory for Software Restriction Policies

Article • 07/29/2021 • 3 minutes to read

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic for the IT professional gives guidance how to create an allow and deny list for applications to be managed by Software Restriction Policies (SRP) beginning with Windows Server 2008 and Windows Vista.

Introduction

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. You use software restriction policies to create a highly restricted configuration for computers, in which you allow only specifically identified applications to run. These are integrated with Microsoft Active Directory Domain Services and Group Policy but can also be configured on stand-alone computers. For a starting point for SRP, see the Software Restriction Policies.

Beginning with Windows Server 2008 R2 and Windows 7 , Windows AppLocker can be used instead of or in concert with SRP for a portion of your application control strategy.

For information about how to accomplish specific tasks using SRP, see the following:

- Work with Software Restriction Policies Rules
- Use Software Restriction Policies to Help Protect Your Computer Against an Email Virus

What default rule to choose: Allow or Deny

Software restriction policies can be deployed in one of two modes that are the basis of your default rule: Allow List or Deny List. You can create a policy that identifies every application that is allowed to run in your environment; the default rule within your policy is Restricted and will block all applications that you do not explicitly allow to run.

Or you can create a policy that identifies every application that cannot run; the default rule is Unrestricted and restricts only the applications that you have explicitly listed.

> ⓘ **Important**
>
> The Deny List mode might be a high-maintenance strategy for your organization regarding application control. Creating and maintaining an evolving list that prohibits all malware and other problematic applications would be time consuming and susceptible to mistakes.

Create an inventory of your applications for the Allow list

To effectively use the Allow default rule, you need to determine exactly which applications are required in your organization. There are tools designed to produce an application inventory, such as the Inventory Collector in the Microsoft Application Compatibility Toolkit. But SRP has an advanced logging feature to help you understand exactly what applications are running in your environment.

To discover which applications to allow

1. In a test environment, deploy Software Restriction Policy with the default rule set to Unrestricted and remove any additional rules. If you enable SRP without forcing it to restrict any applications, SPR will be able to monitor what applications are being run.

2. Create the following registry value in order to enable the advanced logging feature and set the path to where the log file should be written.

   "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers"

   String Value: *LogFileName path to LogFileName*

   Because SRP is evaluating all applications when they run, an entry is written to the log file *NameLogFile* each time that application is run.

3. Evaluate the log file

   Each log entry states:

   - the caller of the software restriction policy and the process ID (PID) of the calling process

- the target being evaluated
- the SRP rule that was encountered when that application ran
- an identifier for the SRP rule.

An example of the output written to a log file:

explorer.exe (PID = 4728) identifiedC:\Windows\system32\onenote.exe as Unrestricted usingpath rule, Guid ={320bd852-aa7c-4674-82c5-9a80321670a3} All applications and associated code that SRP checks and set to block will be noted in the log file, which you then can use to determine which executables should be considered for your Allowed list.

Work with Software Restriction Policies Rules

Article • 07/29/2021 • 13 minutes to read

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic describes procedures working with certificate, path, internet zone and hash rules using Software Restriction Policies.

Introduction

With software restriction policies, you can protect your computing environment from untrusted software by identifying and specifying what software is allowed to run. You can define a default security level of **Unrestricted** or **Disallowed** for a Group Policy Object (GPO) so that software is either allowed or not allowed to run by default. You can make exceptions to this default security level by creating software restriction policies rules for specific software. For example, if the default security level is set to **Disallowed**, you can create rules that allow specific software to run. The types of rules are as follows:

- **Certificate rules**

  For procedures, see Working with certificate rules.

- **Hash rules**

  For procedures, see Working with hash rules.

- **Internet zone rules**

  For procedures, see Working with Internet Zone rules.

- **Path rules**

  For procedures, see Working with path rules.

For information about other tasks to manage Software Restriction Policies, see Administer Software Restriction Policies.

Working with certificate rules

Software restriction policies can also identify software by its signing certificate. You can create a certificate rule that identifies software and then allows or does not allow the software to run, depending on the security level. For example, you can use certificate rules to automatically trust software from a trusted source in a domain without prompting the user. You can also use certificate rules to run files in disallowed areas of your operating system. Certificate rules are not enabled by default.

When rules are created for the domain using Group Policy, you must have permissions to create or modify a Group Policy Object. If you are creating rules for the local computer, you must have administrative credentials on that computer.

To create a certificate rule

1. Open Software Restriction Policies.
2. In either the console tree or the details pane, right-click **Additional Rules**, and then click **New Certificate Rule**.
3. Click **Browse**, and then select a certificate or signed file.
4. In **Security level**, click either **Disallowed** or **Unrestricted**.
5. In **Description**, type a description for this rule, and then click **OK**.

