AppLocker - Walkthrough

- Get-AppLockerFileInformation

Get-AppLockerFileInformation

Get-AppLockerFileInformation

- Reference

Module:

AppLocker

Gets the file information necessary to create AppLocker rules from a list of files or an event log.

Syntax

PowerShell

```
Get-AppLockerFileInformation
   [[-Path] <System.Collections.Generic.List`1[System.String]>]
   [<CommonParameters>]
```

PowerShell

```
Get-AppLockerFileInformation
   [[-Packages]
<System.Collections.Generic.List`1[Microsoft.Windows.Appx.PackageManager.Commands.AppxPackage]
>]
   [<CommonParameters>]
```

PowerShell

```
Get-AppLockerFileInformation
   -Directory <String>
   [-FileType
<System.Collections.Generic.List`1[Microsoft.Security.ApplicationId.PolicyManagement.PolicyMod
el.AppLockerFileType]>]
   [-Recurse]
```

```
    [<CommonParameters>]
```

PowerShell

```
Get-AppLockerFileInformation
   [-EventLog]
   [-LogPath <String>]
   [-EventType
<System.Collections.Generic.List`1[Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets.A
ppLockerEventType]>]
   [-Statistics]
   [<CommonParameters>]
```

Description

The **Get-AppLockerFileInformation** cmdlet gets the AppLocker file information from a list of files or an event log. File information includes the publisher information, file hash, and file path.

The file information from an event log may not contain all of the publisher information, file hash, and file path fields. Files that are not signed will not have any publisher information.

Examples

Example 1: Get file information for .exe files and scripts

PowerShell

```
PS C:\> Get-AppLockerFileInformation -Directory C:\Windows\system32\ -Recurse -FileType exe,
script
```

This example gets the file information for all the .exe files and scripts under %windir%\system32.

Example 2: Get file information for a file

PowerShell

```
PS C:\> Get-AppLockerFileInformation -Path "C:\Program Files (x86)\Internet
Explorer\iexplore.exe" | Format-List
Path      : %PROGRAMFILES%\INTERNET EXPLORER\IEXPLORE.EXE
Publisher : CN=WINDOWS MAIN BUILD LAB ACCOUNT\WINDOWS® INTERNET
EXPLORER\IEXPLORE.EXE,10.0.8421.0
Hash      : SHA256 0x5F374C2DD91A6F9E9E96F149EE221EC0454649F50E1AF6D3DAEFB849FB7C551C
AppX      : False


PS C:\> Get-AppLockerFileInformation -Path "C:\Program Files\Internet Explorer\iexplore.exe" |
Format-List
Path      : %PROGRAMFILES%\INTERNET EXPLORER\IEXPLORE.EXE
Publisher : CN=WINDOWS MAIN BUILD LAB ACCOUNT\WINDOWS® INTERNET
EXPLORER\IEXPLORE.EXE,10.0.8421.0
Hash      : SHA256 0x5F374C2DD91A6F9E9E96F149EE221EC0454649F50E1AF6D3DAEFB849FB7C551C
AppX      : False
```

This example gets the file information for the file specified by the path.

Example 3: Get file information for all packaged applications for all users

PowerShell

```
PS C:\> Get-AppXPackage -AllUsers | Get-AppLockerFileInformation
Path      : windows.immersivecontrolpanel_6.2.0.0_neutral_neutral_cw5n1h2txyewy.appx
Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington,
            C=US\windows.immersivecontrolpanel\APPX,6.2.0.0
Hash      :
AppX      : True

Path      : windows.RemoteDesktop_1.0.0.0_neutral_neutral_cw5n1h2txyewy.appx
Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington,
            C=US\windows.RemoteDesktop\APPX,1.0.0.0
Hash      :
AppX      : True

Path      : WinStore_1.0.0.0_neutral_neutral_cw5n1h2txyewy.appx
Publisher : CN=Microsoft Windows, O=Microsoft Corporation, L=Redmond, S=Washington,
```

```
C=US\WinStore\APPX,1.0.0.0
Hash      :
AppX      : True
```

This example outputs the file information for all the packaged applications installed on this computer for all users.

Example 4: Get file information for Audited events

PowerShell

```
PS C:\> Get-AppLockerFileInformation -EventLog -EventType Audited
```

This example outputs the file information for all the Audited events in the local event log. Audited events correspond to the Warning event in the AppLocker audit log.

Example 5: Get statistics for Allowed events

PowerShell

```
PS C:\> Get-AppLockerFileInformation -EventLog -EventType Allow -Statistics
```

This example displays statistics for all the Allowed events in the local event log. For each file in the event log, the cmdlet will sum the number of times the event type occurred.

Example 6: Create an AppLocker policy

PowerShell

```
PS C:\> Get-AppLockerFileInformation -EventLog -EventType Audited | New-AppLockerPolicy -
RuleType Publisher, Hash, Path -User Everyone -Optimize | Set-AppLockerPolicy -LDAP
LDAP://TestGPO
```

This example creates a new AppLocker policy from the warning events in the local event log and sets the policy of a test Group Policy Object (GPO).

Parameters

-Directory

Specifies the directory that contains the files for which to get the file information. If all subfolders and files in the specified directory are to be searched, then include the *Recurse* parameter

Type:	String
Position:	Named
Default value:	None
Required:	True
Accept pipeline input:	False
Accept wildcard characters:	False

-EventLog

Specifies that the file information is retrieved from the event log.

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	True
Accept pipeline input:	False
Accept wildcard characters:	False

-EventType

Specifies the event type by which to filter the events. The acceptable values for this parameter are: Allowed, Denied, or Audited. The event types correspond to the Informational, Error, and Warning level events in the AppLocker event logs.

Type:	List<T>[Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets.AppLockerEventType]
Accepted values:	Allowed, Denied, Audited
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False

-FileType

Specifies the generic file type for which to search. All files having the appropriate file name extension will be included. The acceptable values for this parameter are:

- Exe
- Dll
- WindowsInstaller
- Script
- Appx.

Type:	List<T>[Microsoft.Security.ApplicationId.PolicyManagement.PolicyModel.AppLockerFileType]
Accepted values:	Exe, Dll, WindowsInstaller, Script, Appx
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False

-LogPath

Specifies the log name or file path of the event log where the AppLocker events are located. By default, if this parameter is not specified, the local Microsoft-Windows-AppLocker/EXE and DLL channel is used.

Type:	String
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False

-Packages

Specifies a list of installed packaged applications, from which the file information is retrieved.

Type:	List<T>[Microsoft.Windows.Appx.PackageManager.Commands.AppxPackage]
Position:	0
Default value:	None
Required:	False
Accept pipeline input:	True
Accept wildcard characters:	False

-Path

Specifies a list of paths to the files from which the file information is retrieved. Supports regular expressions.

Type:	List<T>[String]
Position:	0
Default value:	None
Required:	False
Accept pipeline input:	True
Accept wildcard characters:	False

-Recurse

Specifies that all files and folders in the specified directory will be searched.

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False

-Statistics

Specifies the statistics to retrieve on the files included in the event log. Calculates a simple sum of the number of times a file is included in the event log based on specified parameters.

Type:	SwitchParameter
Position:	Named
Default value:	None

Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False

Inputs

None

Outputs

Microsoft.Security.ApplicationId.PolicyManagement.PolicyModel.FileInformation

String

Related Links

- Get-AppLockerPolicy
- New-AppLockerPolicy
- Set-AppLockerPolicy
- Test-AppLockerPolicy