**Windows AppLocker 概述**

AppLocker 是 Windows 7 中的新功能，Windows Server 2008 R2 取代了软件限制策略功能。AppLocker 包含减少管理开销的新功能和扩展（如可执行文件、脚本、Windows Installer 文件和 DLL），帮助管理员控制用户如何访问和使用文件。使用 AppLocker，您可以：

* 基于从数字签名派生的文件属性（包括发布者、产品名称、文件名和文件版本）定义规则。例如，可以根据更新过程中持续存在的发布者属性创建规则，或者为特定版本的文件创建规则。
* 向安全组或单个用户分配规则。
* 创建规则的例外。例如，可以创建一个规则，允许除注册表编辑器（Regedit.exe）之外的所有 Windows 进程运行。
* 使用仅审核模式部署策略并了解其影响，然后再强制该策略。
* 导入和导出规则。导入和导出影响整个策略。例如，如果导出策略，则会导出所有规则集合中的所有规则，包括规则集合的强制设置。如果导入策略，则会覆盖现有策略。
* 使用 AppLocker PowerShell cmdlet 简化 AppLocker 规则的创建和管理。

有关 AppLocker 规则的详细信息，请参阅[了解 AppLocker 规则](mk:@MSITStore:C:\Windows\help\mui\0804\applocker_help.chm::/html/2a7b3de9-06f2-4647-9a61-53148781f313.htm)。

**什么发生了更改？**

下表将 AppLocker 和软件限制策略进行了对比。

|  |  |  |
| --- | --- | --- |
| **功能** | **软件限制策略** | **AppLocker** |
| 规则作用域 | 所有用户 | 特定用户或组 |
| 提供的规则条件 | 文件哈希、路径、证书、注册表路径和 Internet 区域规则 | 文件哈希、路径和发布者规则 |
| 提供的规则类型 | 允许和拒绝 | 允许和拒绝 |
| 默认规则操作 | 允许或拒绝 | 拒绝 |
| 仅审核模式 | 否 | 是 |
| 一次创建多个规则的向导 | 否 | 是 |
| 策略导入或导出 | 否 | 是 |
| 规则集合 | 否 | 是 |
| PowerShell 支持 | 否 | 是 |
| 自定义错误消息 | 否 | 是 |

**AppLocker 要求**

AppLocker 在所有版本的 Windows Server 2008 R2、Windows 7 旗舰版 和 Windows 7 企业版 中可用。若要使用 AppLocker，您需要：

* 运行 Windows Server 2008 R2、Windows 7 旗舰版、Windows 7 企业版 或 Windows 7 专业版 的计算机创建 AppLocker 规则。Windows 7 专业版 可用于创建规则，但无法在运行 Windows 7 专业版 的计算机上强制执行规则。计算机可以是域控制器。
* 对于组策略部署，至少一台已安装组策略管理控制台 (GPMC) 或远程管理工具 (RSAT) 的计算机用于驻留 AppLocker 规则。
* 运行 Windows Server 2008 R2、Windows 7 旗舰版 或 Windows 7 企业版 的计算机强制执行您创建的 AppLocker 规则。