> ⓘ **Note**
>
> - It might be necessary to create a new software restriction policy setting for the Group Policy Object (GPO) if you have not already done so.
> - Certificate rules are not enabled by default.
> - The only file types that are affected by certificate rules are those that are listed in **Designated file types** in the details pane for Software Restriction Policies. There is one list of designated file types that is shared by all rules.
> - For software restriction policies to take effect, users must update policy settings by logging off from and logging on to their computers.
> - When more than one software restriction policies rule is applied to policy settings, there is a precedence of rules for handling conflicts.

Enabling certificate rules

There are different procedures for enabling certificate rules depending on your environment:

- For your local computer
- For a Group Policy Object, and you are on a server that is joined to a domain
- For a Group Policy Object, and you are on a domain controller or a on workstation that has the Remote Server Administration Tools installed
- For only domain controllers, and you are on a domain controller or on a workstation that has the Remote Server Administration Tools Pack installed

To enable certificate rules for your local computer

1. Open Local Security Settings.
2. In the console tree, click **Security Options** located under Security Settings/Local Policies.
3. In the details pane, double-click **System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies**.
4. Do one of the following, and then click **OK**:
   - To enable certificate rules, click **Enabled**.
   - To disable certificate rules, click **Disabled**.

To enable certificate rules For a Group Policy Object, and you are on a server that is joined to a domain

1. Open Microsoft Management Console (MMC).
2. On the **File** menu, click **Add/Remove snap-in**, and then click **Add**.
3. Click **Local Group Policy Object Editor**, and then click **Add**.
4. In **Select Group Policy Object**, click **Browse**.
5. In **Browse for a Group Policy Object**, select a Group Policy Object (GPO) in the appropriate domain, site, or organizational unit-or create a new one, and then click **Finish**.
6. Click **Close**, and then click **OK**.

7. In the console tree, click **Security Options** located under *GroupPolicyObject* [*ComputerName*] Policy/Computer Configuration/Windows Settings/Security Settings/Local Policies/.

8. In the details pane, double-click **System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies**.

9. If this policy setting has not yet been defined, select the **Define these policy settings** check box.

10. Do one of the following, and then click **OK**:

    - To enable certificate rules, click **Enabled**.

    - To disable certificate rules, click **Disabled**.

To enable certificate rules for a Group Policy Object, and you are on a domain controller or on a workstation that has the Remote Server Administration Tools installed

1. Open Active Directory Users and Computers.

2. In the console tree, right-click the Group Policy Object (GPO) for which you want to enable certificate rules.

3. Click **Properties**, and then click the **Group Policy** tab.

4. Click **Edit** to open the GPO that you want to edit. You can also click **New** to create a new GPO, and then click **Edit**.

5. In the console tree, click **Security Options** located under *GroupPolicyObject*[*ComputerName*] Policy/Computer Configuration/Windows Settings/Security Settings/Local Policies.

6. In the details pane, double-click **System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies**.

7. If this policy setting has not yet been defined, select the **Define these policy settings** check box.

8. Do one of the following, and then click **OK**:

    - To enable certificate rules, click **Enabled**.

    - To disable certificate rules, click **Disabled**.

To enable certificate rules for only domain controllers, and you are on a domain controller or on a workstation that has the Remote Server Administration Tools installed

1. Open Domain Controller Security Settings.

2. In the console tree, click **Security Options** located under *GroupPolicyObject* [*ComputerName*] Policy/Computer Configuration/Windows Settings/Security Settings/Local Policies.

3. In the details pane, double-click **System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies**.

4. If this policy setting has not yet been defined, select the **Define these policy settings** check box.

5. Do one of the following, and then click **OK**:

   - To enable certificate rules, click **Enabled**.

   - To disable certificate rules, click **Disabled**.

> ⓘ **Note**
>
> You must perform this procedure before certificate rules can take effect.

Set trusted publisher options

Software signing is being used by a growing number of software publishers and application developers to verify that their applications come from a trusted source. However, many users do not understand or pay little attention to the signing certificates associated with applications that they install.

The policy settings in the **Trusted Publishers** tab of the certificate path validation policy allows administrators to control which certificates can be accepted as coming from a trusted publisher.

To configure the trusted publishers policy settings for a local computer

1. On the **Start** screen, type**gpedit.msc** and then press ENTER.

2. In the console tree under **Local Computer Policy\Computer Configuration\Windows Settings\Security Settings**, click **Public Key Policies**.

