BETA CONTENT: AppLocker Frequently Asked Questions

Microsoft Corporation

Status: Preliminary documentation

Beta content: This guide is currently in beta form. The AppLocker team greatly appreciates you reviewing the document and looks forward to receiving your feedback. To report bugs or ask questions about any of the content in this guide, please send e-mail to the AppLocker Feedback alias applock@microsoft.com.

Abstract: This article details questions that IT professionals have frequently asked about AppLocker in Windows 7 and Windows Server 2008 R2.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

AppLocker Frequently Asked Questions

Contents

Understanding AppLocker 4

What is AppLocker? 4

How does AppLocker differ from Software Restriction Policies (SRP)? 4

What kinds of files can I manage with AppLocker? 5

Where can I find more information about AppLocker? 5

Planning and Deploying AppLocker 5

Which editions of Windows 7 and Windows Server 2008 R2 support AppLocker rules? 5

Which editions of Windows can I use to create AppLocker rules? 5

Can SRP rules be migrated to AppLocker rules? 6

What are rule conditions? 6

Can I configure the default AppLocker rule action? 6

Why can't I change the default rule action? 6

Can I test my AppLocker rules before I enforce them? 6

Can AppLocker rules be applied to specific users or groups? 7

Do I need to upgrade my domain controllers to use AppLocker rules? 7

Does AppLocker use any services for its rule enforcement? 7

How do I create DLL rules? 7

Why is the DLL rule collection disabled by default? 7

Managing AppLocker 7

Why aren't my AppLocker rules being enforced? 7

How can I view the AppLocker events on client computers? 8

What should I do if my rules are too restrictive and Windows is behaving irregularly or will not boot? 8

Understanding AppLocker

What is AppLocker?

AppLocker™ is a new feature in Windows 7 and Windows Server 2008 R2 that replaces the Software Restriction Policies feature. AppLocker contains new capabilities and extensions that reduce administrative overhead and help administrators control how users can access and use files, such as executable files, scripts, Windows Installer files, and DLLs. Using AppLocker, you can:

- Define rules based on file attributes derived from the digital signature, including the publisher, product name, file name, and file version. For example, you can create rules based on the publisher attribute that is persistent through updates, or you can create rules for a specific version of a file.
- Assign a rule to a security group or an individual user.
- Create exceptions to rules. For example, you can create a rule that allows all Windows processes to run except Registry Editor (Regedit.exe).
- Use audit-only mode to deploy the policy and understand its impact before enforcing it.
- Import and export rules. The import and export affects the entire policy. For example, if you export a policy, all of the rules from all of the rule collections are exported, including the enforcement settings for the rule collections. If you import a policy, the existing policy is overwritten.
- Simplify creating and managing AppLocker rules by using AppLocker PowerShell cmdlets.

How does AppLocker differ from Software Restriction Policies?

Software Restriction Policies (SRP) were originally designed in Windows XP and Windows Server 2003 to help IT professionals limit the number of applications that would require administrator access. With the introduction of User Account Control (UAC) and the emphasis of standard user accounts in Windows Vista, fewer applications today require administrator privileges. As a result, AppLocker was introduced to expand the goals of the original SRP by allowing IT administrators to create a comprehensive list of applications that should be allowed to run.

The following table compares AppLocker to Software Restriction Policies.

Feature	Software Restriction Policies	AppLocker
Rule scope	Specific user or group (per GPO)	Specific user or group (per rule)
Rule conditions provided	File hash, path, certificate, registry path, and Internet zone rules	File hash, path, and publisher rules

Rule types provided	Allow and deny	Allow and deny
Default rule action	Allow or deny	Deny
Audit-only mode	No	Yes
Wizard to create multiple rules at one time	No	Yes
Policy import or export	No	Yes
Rule collection	No	Yes
PowerShell support	No	Yes
Custom error messages	No	Yes

What kinds of files can I manage with AppLocker?

AppLocker can be used to manage four different types of files: **executable** (.exe), **Windows Installer** (.msi and .msp), **script** (.bat, .cmd, .js, .ps1, and .vbs), and **DLL** (.dll and .ocx). Each of these file types is managed in its own rule collection.

Where can I find more information about AppLocker?

- AppLocker page on the Windows Server TechCenter (http://technet.microsoft.com/en-us/library/dd723678(WS.10).aspx)
- AppLocker Silverlight demo (http://technet.microsoft.com/en-us/windows/dd320283.aspx)
- AppLocker documentation on the Microsoft Download Center (http://www.microsoft.com/downloads/details.aspx?FamilyID=025cf2e8-b0ab-4419-b5bb-86ab2d5eca83&displaylang=en)

Planning and Deploying AppLocker

Which editions of Windows 7 and Windows Server 2008 R2 support AppLocker rules?

AppLocker rules can be enforced on Windows 7 Ultimate edition, Windows 7 Enterprise edition, and all editions of Windows Server 2008 R2 except Windows Web Server and Windows Server Foundation.

Which editions of Windows can I use to create AppLocker rules?

To create rules for a local computer, the computer must be running Windows 7 Ultimate edition or Windows 7 Enterprise edition. If you want to create rules for a GPO, you can use a computer that is running any edition of Windows 7, provided that the Remote Server Administration Toolkit is installed. AppLocker rules can be created on any edition of Windows

Server 2008 R2. While you can create AppLocker rules on Windows Professional computers, they will not be enforced on those computers. However, you could create the rules there and export the policy for implementation on an edition of Windows that does support AppLocker rule enforcement.

