

【AppLocker】你的应用程序保镖！控制权限，保护你的设备安全！（一）

大家好！今天要给大家介绍一个超级好用的 Windows 功能——AppLocker！

你有没有遇到过这样的情况？你的电脑上的应用程序，被别人随意安装、运行或卸载？或者是在工作环境中的敏感数据，被未授权的用户访问？

别担心，AppLocker 来帮你解决这些问题！

AppLocker 是一款功能强大的应用程序控制策略，它可以帮助你保护你的应用程序，控制应用的权限，让你的设备安全无忧！

使用 AppLocker，你可以设置规则，控制谁可以在你的设备上安装、运行或卸载应用程序。

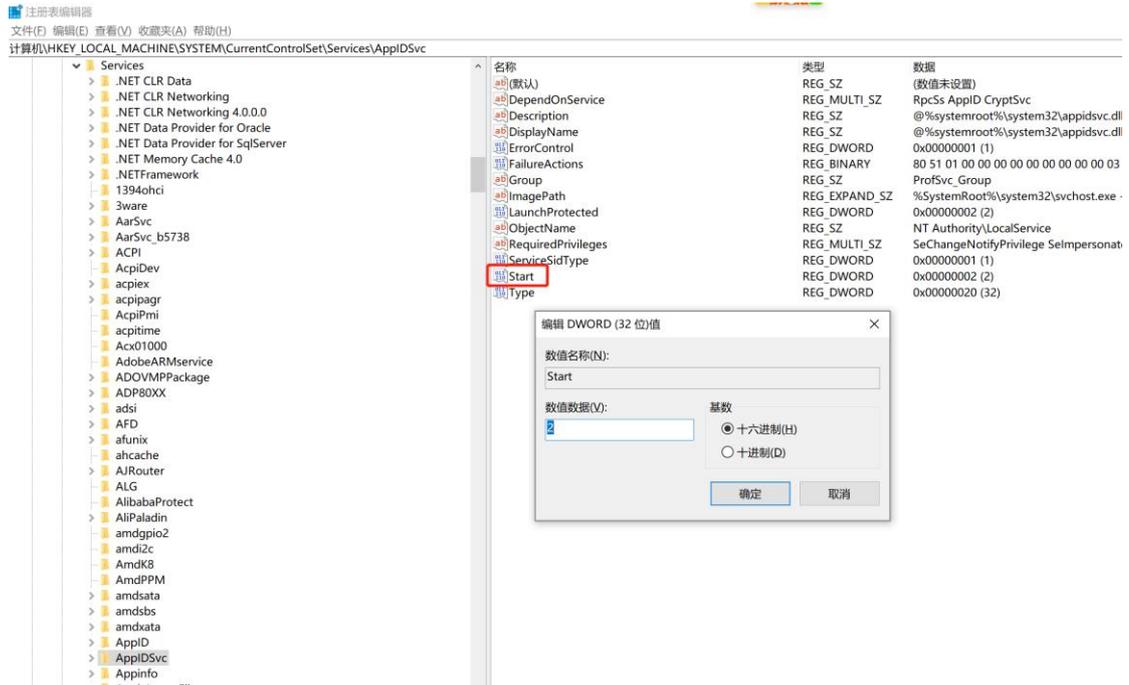
在企业环境中，IT 管理员可以使用 AppLocker 来确保员工只能访问公司批准的应用程序，提高安全性和合规性。

