Introduction to Microsoft AppLocker

Scott Quimby

January 2017

Microsoft AppLocker

- AppLocker was introduced in Windows Server 2008 R2 and Windows 7 that advances the application control features and functionality of Software Restriction Policies. AppLocker contains new capabilities and extensions that allow you to create rules to allow or deny applications from running based on unique identities of files and to specify which users or groups can run those applications.

Microsoft AppLocker

- **Using AppLocker you can:**
  - Control the following types of applications: executable files (.exe and .com), scripts (.js, .ps1, .vbs, .cmd, and .bat), Windows Installer files (.mst, .msi and .msp), and DLL files (.dll and .ocx), and packaged apps and packaged app installers (appx).
  - 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, all criteria in the existing policy are overwritten.
  - Streamline creating and managing AppLocker rules by using Windows PowerShell cmdlets.
- **AppLocker helps reduce administrative overhead and helps reduce the organization's cost of managing computing resources by decreasing the number of help desk calls that result from users running unapproved applications.**

Previously EXE Run Lists

- **EXE Run Lists**
  - Controlled by GPO
  - Run only these EXEs
  - Run anything but these EXEs
- **Then Software Restriction Policies**
  - Run EXE only from a specific location.
  - Tag an EXE so that only the real EXE and not a renamed EXE will be allowed to run (hash rules).

Use Scenarios

- Application Inventory
- Protection Against Unwanted Software
- Licensing Conformance
- Software Standardization
- Manageability Improvements

Compare AppLocker to Software Restriction Policies

What features are different between Software Restriction Policies and AppLocker?

Feature differences

The following table compares AppLocker to Software Restriction Policies.

Feature	Software Restriction Policies	AppLocker
Rule scope	All users	Specific user or group
Rule conditions provided	File hash, path, certificate, registry path, and Internet zone	File hash, path, and publisher
Rule types provided	Defined by the security levels: • Disallowed • Basic User • Unrestricted	Allow and deny
Default rule action	Unrestricted	Implicit 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
Windows PowerShell support	No	Yes
Custom error messages	No	Yes

Compare AppLocker to Software Restriction Policies

Application control function	SRP	AppLocker
Operating system scope	SRP policies can be applied to all Windows operating systems beginning with Windows XP and Windows Server 2003.	AppLocker policies apply only to those supported operating system versions and editions listed in Requirements to Use AppLocker. But these systems can also use SRP. **Note** Use different GPOs for SRP and AppLocker rules.
User support	SRP allows users to install applications as an administrator.	AppLocker policies are maintained through Group Policy, and only the administrator of the computer can update an AppLocker policy. AppLocker permits customization of error messages to direct users to a Web page for help.
Policy maintenance	SRP policies are updated by using the Local Security Policy snap-in or the Group Policy Management Console (GPMC).	AppLocker policies are updated by using the Local Security Policy snap-in or the GPMC. AppLocker supports a small set of PowerShell cmdlets to aid in administration and maintenance.
Policy management infrastructure	To manage SRP policies, SRP uses Group Policy within a domain and the Local Security Policy snap-in for a local computer.	To manage AppLocker policies, AppLocker uses Group Policy within a domain and the Local Security Policy snap-in for a local computer.
Block malicious scripts	Rules for blocking malicious scripts prevents all scripts associated with the Windows Script Host from running, except those that are digitally signed by your organization.	AppLocker rules can control the following file formats: .ps1, .bat, .cmd, .vbs, and .js. In addition, you can set exceptions to allow specific files to run.
Manage software installation	SRP can prevent all Windows Installer packages from installing. It allows .msi files that are digitally signed by your organization to be installed.	The Windows Installer rule collection is a set of rules created for Windows Installer file types (.mst, .msi and .msp) to allow you to control the installation of files on client computers and servers.
Manage all software on the computer	All software is managed in one rule set. By default, the policy for managing all software on a computer disallows all software on the user's computer, except software that is installed in the Windows folder, Program Files folder, or subfolders.	Unlike SRP, each AppLocker rule collection functions as an allowed list of files. Only the files that are listed within the rule collection will be allowed to run. This configuration makes it easier for administrators to determine what will occur when an AppLocker rule is applied.
Different policies for different users	Rules are applied uniformly to all users on a particular computer.	On a computer that is shared by multiple users, an administrator can specify the groups of users who can access the installed software. Using AppLocker, an administrator can specify the user to whom a specific rule should apply.