3. Double-click **Certificate Path Validation Settings**, and then click the **Trusted Publishers** tab.

4. Select the **Define these policy settings** check box, select the policy settings that you want to apply, and then click **OK** to apply the new settings.

To configure the trusted publishers policy settings for a domain

1. Open **Group Policy Management**.

2. In the console tree, double-click **Group Policy Objects** in the forest and domain containing the **Default Domain Policy** Group Policy Object (GPO) that you want to edit.

3. Right-click the **Default Domain Policy** GPO, and then click **Edit**.

4. In the console tree under **Computer Configuration\Windows Settings\Security Settings**, click **Public Key Policies**.

5. Double-click **Certificate Path Validation Settings**, and then click the **Trusted Publishers** tab.

6. Select the **Define these policy settings** check box, select the policy settings that you want to apply, and then click **OK** to apply the new settings.

To allow only administrators to manage certificates used for code signing for a local computer

1. On the **Start** screen, type, **gpedit.msc** in the **Search programs and files** or in Windows 8, on the Desktop, and then press ENTER.

2. In the console tree under **Default Domain Policy** or **Local Computer Policy**, double-click **Computer Configuration**, **Windows Settings**, and **Security Settings**, and then click **Public Key Policies**.

3. Double-click **Certificate Path Validation Settings**, and then click the **Trusted Publishers** tab.

4. Select the **Define these policy settings** check box.

5. Under **Trusted publisher management**, click **Allow only all administrators to manage Trusted Publishers**, and then click **OK** to apply the new settings.

To allow only administrators to manage certificates used for code signing for a domain

1. Open **Group Policy Management**.
2. In the console tree, double-click **Group Policy Objects** in the forest and domain containing the **Default Domain Policy** GPO that you want to edit.
3. Right-click the **Default Domain Policy** GPO, and then click **Edit**.
4. In the console tree under **Computer Configuration\Windows Settings\Security Settings**, click **Public Key Policies**.
5. Double-click **Certificate Path Validation Settings**, and then click the **Trusted Publishers** tab.
6. Select the **Define these policy settings** check box, implement the changes you want, and then click **OK** to apply the new settings.

Working with hash rules

A hash is a series of bytes with a fixed length that uniquely identifies a software program or file. The hash is computed by a hash algorithm. When a hash rule is created for a software program, software restriction policies calculate a hash of the program. When a user tries to open a software program, a hash of the program is compared to existing hash rules for software restriction policies. The hash of a software program is always the same, regardless of where the program is located on the computer. However, if a software program is altered in any way, its hash also changes, and it no longer matches the hash in the hash rule for software restriction policies.

For example, you can create a hash rule and set the security level to **Disallowed** to prevent users from running a certain file. A file can be renamed or moved to another folder and still result in the same hash. However, any changes to the file itself also change its hash value and allow the file to bypass restrictions.

To create a hash rule

1. Open Software Restriction Policies.
2. In either the console tree or the details pane, right-click **Additional Rules**, and then click **New Hash Rule**.
3. Click **Browse** to find a file.

> ⓘ Note
>
> In Windows XP it is possible to paste a pre-calculated hash in **File hash**. In Windows Server 2008 R2 , Windows 7 and later versions, this option is not available.

4. In **Security level**, click either **Disallowed** or **Unrestricted**.

5. In **Description**, type a description for this rule, and then click **OK**.

> ⓘ Note
>
> - It may be necessary to create a new software restriction policy setting for the Group Policy Object (GPO) if you have not already done so.
> - A hash rule can be created for a virus or a Trojan horse to prevent them from running.
> - If you want other people to use a hash rule so that a virus cannot run, calculate the hash of the virus by using software restriction policies, and then e-mail the hash value to the other people. Never e-mail the virus itself.
> - If a virus has been sent through e-mail, you can also create a path rule to prevent execution of e-mail attachments.
> - A file that is renamed or moved to another folder results in the same hash. Any change to the file itself results in a different hash.
> - The only file types that are affected by hash rules are those that are listed in **Designated File Types** in the details pane for Software Restriction Policies. There is one list of designated file types that is shared by all rules.
> - For software restriction policies to take effect, users must update policy settings by logging off from and logging on to their computers.
> - When more than one software restriction policies rule is applied to policy settings, there is a precedence of rules for handling conflicts.

Working with Internet Zone rules

Internet zone rules apply only to Windows Installer packages. A zone rule can identify software from a zone that is specified through Internet Explorer. These zones are Internet, Local intranet, Restricted sites, Trusted sites, and My Computer. An Internet Zone rule is designed to prevent users from downloading and installing software.