AppLocker 还可以与用户账户控制（UAC）结合使用，为不同的用户组设置不同的访问级别，这样管理员就可以更精细地管理用户对应用程序的访问权限。

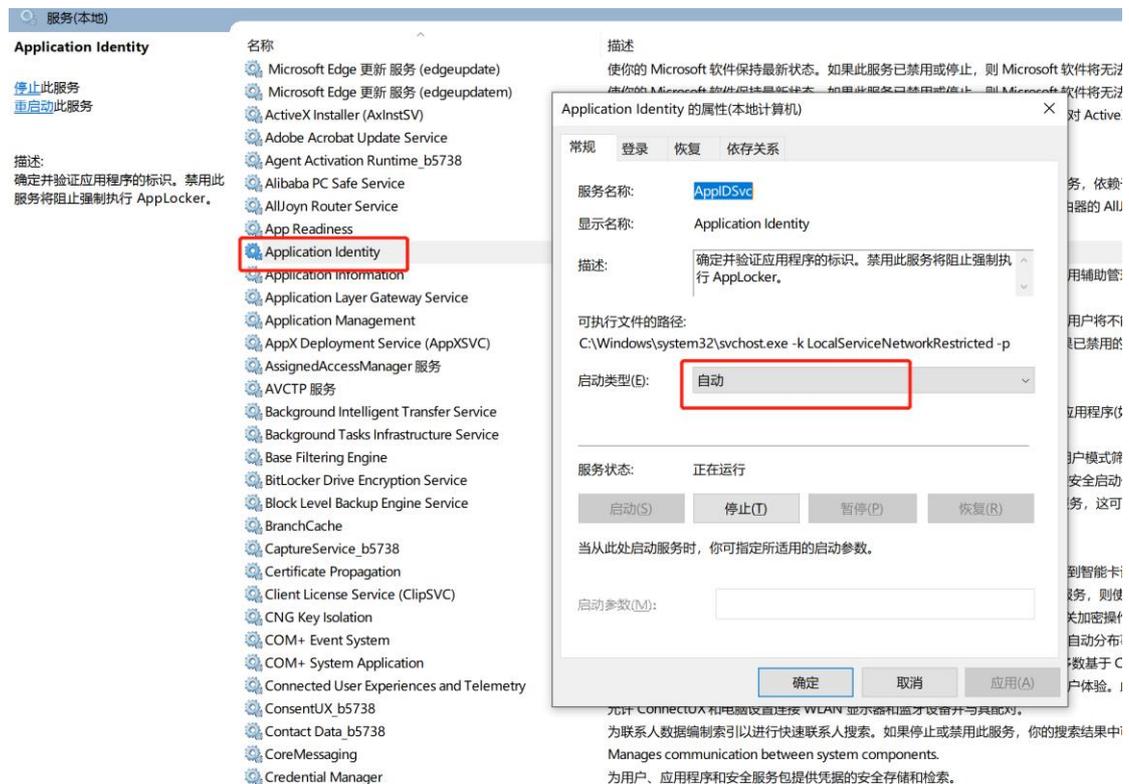
AppLocker 的使用非常简单，只需要几步就可以完成设置。

如何使用 AppLocker 创建规则：

- 1) 按 Win+R，输入“regedit”，打开注册表编辑器，跳转至
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AppIDSvc，
将 start 键值置为 2.



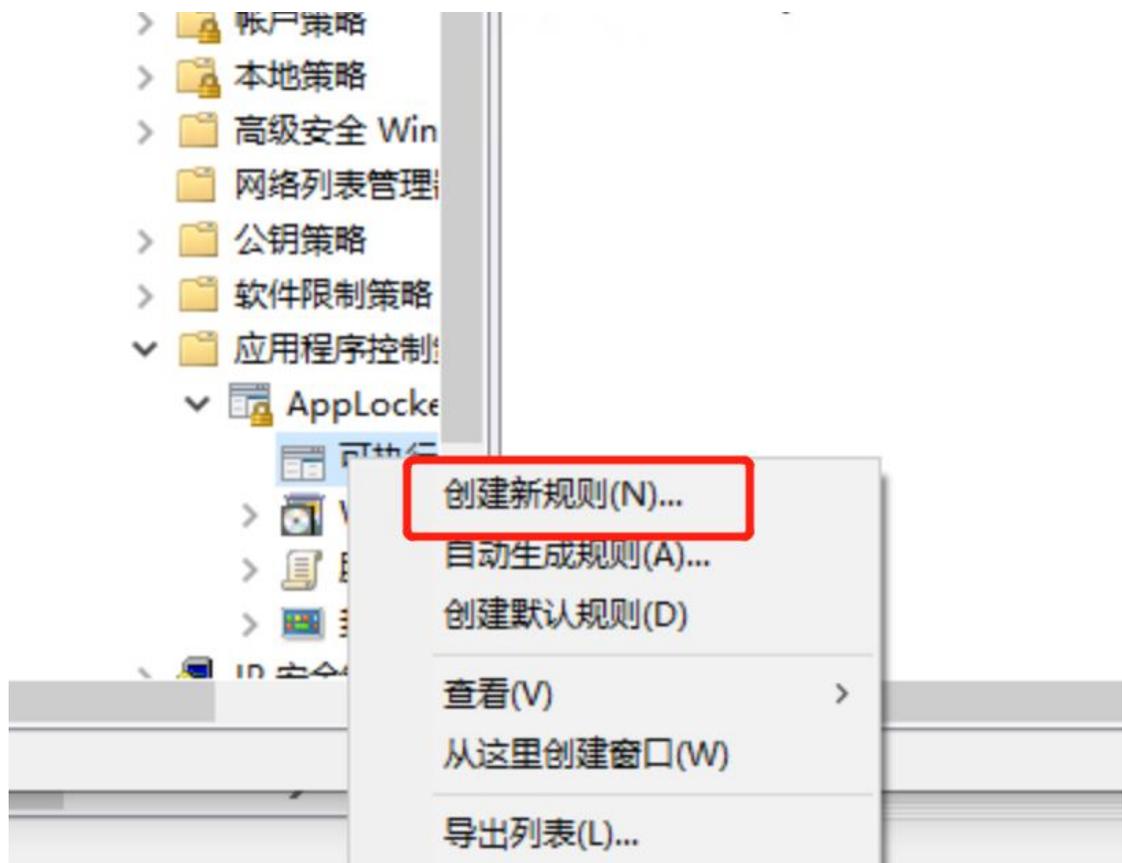
2) 按 Win+R, 输入“services.msc”, 打开服务, 双击 application identity 服务, 点击启动。



