**了解 AppLocker 规则**

**规则集合**

AppLocker Microsoft 管理控制台 (MMC) 管理单元组织在称为规则集合的四个区域。四个规则集合是可执行文件、脚本、Windows Installer 文件和 DLL 文件。这些集合使管理员易于区分不同类型应用程序的规则。下表列出了每个规则集合中包含的文件格式。

|  |  |
| --- | --- |
|  | 注意 |
|  | 默认情况下不启用 DLL 规则集合。若要了解如何启用 DLL 规则集合，请参阅[强制执行 AppLocker 规则](mk:@MSITStore:C:\\Windows\\help\\mui\\0804\\applocker_help.chm::/html/9c045c1f-f7b2-4bb1-ac1d-714f88dde245.htm)。 |

|  |  |
| --- | --- |
| **规则集合** | **相关文件格式** |
| 可执行文件 | .exe  .com |
| 脚本 | .ps1  .bat  .cmd  .vbs  .js |
| Windows Installer | .msi  .msp |
| DLL | .dll  .ocx |

|  |  |
| --- | --- |
|  | 重要 |
|  | 如果使用 DLL 规则，则必须为每个由所有允许的应用程序使用的 DLL 创建一个 DLL 允许规则。 |

|  |  |
| --- | --- |
|  | 小心 |
|  | 使用 DLL 规则时，AppLocker 必须检查应用程序加载的每个 DLL。因此，如果使用 DLL 规则，用户可能会感觉到性能降低。 |

**规则条件**

规则条件是 AppLocker 规则的条件基础。创建 AppLocker 规则需要主条件。三个主规则条件为发布者、路径和文件哈希。

**发布者**

此条件根据应用程序的数字签名和扩展属性来标识应用程序。数字签名包含有关创建此应用程序的公司（发布者）的信息。从二进制资源获取的扩展属性包含产品（应用程序是其一部分）的名称和应用程序版本号。发布者可能是软件开发公司，如 Microsoft 或您所在组织的信息技术部门。

|  |  |
| --- | --- |
|  | 注意 |
|  | 可能时使用发布者条件。可以创建发布者条件以允许应用程序继续工作，即使应用程序的位置已更改或应用程序已更新。 |

为发布者条件选择引用文件时，向导会创建指定发布者、产品、文件名和版本号的规则。可以通过向下移动滑块或在产品、文件名或版本号字段中使用通配符 (\*) 使规则更通用。

|  |  |
| --- | --- |
|  | 注意 |
|  | 若要在创建规则向导中创建规则时输入自定义值，必须选中**“使用自定义值”**复选框。选中此复选框时，无法使用滑块调整规则的通用程度。 |

**文件版本**控制用户可以运行特定版本、早期版本还是更新版本。可以选择版本号，然后配置下列选项：

* **严格一致。**该规则仅适用于此版本应用程序。
* **及以上版本。**该规则适用于此版本和所有更新版本。
* **及以下版本。**该规则适用于此版本和所有早期版本。

下表描述如何应用发布者条件。

|  |  |  |
| --- | --- | --- |
| **选项** | | **发布者条件允许或拒绝…** |
| **所有已签名的文件** | | 由发布者签名的所有文件。 |
| **仅限发布者** | | 由命名发布者签名的所有文件。 |
| **发布者和产品名称** | | 由命名发布者签名的指定产品的所有文件。 |
| **发布者和产品名称以及文件名。** | | 由发布者签名的命名产品的任何版本命名文件。 |
| **发布者、产品名称、文件名和文件版本** | **严格一致** | 由发布者签名的命名产品的指定版本命名文件。 |
| **发布者、产品名称、文件名和文件版本** | **及以上版本** | 由发布者签名的产品的指定版本命名文件和任何新版本。 |
| **发布者、产品名称、文件名和文件版本** | **及以下版本** | 由发布者签名的产品的指定版本命名文件和任何旧版本。 |
| **自定义** | | 可以编辑**“发布者”**、**“产品名称”**、**“文件名”**和**“版本”**字段来创建自定义规则。 |

