Using Software Restriction Policies and AppLocker Policies

By Archiveddocs

Archived: 2026-04-06 02:10:19 UTC

Applies To: Windows 7, Windows 8.1, Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2012, Windows 8

This topic for the IT professional describes how to use Software Restriction Policies (SRP) and AppLocker policies in the same Windows deployment.

You might want to deploy application control policies in Windows operating systems earlier than Windows Server 2008 R2 or Windows 7. You can use AppLocker policies only on the supported versions and editions of Windows as listed in Requirements to Use AppLocker. However, you can use SRP on those supported editions of Windows plus Windows Server 2003 and Windows XP. To compare features and functions in SRP and AppLocker so that you can determine when to use each technology to meet your application control objectives, see Determine Your Application Control Objectives.

SRP and AppLocker use Group Policy for domain management. However, when policies are generated by SRP and AppLocker exist in the same domain, and they are applied through Group Policy, AppLocker policies take precedence over policies generated by SRP on computers that are running an operating system that supports AppLocker. For information about how inheritance in Group Policy applies to AppLocker policies and policies generated by SRP, see Understand AppLocker Rules and Enforcement Setting Inheritance in Group Policy.

Important

As a best practice, use separate Group Policy Objects to implement your SRP and AppLocker policies. To reduce troubleshooting issues, do not combine them in the same GPO.

The following scenario provides an example of how each type of policy would affect a bank teller software application, where the application is deployed on different Windows desktop operating systems and managed by the Tellers GPO.

Operating system	Tellers GPO with AppLocker policy	Tellers GPO with SRP	Tellers GPO with AppLocker policy and SRP
Windows 8.1, Windows 8,and Windows 7	AppLocker policies in the GPO are applied, and they supersede any local AppLocker policies.	Local AppLocker policies supersede policies generated by SRP that are applied through the GPO.	AppLocker policies in the GPO are applied, and they supersede the policies generated by SRP in the GPO and local AppLocker policies or policies generated by SRP.
Windows Vista	AppLocker policies are not applied.	Policies generated by SRP in the GPO are applied, and they supersede local policies generated by SRP.AppLocker policies are not applied.	Policies generated by SRP in the GPO are applied, and they supersede local policies generated by SRP. AppLocker policies not applied.
Windows XP	AppLocker policies are not applied.	Policies generated by SRP in the GPO are applied, and they supersede local policies generated by SRP. AppLocker policies are not applied.	Policies generated by SRP in the GPO are applied, and they supersede local policies generated by SRP. AppLocker policies not applied.

Because SRPs and AppLocker policies function differently, they should not be implemented in the same GPO. This makes testing the result of the policy straightforward, which is critical to successfully controlling application usage in the organization. Configuring a testing and policy distribution system can help you understand the result of a policy. The effects of policies generated by SRP and AppLocker policies need to be tested separately and by using different tools.

You can use the Group Policy Management Console (GPMC) or the Resultant Set of Policy (RSoP) snap-in to determine the effect of applying SRPs by using GPOs. For information about using the GPMC, see Group Policy Management Overview [w8]. For information about using RSoP, see Resultant Set of Policy Overview [w8].

You can test AppLocker policies by using Windows PowerShell cmdlets. For information about investigating the result of a policy, see:

- Test an AppLocker Policy by Using Test-AppLockerPolicy

- Monitor Application Usage with AppLocker

Another method to use when determining the result of a policy is to set the enforcement mode to **Audit only**. When the policy is deployed, events will be written to the AppLocker logs as if the policy was enforced. For information about using the **Audit only** mode, see:

- Understand AppLocker Enforcement Settings
- Configure an AppLocker Policy for Audit Only

AppLocker Policies Deployment Guide
