educación IT
CODE YOUR FUTURE

Introducción a la Ciberseguridad

Módulo 4

AppLocker

AppLocker

AppLocker es una característica disponible en las versiones *Enterprise* y *Ultimate* de Windows 7. Las directivas de AppLocker son similares a las de restricción de software, aunque AppLocker posee varias ventajas, puede ser aplicado a usuario, cuentas de grupo y la capacidad de aplicar a todas las versiones de un producto.

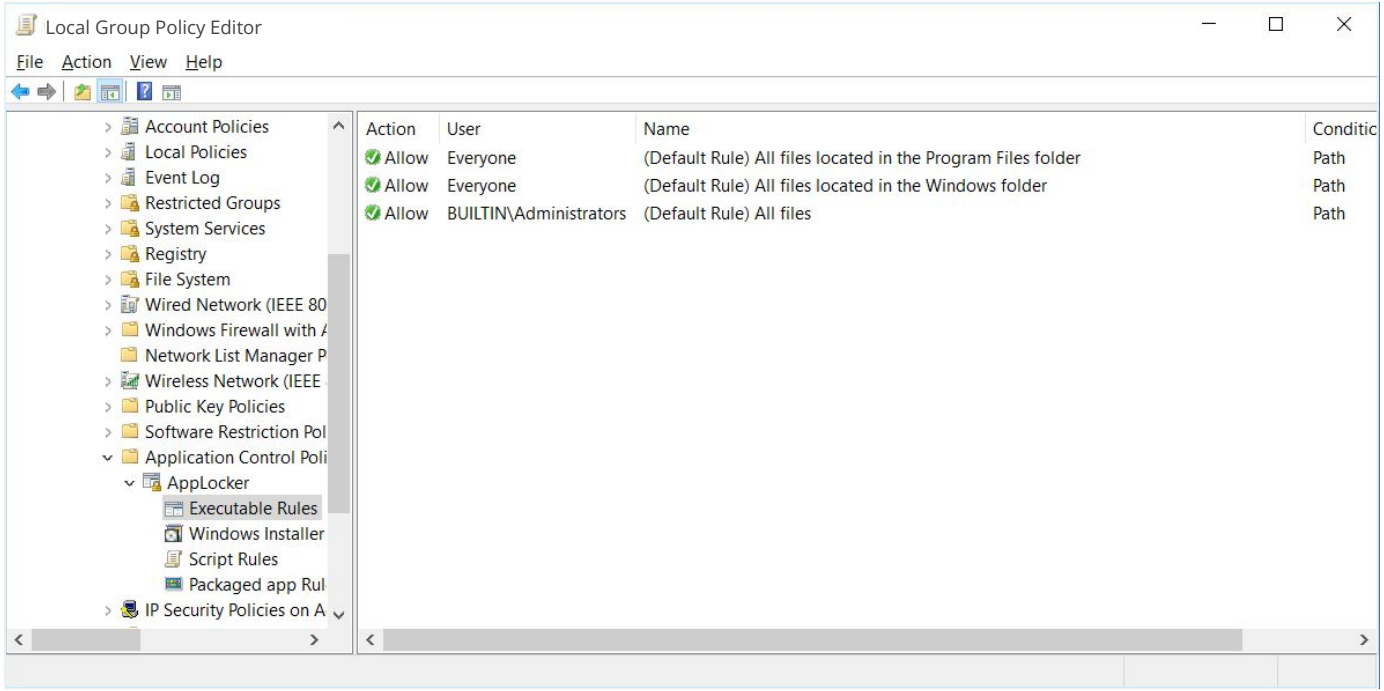
AppLocker se basa en un servicio denominado ***Identidad de la aplicación*** y el **tipo de inicio** de este servicio está configurado como ***Manual.*** Al probar AppLocker, se recomienda mantener el tipo de inicio como *Manual.*

Si se configura una regla de forma incorrecta puedes reiniciar el equipo y la regla de AppLocker dejará de estar en vigor.

Sólo cuando estemos seguros de que las directivas se aplican correctamente debemos configurar el inicio ***Tipo de Servicio de Identidad*** de la aplicación en ***Automático.***

La configuración incorrecta de AppLocker puede bloquear un equipo de forma inutilizable.

