【AppLocker】VS【SRP】，两大 Windows 安全策略，你了解多少？

大家好！上期给大家介绍一个超级好用的 Windows 功能——AppLocker，可以帮助你保护你的应用程序，控制应用的权限。

你可能会问，AppLocker 和 软件限制策略（Software Restriction Policies，SRP）都是微软 Windows 操作系统中用于应用程序控制和安全策略的工具，那它们有什么不同呢？别急，让我来告诉你！

AppLocker 支持在 Windows 10 神州网信政府版上运行，该功能可帮助管理员锁定系统防止未经授权程序运行。最早在 Windows XP 中引入的 SRP 是为实现该功能采取的第一步，但 SRP 很难管理，并且无法应用于特定的用户或组。(所有用户都会受到 SRP 规则影响。)AppLocker 取代了 SRP，但目前依然与 SRP 共存，不过 AppLocker 的规则会和 SRP 的规则分开存储。如果针对同一个组策略对象(Group Policy Object, GPO)同时应用了 AppLocker 和 SRP 规则，最终将只应用 AppLocker 规则。

控制粒度

AppLocker 提供了更细粒度的控制，允许管理员基于应用程序的以下属性来限制或允许应用程序的运行。这些规则可以单独或组合使用。

- **发布者**：根据应用的数字签名标识应用
- **路径**：按应用在计算机文件系统或网络上的位置标识应用

- **文件哈希**：表示已标识文件的系统计算的加密 Authenticode 哈希

SRP 的控制粒度相对较粗，它主要基于应用程序的证书、哈希值、互联网区域和路径来限制或允许应用程序的运行。

应用场景