To create an Internet zone rule

1. Open Software Restriction Policies.

2. In either the console tree or the details pane, right-click **Additional Rules**, and then click **New Internet Zone Rule**.

3. In **Internet zone**, click an Internet zone.

4. In **Security level**, click either **Disallowed** or **Unrestricted**, and then click **OK**.

> ⓘ **Note**
>
> - It may be necessary to create a new software restriction policy setting for the Group Policy Object (GPO) if you have not already done so.
> - Zone rules only apply to files with an .msi file type, which are Windows Installer packages.
> - For software restriction policies to take effect, users must update policy settings by logging off from and logging on to their computers.
> - When more than one software restriction policies rule is applied to policy settings, there is a precedence of rules for handling conflicts.

Working with path rules

A path rule identifies software by its file path. For example, if you have a computer that has a default security level of **Disallowed**, you can still grant unrestricted access to a specific folder for each user. You can create a path rule by using the file path and setting the security level of the path rule to **Unrestricted**. Some common paths for this type of rule are %userprofile%, %windir%, %appdata%, %programfiles%, and %temp%. You can also create registry path rules that use the registry key of the software as its path.

Because these rules are specified by the path, if a software program is moved, the path rule no longer applies.

To create a path rule

1. Open Software Restriction Policies.

2. In either the console tree or the details pane, right-click **Additional Rules**, and then click **New Path Rule**.

3. In **Path**, type a path, or click **Browse** to find a file or folder.

4. In **Security level**, click either **Disallowed** or **Unrestricted**.

5. In **Description**, type a description for this rule, and then click **OK**.

⊗ Caution

- On certain folders, such as the Windows folder, setting the security level to **Disallowed** can adversely affect the operation of your operating system. Make sure that you do not disallow a crucial component of the operating system or one of its dependent programs.

ⓘ Note

- It may be necessary to create new software restriction policies for the Group Policy Object (GPO) if you have not already done so.
- If you create a path rule for software with a security level of **Disallowed**, users can still run the software by copying it to another location.
- The wildcard characters that are supported by the path rule are * and ?.
- You can use environment variables, such as %programfiles% or %systemroot%, in the path rule.
- If you want to create a path rule for software when you do not know where it is stored on a computer but you have its registry key, you can create a registry path rule.
- To prevent users from executing e-mail attachments, you can create a path rule for your e-mail program's attachment directory that prevents users from running e-mail attachments.
- The only file types that are affected by path rules are those that are listed in **Designated File Types** in the details pane for Software Restriction Policies. There is one list of designated file types that is shared by all rules.
- For software restriction policies to take effect, users must update policy settings by logging off from and logging on to their computers.
- When more than one software restriction policies rule is applied to policy settings, there is a precedence of rules for handling conflicts.

To create a registry path rule

1. On the **Start** screen, type regedit.

2. In the console tree, right-click the registry key that you want to create a rule for, and then click **Copy Key Name**. Note the value name in the details pane.

3. Open Software Restriction Policies.

4. In either the console tree or the details pane, right-click **Additional Rules**, and then click **New Path Rule**.

5. In **Path**, paste the registry key name, followed by the value name.

6. Enclose the registry path in percent signs (%), for example, %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PlatformSDK\Directories\InstallDir%.

7. In **Security level**, click either **Disallowed** or **Unrestricted**.

8. In **Description**, type a description for this rule, and then click **OK**.

Use Software Restriction Policies to Help Protect Your Computer Against an Email Virus

Article • 07/29/2021 • 2 minutes to read

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic provides information how to set application control polices using Software Restriction Policies (SRP) to help protect your computer against e-mail virus beginning with Windows Server 2008 and Windows Vista.

Introduction

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. You use software restriction policies to create a highly restricted configuration for computers, in which you allow only specifically identified applications to run. These are integrated with Microsoft Active Directory Domain Services and Group Policy but can also be configured on stand-alone computers. For a starting point for SRP, see the Software Restriction Policies.

Beginning with Windows Server 2008 R2 and Windows 7 , Windows AppLocker can be used instead of or in concert with SRP for a portion of your application control strategy.

Configure SRP to help protect against an e-mail virus

1. Review the best practices for software restriction policies to understand how SRP works.

    - Best practices

    - How Software Restriction Policies Work

2. Open Software Restriction Policies.

    - For your local computer

    - For a domain, site, or organizational unit, and you are on a member server or on a workstation that is joined to a domain

3. If you have not previously defined software restriction policies, create new software restriction policies.

   - To create new software restriction policies

4. Create a path rule for the folder that your e-mail program uses to run e-mail attachments, and then set the security level to **Disallowed**.