AppLocker


Local Group Policy Editor
File Action View Help
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 80
Windows Firewall with A
Network List Manager P
Wireless Network (IEEE
Public Key Policies
Software Restriction Pol
Application Control Poli
AppLocker
Executable Rules
Windows Installer
Script Rules
Packaged app Rul
IP Security Policies on A
Action User Name Conditic
Allow Everyone (Default Rule) All files located in the Program Files folder Path
Allow Everyone (Default Rule) All files located in the Windows folder Path
Allow BUILTIN\Administrators (Default Rule) All files Path

Reglas predeterminadas

Existen reglas que se deben crear de forma automática y que permiten el acceso por defecto de Windows y archivos de programa. Son necesarias porque **AppLocker limita la ejecución de cualquier aplicación que no esté en una regla de permiso.** Esto significa que cuando se habilita AppLocker, no se puede ejecutar ninguna aplicación, script o instalador que no figure en una regla ***Permitir.***

Reglas de Bloqueo

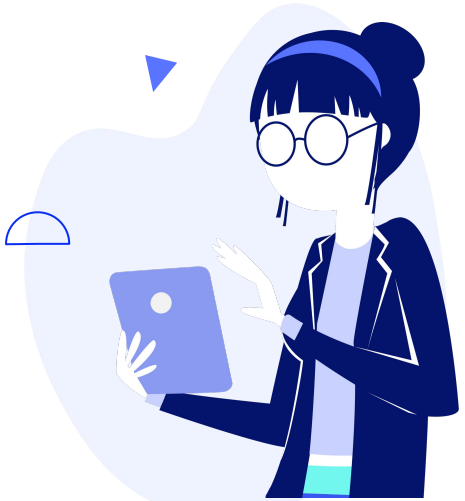
Es necesario añadir una regla de bloqueo sólo si otra regla de AppLocker permite una aplicación, podemos utilizar explícitamente **reglas definidas de bloqueo para impedir la ejecución de aplicaciones que son activadas a través de las reglas predeterminadas.**

Reglas ejecutables

Aplicadas a los archivos ***Exe*** y ***Com***, por defecto son reglas de ruta que **permiten a todos ejecutar todas las aplicaciones en la carpeta *Archivos de programa* y la carpeta de Windows.**

Las reglas predeterminadas también permiten a los administradores ejecutar aplicaciones en cualquier lugar en el equipo.

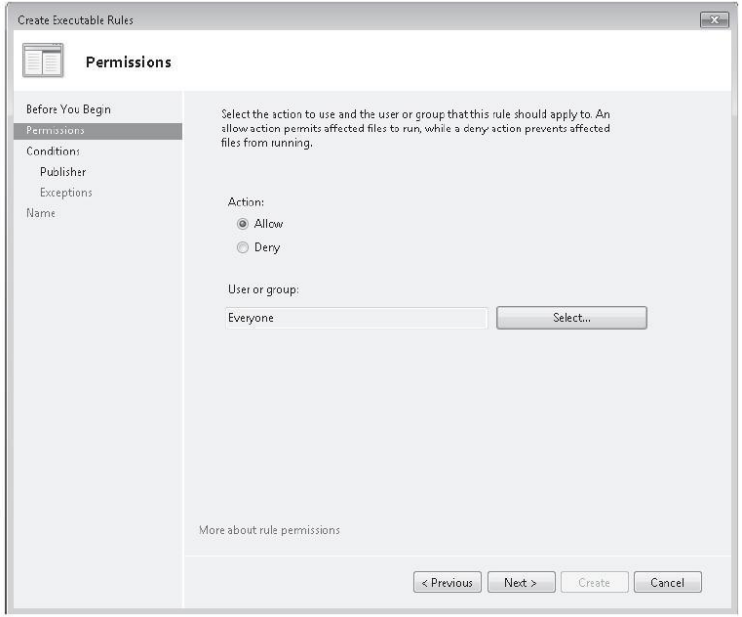
Es necesario utilizar las reglas por defecto, ya que Windows no funcionará correctamente a menos que ciertas aplicaciones, cubiertas por estas reglas, tengan autorización para ejecutar.