3) 按 Win+R, 输入“taskschd.msc”, 展开计划任务-Microsoft-Windows-AppID, 查看对应计划任务是否运行。(如禁用, 可手动开启)



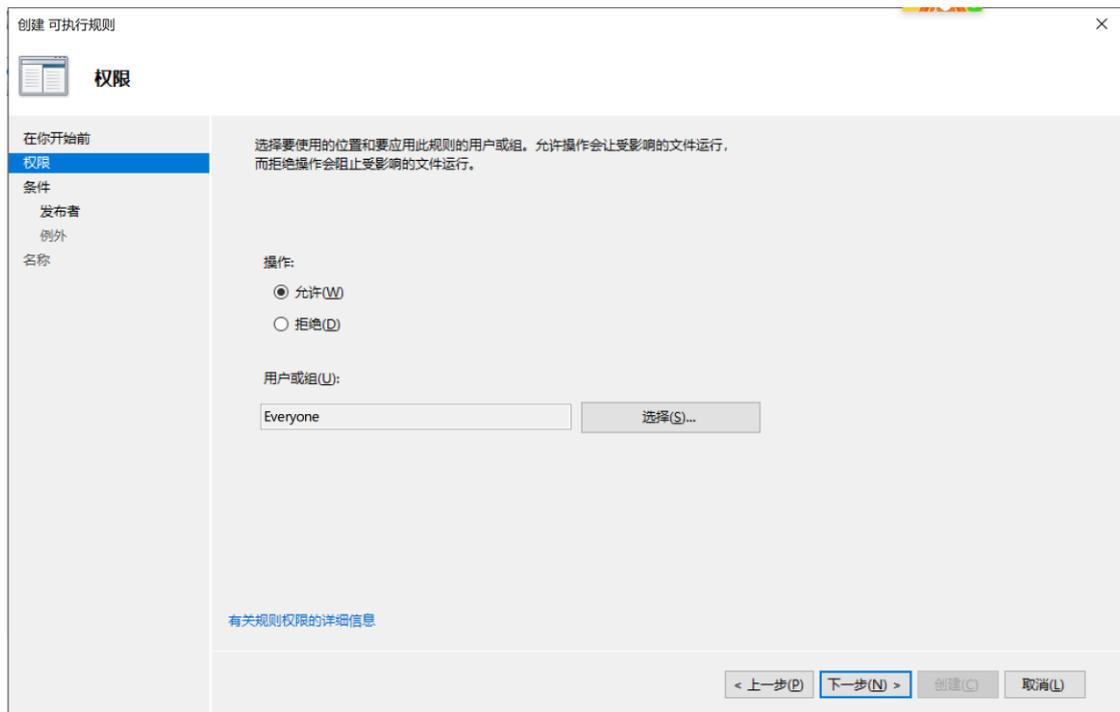
- 4) 在开始菜单-Windows 管理工具-本地安全策略中，展开应用程序控制策略-applocker，根据需要创建规则类型，选择文件类型，以“可执行规则”为例，右键选择“创建新规则”，按照向导进行操作：