   - Working with path rules

5. Specify the file types to which the rule applies.

   - To add or delete a designated file type

6. Modify policy settings so that they apply to the users and groups that you want:

   - Specify users or groups to which you do not want the Group Policy Object's (GPO) policy settings to apply.

   - Exclude local administrators from the software restriction policies of a specific policy setting in Group Policy and still have the rest of Group Policy apply to the administrators.
     - To prevent software restriction policies from applying to local administrators

7. Test the policy.

Troubleshoot Software Restriction Policies

Article • 07/29/2021 • 4 minutes to read

> Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012

This topic describes common problems and their solutions when troubleshooting Software Restriction Policies (SRP) beginning with Windows Server 2008 and Windows Vista.

Introduction

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. You use software restriction policies to create a highly restricted configuration for computers, in which you allow only specifically identified applications to run. These are integrated with Microsoft Active Directory Domain Services and Group Policy but can also be configured on stand-alone computers. For more information about SRP, see the Software Restriction Policies.

Beginning with Windows Server 2008 R2 and Windows 7 , Windows AppLocker can be used instead of or in concert with SRP for a portion of your application control strategy.

Windows cannot open a program

Users receive a message that says "Windows cannot open this program because it has been prevented by a software restriction policy. For more information, open Event Viewer or contact your system administrator." Or, on the command line, a message says "The system cannot execute the specified program."

Cause: The default security level (or a rule) was created so that the software program is set as **Disallowed**, and as a result it will not start.

Solution: Look in the event log for an in-depth description of the message. The event log message indicates what software program is set as **Disallowed** and what rule is applied to the program.

Modified software restriction policies are not taking effect

Cause: Software restriction policies that are specified in a domain through Group Policy override any policy settings that are configured locally. This might imply that there is a policy setting from the domain that is overriding your policy setting.

Cause: Group Policy might not have refreshed its policy settings. Group Policy applies changes to policy settings periodically; therefore, it is likely that the policy changes that were made in the directory have not yet been refreshed.

Solutions:

1. The computer on which you modify software restriction policies for the network must be able to contact a domain controller. Ensure the computer can contact a domain controller.

2. Refresh policy by logging off of the network and then logging on to the network again. If any policy is applied through Group Policy, logging back in will refresh those policies.

3. You can refresh policy settings with the command-line utility gpupdate or by logging off from and then logging back on to your computer. For best results, run gpupdate, and then log off from and log back on to your computer. Generally, the security settings are refreshed every 90 minutes on a workstation or server and every 5 minutes on a domain controller. The settings are also refreshed every 16 hours, whether or not there are any changes. These are configurable settings so refresh intervals might be different in each domain.

4. Check which policies apply. Check domain level policies for **No Override** settings.

5. Software restriction policies that are specified in a domain through Group Policy override any policies that are configured locally. Use Gpresult command-line tool to determine what the net effect of the policy is. This might imply that there is a policy from the domain that is overriding your local setting.

6. If SRP and AppLocker policy settings are in the same GPO, AppLocker settings will take precedence on Windows 7 , Windows Server 2008 R2 , and later. It is recommended to put SRP and AppLocker policy settings in different GPOs.

After adding a rule through SRP, you cannot log on to your computer

Cause: Your computer accesses many programs and files when it starts. You might have inadvertently set one of these programs or files to **Disallowed**. Because the computer cannot access the program or file, it cannot start properly.

Solution: Start the computer in Safe Mode, log on as a local administrator, and then change software restriction policies to allow the program or file to run.

A new policy setting is not applying to a specific file name extension

Cause: The filename extension is not in the list of supported file types.

Solution: Add the filename extension to the list of file types supported by SRP.

Software restriction policies address the problem of regulating unknown or untrusted code. Software restriction policies are security settings to identify software and control its ability to run on a local computer, in a site, domain, or OU and can be implemented through a GPO.

A default rule is not restricting as expected

Cause: Rules which are applied in a particular order which can cause default rules to be overridden by specific rules. SRP applies rules in the following order (most specific to general):

1. Hash rules
2. Certificate rules
3. Path rules
4. Internet Zone rules
5. Default rules

Solution: Evaluate the rules restricting the application and, if appropriate, remove all but the Default rule.

Unable to discover which restrictions are applied

Cause: There is no apparent cause for the unexpected behavior, and GPO refresh has not solved the issue so further investigation is necessary.

Solutions:

1. Investigate the System Event Log, filtering on source of "Software Restriction Policy." The entries explicitly state which rule is implemented for each application.

2. Enable advanced logging. See Determine Allow-Deny List and Application Inventory for Software Restriction Policies for more information.