Reglas de instalación

Por defecto, permite a todos utilizar archivos firmados por *Windows Installer* en la carpeta **% SystemDrive% \Windows** y los miembros del grupo de administradores local para ejecutar cualquier archivo *msi* o *msp*. Las reglas predeterminadas permiten la instalación y actualización de *software* a través de *Directivas de grupo.*

Es importante recordar que incluso si una regla de AppLocker permite a todos acceder a un archivo de instalación en particular, todavía **necesitan los permisos administrativos pertinentes para instalar *software* en el ordenador.**



Reglas de comandos

Incluye los archivos **bat, cmd, vbs** y extensiones **js.** Aunque es posible el uso de reglas de publicador con secuencias de comandos, la mayoría de *scripts* se crean sobre una base *ad-hoc* por administradores y rara vez son firmados digitalmente.

Podemos utilizar las reglas de hash con los scripts que son rara vez modificados y reglas de ruta con directorios que contienen secuencias de comandos que se actualizan periódicamente.

Reglas DLL

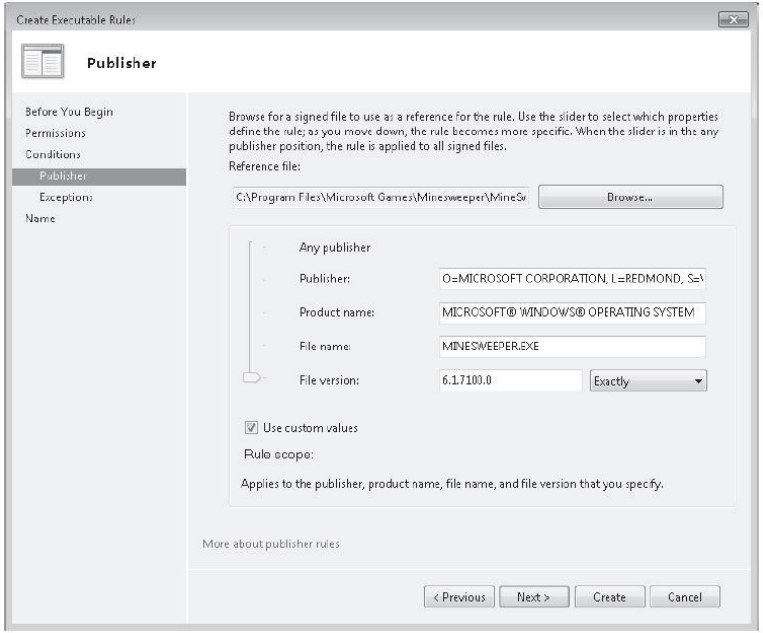
Bibliotecas, archivos DLL y extensiones **ocx**, estas reglas no están habilitadas de forma predeterminada en AppLocker, **es necesario crear una regla para cada DLL utilizada por las aplicaciones,** aunque la creación de reglas es fácil generando reglas automáticamente.

Reglas de publicador

A diferencia de una regla de certificados de restricción de software, no es necesario obtener un certificado para utilizar una regla editor porque los detalles de la firma digital son extraídos del archivo de aplicación de referencia.

Si un archivo no tiene firma digital, no se puede restringir ni permitir mediante reglas de AppLocker editor.

Permiten **más flexibilidad** que las reglas hash porque **se puede especificar no sólo una versión específica de un archivo, también todas las versiones futuras** de ese archivo.



Reglas hash

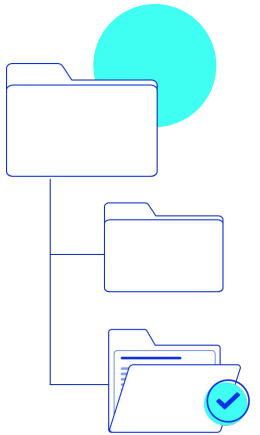
Permiten identificar un archivo binario específico que no está firmado digitalmente, podemos utilizar la identificación por hash.

Podemos utilizar el asistente de creación de reglas para automatizar la creación de hash de archivo para todos los archivos en una ubicación específica.