Requirements

- **AppLocker is available in the following editions of Windows:**
  - Windows Server 2008 R2 Standard
  - Windows Server 2008 R2 Enterprise
  - Windows Server 2008 R2 Datacenter
  - Windows Server 2008 R2 for Itanium-Based Systems
  - Windows 7 Ultimate
  - Windows 7 Enterprise

Review/Audit AppLocker Policies

Discover the effect of an AppLocker policy

You can evaluate how the AppLocker policy is currently implemented for documentation or audit purposes, or before you modify the policy. Updating your AppLocker Policy Deployment Planning document will help you track your findings. For information about creating this document, see Creating Your AppLocker Planning Document. You can perform one or more of the following steps to understand what application controls are currently enforced through AppLocker rules.

- **Analyze the AppLocker logs in Event Viewer**

  When AppLocker policy enforcement is set to **Enforce rules**, rules are enforced for the rule collection and all events are audited. When AppLocker policy enforcement is set to **Audit only**, rules are not enforced but are still evaluated to generate audit event data that is written to the AppLocker logs.

  For the procedure to access the log, see View the AppLocker Log in Event Viewer.

- **Enable the Audit only AppLocker enforcement setting**

  By using the **Audit only** enforcement setting, you can ensure that the AppLocker rules are properly configured for your organization. When AppLocker policy enforcement is set to **Audit only**, rules are only evaluated but all events generated from that evaluation are written to the AppLocker log.

  For the procedure to do this, see Configure an AppLocker Policy for Audit Only.

- **Review AppLocker events with Get-AppLockerFileInformation**

  For both event subscriptions and local events, you can use the **Get-AppLockerFileInformation** Windows PowerShell cmdlet to determine which files have been blocked or would have been blocked (if you are using the audit-only enforcement mode) and how many times the event has occurred for each file.

  For the procedure to do this, see Review AppLocker events with Get-AppLockerFileInformation.

- **Review AppLocker events with Test-AppLockerPolicy**

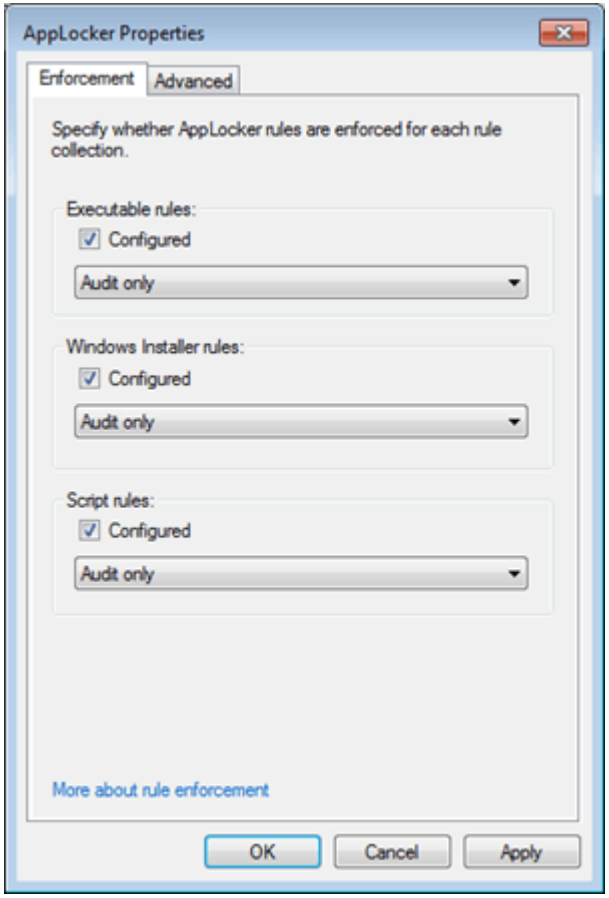
  You can use the **Test-AppLockerPolicy** Windows PowerShell cmdlet to determine determine whether any of the rules in your rule collections will be blocked on your reference computer or the computer on which you maintain policies.