Can SRP rules be migrated to AppLocker rules?

No, not directly. Because AppLocker is an entirely new feature in Windows 7 and Windows Server 2008 R2, AppLocker rules are not based on the same technology as Software Restriction Policies (SRP) rules. To migrate existing SRP rules, you must carefully analyze your existing SRP rules and determine how they would conceptually map to new AppLocker rules.

What are rule conditions?

Rule conditions are properties of files that AppLocker uses to enforce rules. Each AppLocker rule can use one primary rule condition. There are three rule conditions in AppLocker: publisher, path, and file hash.

- **Publisher**: Can only be used for files that are digitally signed by a software publisher. This condition type uses the digital certificate (publisher name and product name) and properties of the file (file name and file version). This type of rule can be created for an entire product suite, which allows the rule in most cases to still be applicable when the application is updated.
- **Path**: Based on the file or folder path of where specific applications are installed.
- **File hash**: Based on the unique file hash that Windows cryptographically computes for each file. This condition type is unique, so each time that a publisher updates a file, you must create a new rule.

Can I configure the default AppLocker rule action?

The default rule action is to run only those applications that are specifically allowed in the AppLocker rule set. While there is no setting to configure the default rule behavior, you can use AppLocker's rule set to override it. To do this, create an allow rule with a path condition set to *. This configuration will allow all files to run. You can then create deny rules to block specific files.

Why isn't there a setting to configure the default rule action?

Managing files that are allowed is a more secure and manageable way of controlling applications in an organization. Although initial rule setup can be easier with a deny list, organizations wanting to lock down their environments will find that they will need many more rules to block specific files than if they had created a list of allowed files.

Can I test my AppLocker rules before I enforce them?

Yes, you can use the AppLocker audit only enforcement mode to test your rules before they are enforced.

Can AppLocker rules be applied to specific users or groups?

Yes, rules can be created for specific users or groups. However, a rule can only apply to one user or one group. You can also create AppLocker rules to apply to all users (the Everyone group) and then apply that Group Policy object (GPO) to a specific computer group.

Do I need to upgrade my domain controllers to use AppLocker rules?

No, you do not need to update your domain controllers. You can use existing Windows Server 2003 and Windows Server 2008 domain controllers to host the AppLocker policy. However, you cannot use Windows Server 2003 or Windows Server 2008 computers to create AppLocker rules.

Does AppLocker use any services for its rule enforcement?

Yes, AppLocker uses the Application Identity service (AppIDSvc) for rule enforcement. This service must be set to start automatically in the GPO in order for AppLocker rules to be enforced.

How do I create DLL rules?

To create DLL rules in a GPO, you must enable to DLL rule collection in the Group Policy Management Editor console (gpedit.msc).

1. In the Group Policy Management Editor console, navigate to the AppLocker snap-in in the console tree. (Computer Configuration\Windows Settings\Security Settings\Application Control Policies\AppLocker)
2. Right-click **AppLocker**, and then click **Properties**.
3. Click the **Advanced** tab, click the **Enable the DLL rule collection** check box, and then click **OK**.

Why is the DLL rule collection disabled by default?

Managing DLLs can be a difficult task. Each application requires that specific DLLs are allowed to run, and one application can launch many DLLs. For this reason, implementing DLL rules is a more advanced way of using AppLocker. Improperly configuring DLL rules can cause application compatibility problems, and because AppLocker checks whether a DLL is allowed each time before it is allowed to run, many AppLocker events can be generated in the event log. Therefore, you should carefully plan your DLLs before enabling the rule collection.

Managing AppLocker

Why aren't my AppLocker rules being enforced?

There are two reasons why the AppLocker rules might not be enforced:

- The Application Identity service (AppIDsvc) is not running.
- Rule enforcement is set to **Audit only**.

To determine why your AppLocker rules are not being enforced first check whether the Application Identity service (AppIDSvc) is running.

On a local computer:

1. Using the Services Microsoft Management Console (MMC) snap-in:
    - Click the Start button, type *Services.msc* into the **Search programs and files** box, and then press ENTER.
    - Confirm that the status for **Application Identity** is **Started**.
2. Using PowerShell:
    - Open a PowerShell prompt and run: `get-service appidsvc`
    - Confirm that the service is started.

On a remote computer:

- Open a PowerShell prompt and run: `get-service <computerName> appidsvc`
- Confirm that the service is started.

If the service is running, determine what the rule enforcement for the rule collection is set to enforce rules.

How can I view the AppLocker events on client computers?

To view AppLocker events, you can use event forwarding technologies, Event Viewer (eventvwr.msc), or the get-winevent PowerShell cmdlet. In the Event Viewer, AppLocker events are stored in a log under:

Applications and Services Logs\Microsoft\Windows\AppLocker.

There are two child logs: one for executables and DLLs and another for Windows Installer files and scripts.

What should I do if my rules are too restrictive and Windows is behaving irregularly or will not boot?

When AppLocker is enabled, only applications that are specified will be allowed to run. When you first create rules, AppLocker will prompt you to create the default rules. These default rules ensure that key Windows system files and all files in the Program Files directory will be permitted to run. While the default rules are not mandatory, we recommend that you start with the default rules as a baseline and then edit them or create your own to ensure that Windows will function properly.

If computers cannot start properly due to your AppLocker policy, edit the AppLocker rules in the corresponding Group Policy object (GPO) to be less restrictive. If the AppLocker rules are defined in a computer's local policy, boot the computer into safe mode, create the default AppLocker rules, and then reboot the computer.