点击“下一步”；



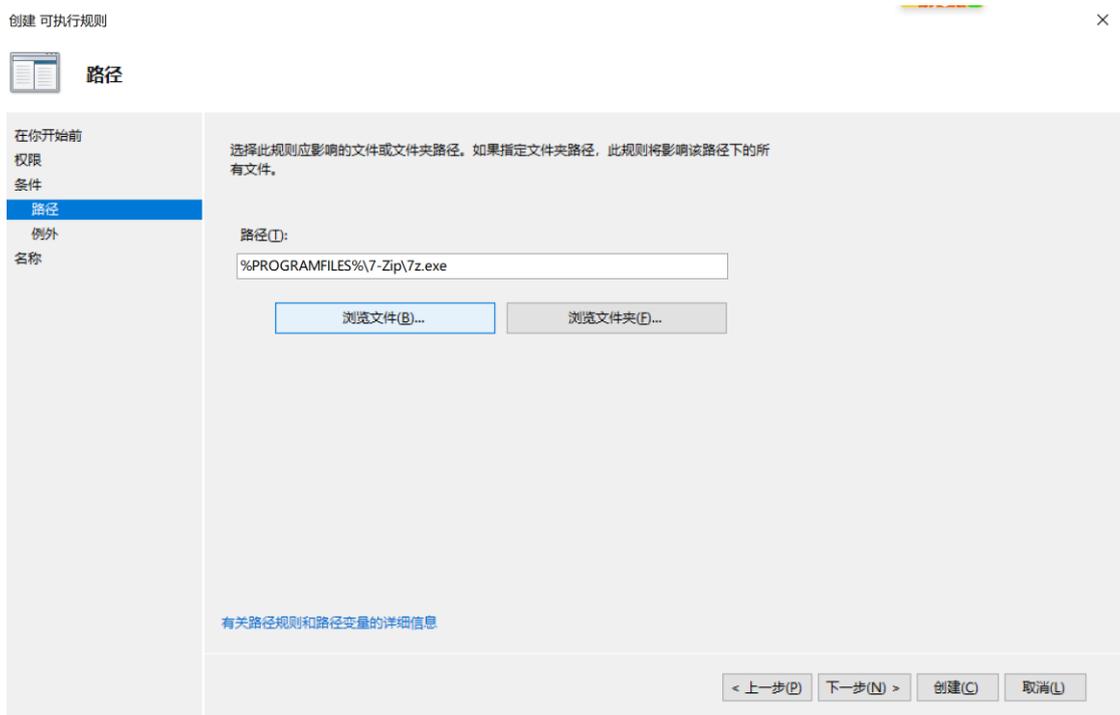
选择操作类型: 允许或拒绝; 选择用户权限, 点击“下一步”;



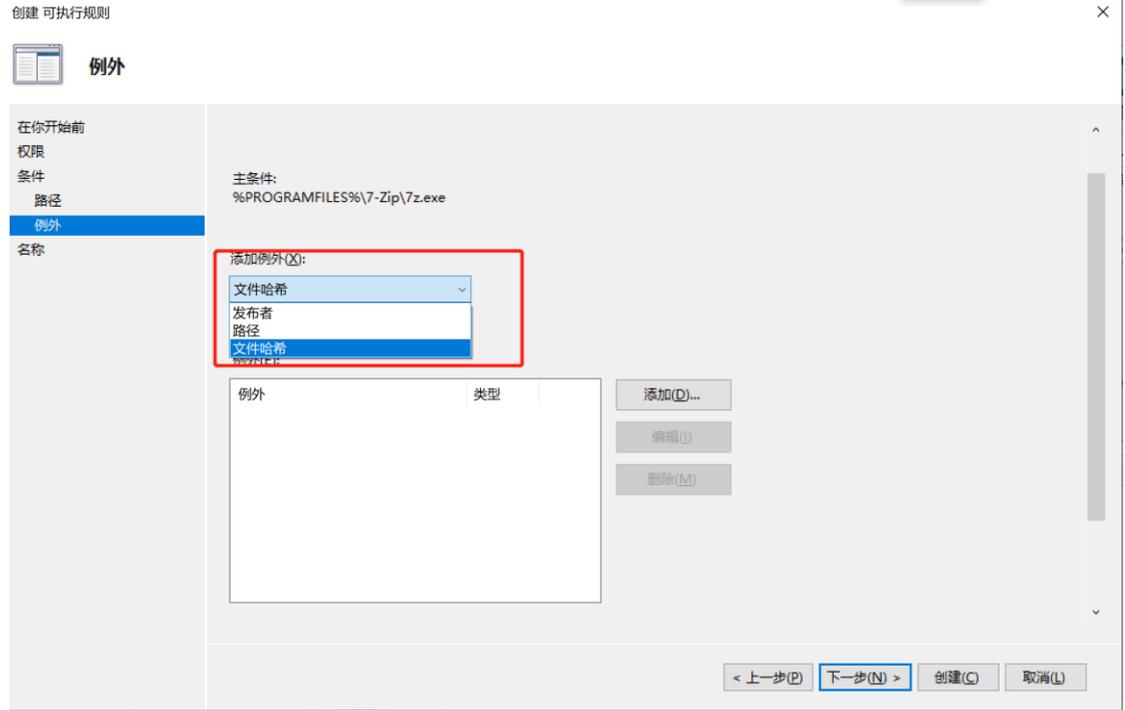
选择条件类型: 发布者, 路径或文件哈希, 点击“下一步”;