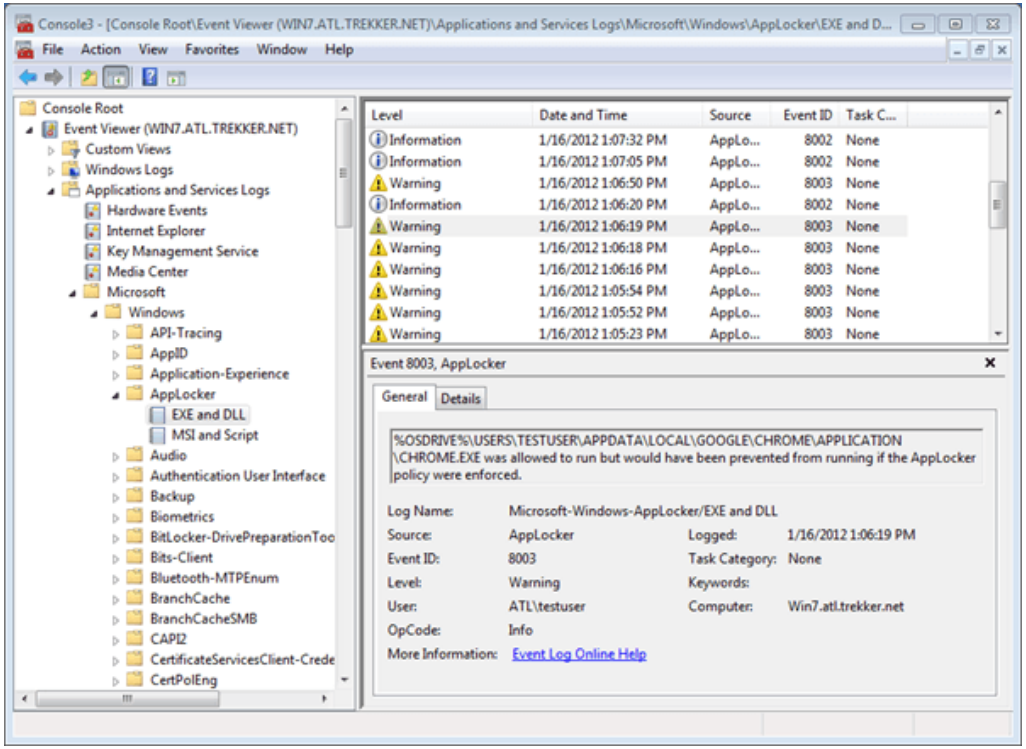
  For the procedure to do this, see Test an AppLocker Policy by Using Test-AppLockerPolicy.

Best Practices

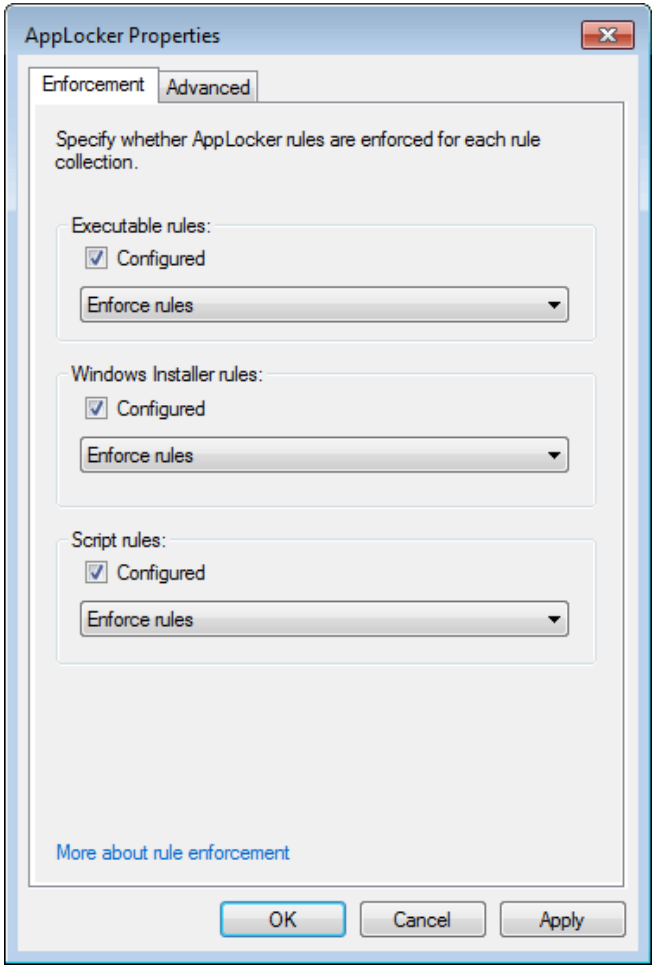
- Whenever possible use default rules
- Use publisher digital signatures
- Name your rules so you understand them
- Specify file paths for places you download from including SYSVOL.
- UAC causes Denys for Builtin\Administrators