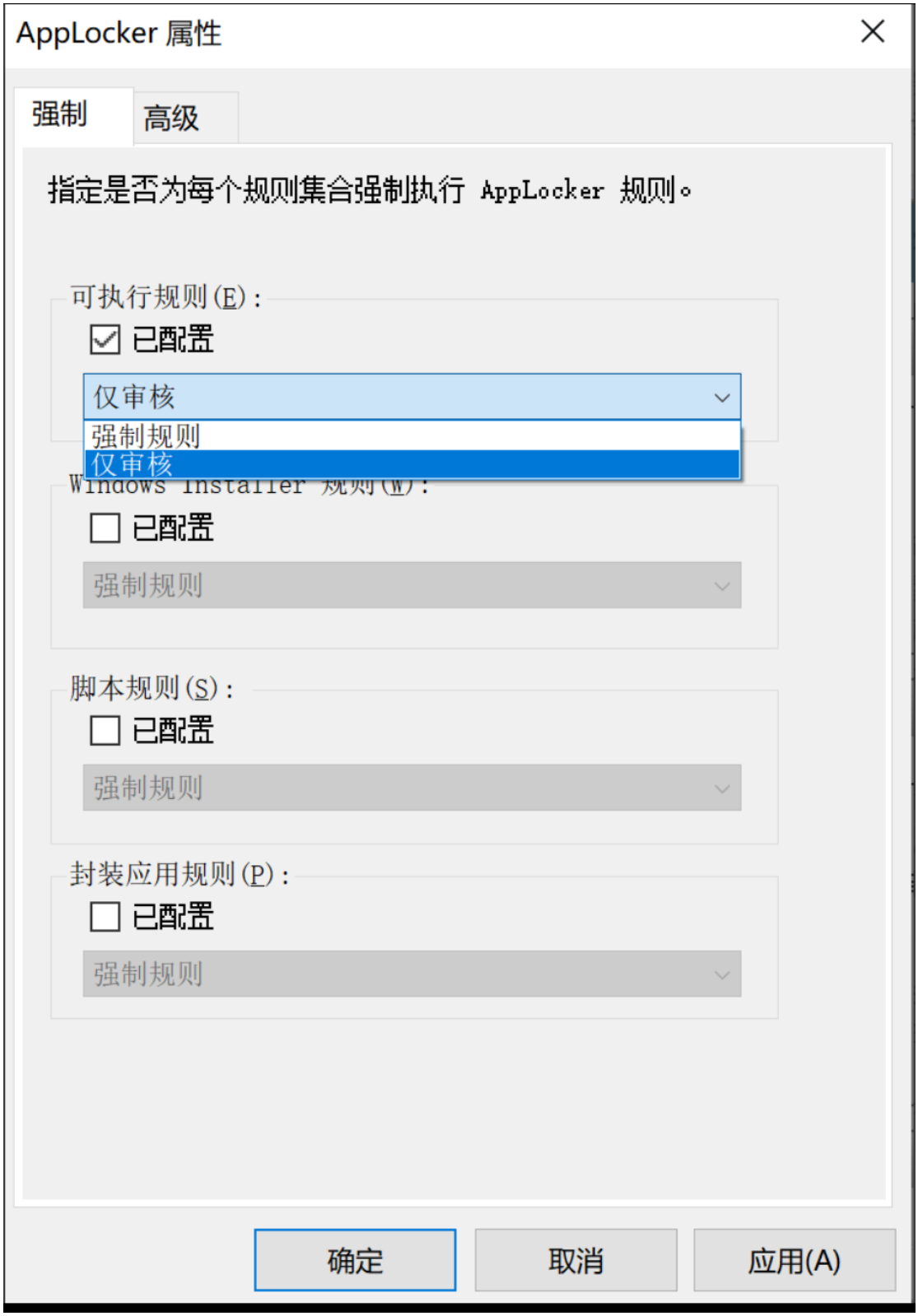
AppLocker 是基于用户账户的，更适合需要对用户进行个性化控制的场景。

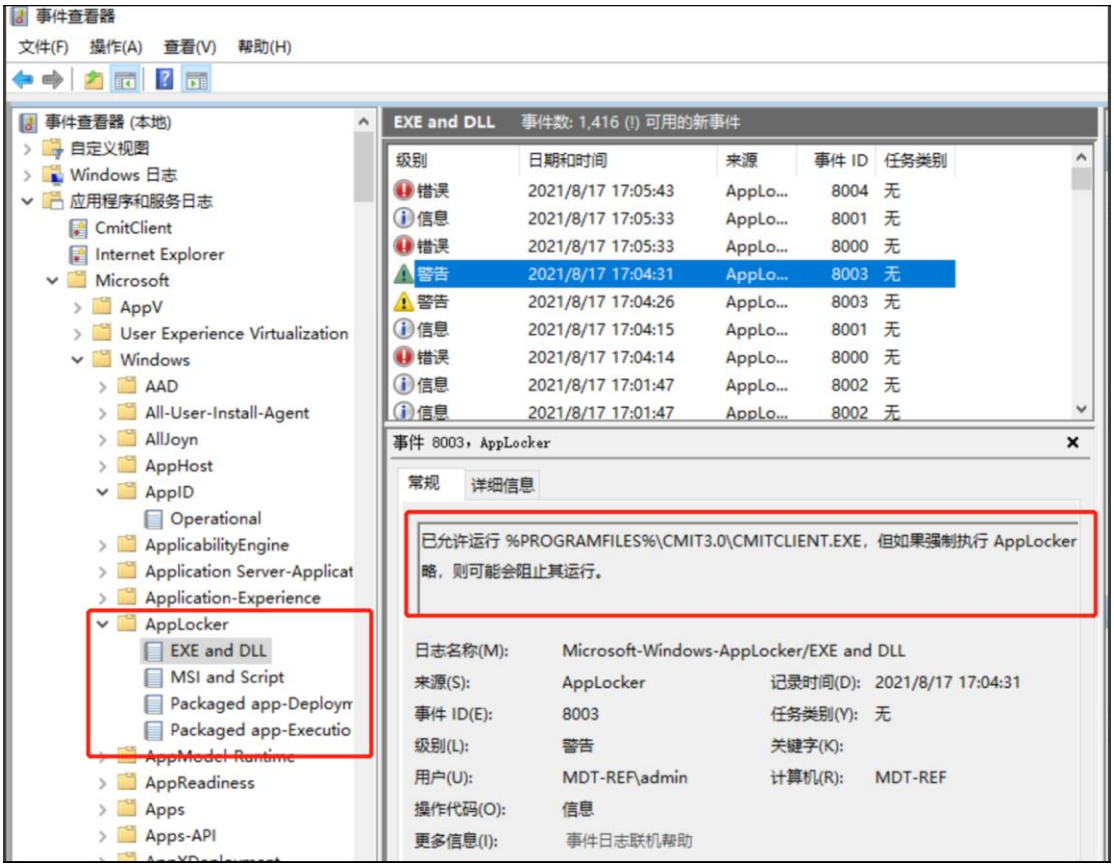
SRP 是基于计算机的，更适合对整个计算机或计算机组进行统一控制的场景。

审核模式

审核模式是 AppLocker 比 SRP 更胜一筹功能。

审核模式可供管理员创建 AppLocker 策略并检查其结果（存储在系统事件日志中），以确定策略是否能按照预期执行，但这一过程中并不会真正执行这些限制。AppLocker 审核模式可用于监视系统中的一个或多个用户曾使用过哪些应用程序。


AppLocker 属性
强制
高级
指定是否为每个规则集合强制执行 AppLocker 规则。
可执行规则(E):
已配置
仅审核
强制规则
仅审核
Windows Installer 规则(W):
已配置
强制规则
脚本规则(S):
已配置
强制规则
封装应用规则(P):
已配置
强制规则
确定
取消
应用(A)



那么，AppLocker 和 SRP 在实际应用中该如何选择呢？这取决于具体的需求和环境。

如果你需要更精细、更灵活的应用程序控制，那么 AppLocker 可能是更好的选择。它提供了更多的规则选项和条件，可以更好地满足复杂的环境需求。

但如果你只需要基本的软件限制和恶意软件防护，SRP 也是一个不错的选择。它相对简单，容易配置，适合一些基础的安全需求。

总的来说，AppLocker 和 SRP 都是 Windows 中强大的安全策略工具，它们各有特点和优势。管理员需要根据具体的需求和环境来选择使用哪种工具。

希望这次的比较能帮助你更好地了解 AppLocker 和 SRP，选择适合自己的安全策略工具！