



Windows PowerShell Get-Help on Cmdlet 'Get-AppLockerFileInformation'

PS:\>Get-HELP Get-AppLockerFileInformation -Full

NAME

Get-AppLockerFileInformation

SYNOPSIS

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

SYNTAX

Get-AppLockerFileInformation -Directory <String> [-FileType {Exe | Dll | WindowsInstaller | Script | Appx}] [-Recurse]
[<CommonParameters>]

Get-AppLockerFileInformation -EventLog [-EventType {Allowed | Denied | Audited}] [-LogPath <String>] [-Statistics]
[<CommonParameters>]

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

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

PARAMETERS

-Directory <String>

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

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-EventLog [<SwitchParameter>]

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

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

<System.Collections.Generic.List`1[Microsoft.Security.ApplicationId.PolicyManagement.Cmdlets.AppLockerEventType]>

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.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-FileType

<System.Collections.Generic.List`1[Microsoft.Security.ApplicationId.PolicyManagement.PolicyModel.AppLockerFileType]>

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.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-LogPath <String>

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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

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

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

Required? false

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName, ByValue)

Accept wildcard characters? false

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

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

Required? false

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName, ByValue)

Accept wildcard characters? false

-Recurse [<SwitchParameter>]

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

Required? false

Position? named
Default value False
Accept pipeline input? False
Accept wildcard characters? false

-Statistics [<SwitchParameter>]

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.

Required? false
Position? named
Default value False
Accept pipeline input? False
Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable, and OutVariable. For more information, see about_CommonParameters (<https://go.microsoft.com/fwlink/?LinkID=113216>).

INPUTS

None

OUTPUTS

Microsoft.Security.ApplicationId.PolicyManagement.PolicyModel.FileInformation

System.String

NOTES

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

```
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 -----

```
PS C:\> Get-AppLockerFileInformation -Path "C:\Program Files (x86)\Internet Explorer\iexplore.exe" | Format-List
```

```
Path      : %PROGRAMFILES%\INTERNET EXPLORER\EXPLORE.EXE
```

```
          Publisher    :   CN=WINDOWS   MAIN   BUILD   LAB   ACCOUNT\WINDOWSr   INTERNET
```

```
EXPLORE\EXPLORE.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\EXPLORE.EXE
```

```
          Publisher    :   CN=WINDOWS   MAIN   BUILD   LAB   ACCOUNT\WINDOWSr   INTERNET
```

```
EXPLORE\EXPLORE.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

```
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 -----

```
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 -----

```
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 -----

```
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).

RELATED LINKS

Online

Version:

https://learn.microsoft.com/powershell/module/applocker/get-applockerfileinformation?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

[Get-AppLockerPolicy](#)

[New-AppLockerPolicy](#)

[Set-AppLockerPolicy](#)

[Test-AppLockerPolicy](#)