Reglas de ruta

Las reglas de ruta permiten **definir rutas en las cuales se van a poder ejecutar programas** (tanto para un archivo específico como para todo un directorio).

Debemos tener en consideración que los usuarios con permisos de modificación sobre los archivos y/o directorios, pueden afectar el comportamiento de la política. Por ejemplo, reemplazando un archivo que tiene permisos para ser ejecutado, por otro archivo totalmente diferente.

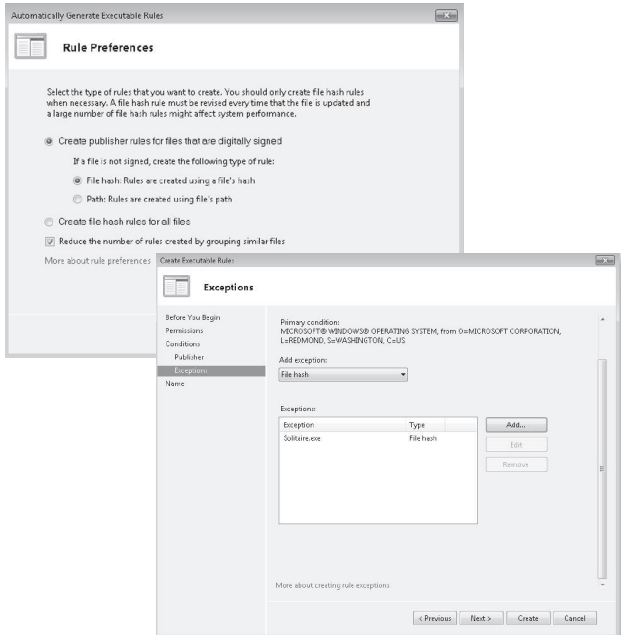


Configurar excepciones

Permiten a aplicaciones específicas estar exentas de reglas más generales.

Se puede utilizar cualquier método para especificar una excepción, y el método que elija no dependerá del tipo de regla que se está creando.

Podemos crear excepciones para las reglas de bloqueo, así como reglas de permiso.



Auditoría

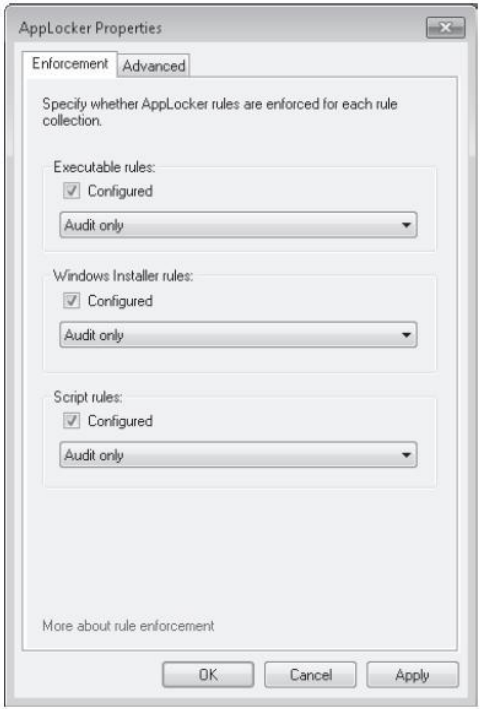
Esto permite **comprobar qué aplicaciones son afectadas por AppLocker** sin llegar a bloquear la ejecución. Se puede configurar AppLocker para auditar normas en lugar de hacerlas cumplir.

Los eventos de auditoría de AppLocker se encuentran en **Visor de Eventos \aplicaciones** y **servicios \Microsoft \Windows.**

Los eventos contienen la siguiente información:

- El nombre de la regla.
- El SID del usuario atacado o grupo.
- Archivo afectado por qué regla y trayectoria.
- Si el archivo está bloqueado o permitido.
- El tipo de regla (hash editor, ruta de acceso o archivo).

Auditoría


AppLocker Properties
Enforcement
Advanced
Specify whether AppLocker rules are enforced for each rule collection.
Executable rules:
Configured
Audit only
Windows Installer rules:
Configured
Audit only
Script rules:
Configured
Audit only
More about rule enforcement
OK
Cancel
Apply

¡Sigamos trabajando!