指定受规则影响的文件或文件夹，点击“下一步”；



如有需要，可根据条件添加例外，完成后点击“下一步”；



添加例外界面：

发布者例外



浏览已签名文件以用作规则参考。使用滑块选择采用哪些属性来定义规则；向下移动时，规则将变得更具体。当滑块位于任何发布者位置时，规则将应用于所有已签名文件。

引用文件：

C:\Program Files\Windows Mail\wab.exe

浏览(B)...

<input type="checkbox"/>	任何发布者	
<input type="checkbox"/>	发布者(U)：	0=MICROSOFT CORPORATION, L=REDMOND, S=V
<input type="checkbox"/>	产品名(I)：	MICROSOFT® WINDOWS® OPERATING SYSTEM
<input type="checkbox"/>	文件名(F)：	WAB.EXE
<input type="checkbox"/>	文件版本(V)：	10.0.0.0 及以上版本

使用自定义值(S)

规则作用域：
仅适用于此文件的指定版本。

确定(O)

取消(L)

点击“创建”，完成规则创建向导；

创建 可执行规则



名称和描述

在你开始前

权限

条件

路径

例外

名称

输入名称以标识此规则。

名称(M)：

%PROGRAMFILES%\7-Zip\7z.exe

描述(D)：(可选)

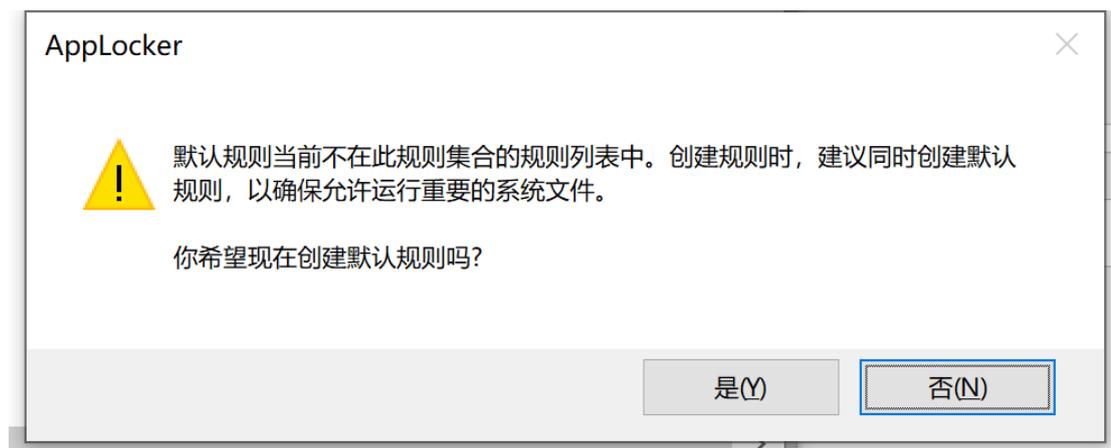
< 上一步(B)