**路径**

此条件按照应用程序在计算机的文件系统中或在网络上的位置标识应用程序。

AppLocker 使用 Windows 中目录的路径变量。

|  |  |
| --- | --- |
|  | 注意 |
|  | 这些路径变量中的两个变量与 Windows 环境变量使用相同格式，这两个变量不是环境变量。AppLocker 只能解释 AppLocker 路径变量。 |

下表详细说明了这些路径变量。

|  |  |  |
| --- | --- | --- |
| **Windows 目录或驱动器** | **AppLocker 路径变量** | **Windows 环境变量** |
| Windows | %WINDIR% | %SystemRoot% |
| System32 | %SYSTEM32% | %SystemDirectory% |
| Windows 安装目录 | %OSDRIVE% | %SystemDrive% |
| Program Files | %PROGRAMFILES% | %ProgramFiles% 和  %ProgramFiles(x86)% |
| 可移动媒体（例如，CD 或 DVD） | %REMOVABLE% |  |
| 可移动存储设备（例如，USB 闪存驱动器） | %HOT% |  |

|  |  |
| --- | --- |
|  | 重要 |
|  | 由于可以将路径条件配置为包含大量文件夹和文件，应仔细计划路径条件。例如，如果带有路径条件的允许规则包含允许非管理员写入数据的文件夹位置，则用户可以将未经批准的文件复制到该位置并运行文件。因此，最好不为标准用户可写位置创建路径条件，如用户配置文件。 |

**文件哈希**

选择文件哈希条件时，系统会计算已标识文件的加密哈希。

**AppLocker 默认规则**

AppLocker 允许您为每个规则类型生成默认规则。

可执行文件默认规则类型：

* 允许本地**管理员**组的成员运行所有应用程序。
* 允许 **Everyone** 组的成员运行位于 Windows 文件夹中的应用程序。
* 允许 **Everyone** 组的成员运行位于 Program Files 文件夹中的应用程序。

Windows Installer 默认规则类型：

* 允许本地**管理员**组的成员运行所有 Windows Installer 文件。
* 允许 **Everyone** 组的成员运行数字签名的 Windows Installer 文件。
* 允许 **Everyone** 组的成员运行位于 Windows\Installer 文件夹中的所有 Windows Installer 文件。

脚本默认规则类型：

* 允许本地**管理员**组的成员运行所有脚本。
* 允许 **Everyone** 组的成员运行位于 Program Files 文件夹中的脚本。
* 允许 **Everyone** 组的成员运行位于 Windows 文件夹中的脚本。

DLL 默认规则类型：

* 允许本地**管理员**组的成员运行所有 DLL。
* 允许 **Everyone** 组的成员运行位于 Program Files 文件夹中的 DLL。
* 允许 **Everyone** 组的成员运行位于 Windows 文件夹中的 DLL。

有关详细信息，请参阅[创建默认 AppLocker 规则](mk:@MSITStore:C:\Windows\help\mui\0804\applocker_help.chm::/html/29eb37a3-bfb9-4681-a52f-be79908d244d.htm)。

**AppLocker 规则行为**

如果不存在特定规则集合的 AppLocker 规则，则允许具有该文件格式的所有文件运行。但是，当为特定规则集合创建了 AppLocker 规则时，仅允许规则中明确允许的文件运行。例如，如果创建了允许 *%SystemDrive%\FilePath* 中的 .exe 文件运行的可执行文件规则，则仅允许位于该路径中的可执行文件运行。