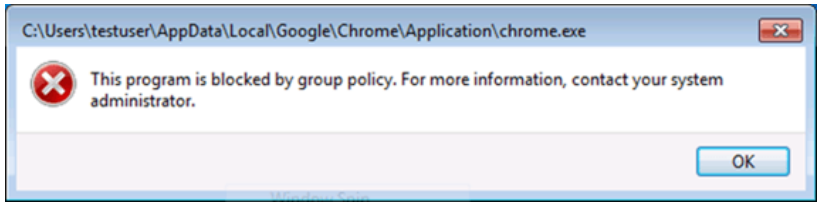
Testing



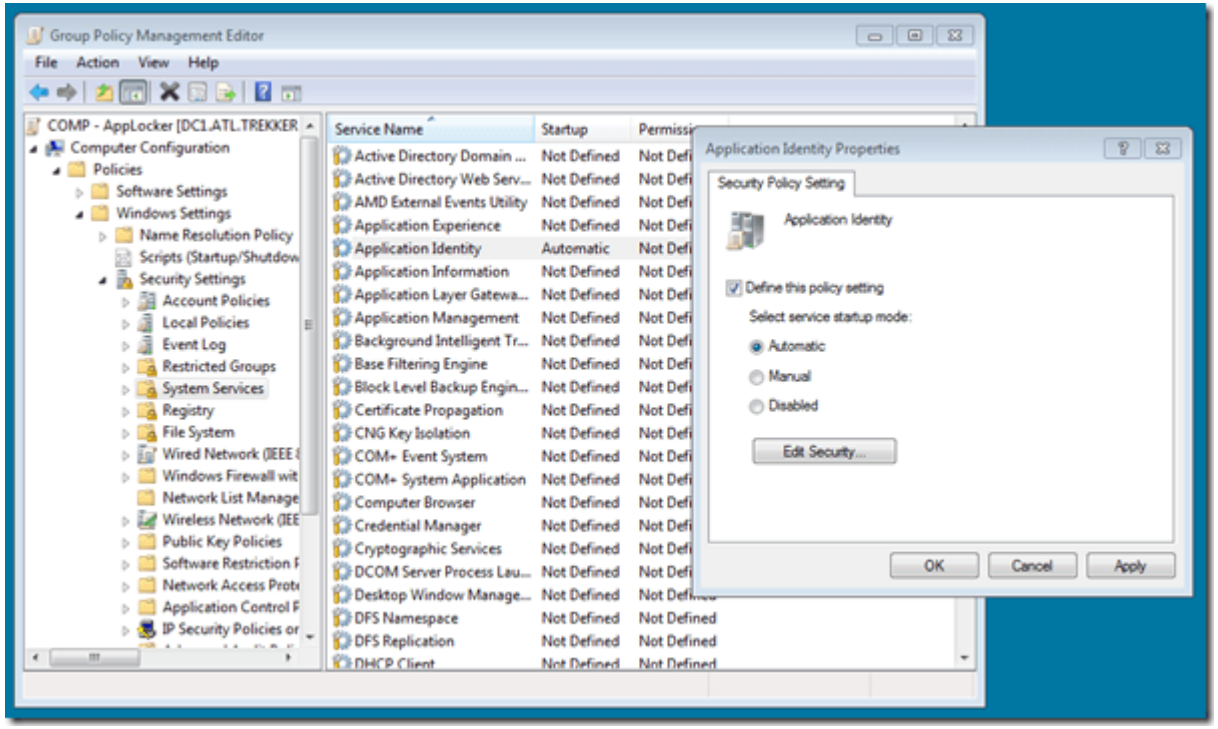


Enforce





Enable Application Identity Service



csiny.com