下一步(N) >

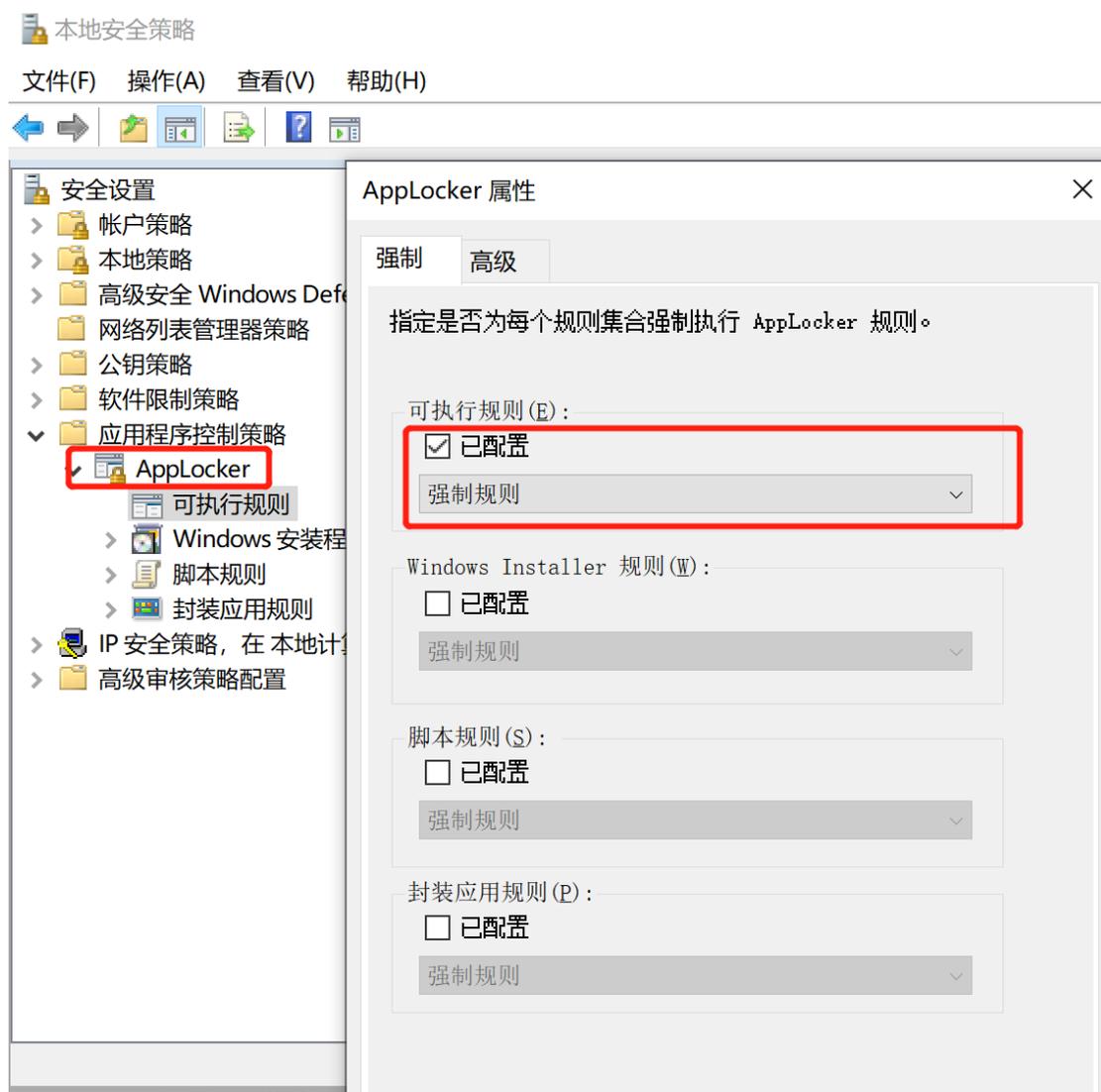
创建(C)

取消(L)

如第一次尚未添加默认规则，系统会询问是否需要添加，点击“是”；



- 5) 右键点击 applocker，选择属性，在“可执行规则”下勾选“已配置”，并选择“强制规则”，点击“确定”；



等待 3-5 分钟或重启电脑，查看新规则是否生效。

祝贺你就成功设置了第一条 AppLocker 规则！

下一期，我将向大家介绍 AppLocker 和软件限制策略的区别，敬请期待！