可将规则配置为使用允许或拒绝操作：

* **允许。**可以指定允许哪些文件在您的环境中运行，以及对哪些用户或用户组运行。还可以将例外配置为标识从规则中排除的文件。
* **拒绝。**可以指定*不*允许哪些文件在您的环境中运行，以及对哪些用户或用户组运行。还可以将例外配置为标识从规则中排除的文件。

|  |  |
| --- | --- |
|  | 重要 |
|  | 可以使用允许操作和拒绝操作的组合。但是，建议使用带有例外的允许操作，因为拒绝操作会覆盖所有情况中的允许操作。还可以避免拒绝操作。 |

**规则例外**

可以将 AppLocker 规则应用于单个用户或用户组。如果将规则应用到用户组，则该组中的所有用户均受该规则影响。如果需要允许用户组的子集使用某个应用程序，可以为该子集创建特殊规则。例如，规则“允许每个人运行除注册表编辑器之外的 Windows”允许组织的每个人运行 Windows 但不允许任何人运行注册表编辑器。此规则的效果可能防止用户（如技术支持人员）运行其支持任务所必需的程序。为了解决此问题，请创建应用于 Helpdesk 用户组的第二个规则：“允许支持人员运行注册表编辑器”。如果创建不允许任何用户运行注册表编辑器的拒绝规则，则拒绝规则将覆盖允许 Helpdesk 用户组运行注册表编辑器的第二个规则。

**AppLocker 向导**

可以使用两种方式创建自定义规则：

1. 创建规则向导使您一次可以创建一个规则。有关详细信息，请参阅[创建 AppLocker 规则](mk:@MSITStore:C:\Windows\help\mui\0804\applocker_help.chm::/html/4961ae4d-4aff-4931-a692-709fc7737a18.htm)。
2. 自动生成规则向导允许您选择文件夹，选择要应用规则的用户或组，然后一次为该文件夹创建多个规则。此向导仅自动生成允许规则。有关详细信息，请参阅[自动生成 AppLocker 规则](mk:@MSITStore:C:\Windows\help\mui\0804\applocker_help.chm::/html/4e23b4e4-913e-4c58-b208-22a59783d2c2.htm)。

**其他注意事项**

* 默认情况下，AppLocker 规则不允许用户打开或运行未得到特别允许的任何文件。管理员应维护一个允许的应用程序的最新列表。
* 有两种类型的 AppLocker 条件不持续下列更新：
  + **文件哈希条件。**文件哈希条件可以与任何应用程序一起使用，因为创建规则时会生成应用程序的加密哈希值。但是，该哈希值特定于应用程序的确切版本。如果组织中正使用多种版本的应用程序，则需要为正使用的每个版本以及已发布的任何新版本创建文件哈希条件。
  + **发布者条件带有特定产品版本集。**如果创建使用 **Exactly** 文件条件选项的发布者条件，则一旦安装新版本应用程序，该规则不再继续有效。必须创建新发布者条件，或必须调低规则版本的特定程度。
* 如果未对某个应用程序进行数字签名，则无法使用发布者条件。
* AppLocker 规则无法用于管理运行 Windows 7 之前的 Windows 操作系统的计算机。必须使用软件限制策略。
* 如果组策略对象 (GPO) 中定义了 AppLocker 规则，则仅应用这些规则。为了确保软件限制策略规则和 AppLocker 规则之间的互操作性，请在不同的 GPO 中定义软件限制策略规则和 AppLocker 规则。
* 将 AppLocker 规则设置为**“仅审核”**时，不强制执行该规则。用户运行包含在规则中的应用程序时，该应用程序正常打开并运行，有关该应用程序的信息会添加到 AppLocker 事件日志。
* 已自定义配置的 URL 可包含在阻止应用程序时显示的消息中。
* 可以预见，由于阻止的应用程序最初会增加技术支持呼叫数量。随着用户开始了解他们无法运行不允许的应用程序，技术支持呼叫可能会减少。

**其他参考**

* [配置 AppLocker 规则](mk:@MSITStore:C:\Windows\help\mui\0804\applocker_help.chm::/html/df5d2dfa-a3ae-43ee-8300-c1c0340c01b6.htm)