



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

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

NAME

Get-AppLockerPolicy

SYNOPSIS

Gets the local, the effective, or a domain AppLocker policy.

SYNTAX

Get-AppLockerPolicy -Domain -Ldap <String> [-Xml] [<CommonParameters>]

Get-AppLockerPolicy -Effective [-Xml] [<CommonParameters>]

Get-AppLockerPolicy -Local [-Xml] [<CommonParameters>]

DESCRIPTION

The Get-AppLockerPolicy cmdlet retrieves the AppLocker policy from the local Group Policy Object (GPO), a specified GPO, or the GP-deployed effective policy on the computer.

By default, the output is an AppLockerPolicy object. If the Xml parameter is used, then the output will be the AppLocker policy as an XML-formatted string.

Note that the Get-AppLockerPolicy cmdlet only functions with policies deployed via GP. It does not have any knowledge of the AppLocker CSP, so it will return

incorrect data if the policy in place has been applied via the CSP.

PARAMETERS

-Domain [<SwitchParameter>]

Gets the AppLocker policy from the GPO specified by the path given in the Ldap parameter.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Effective [<SwitchParameter>]

Gets the effective AppLocker policy on the local computer. The effective policy is the merge of the local AppLocker policy and any applied AppLocker domain policies on the local computer.

Required? true

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Ldap <String>

Specifies the LDAP path of the GPO and must specify a unique GPO.

Required? true

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

-Local [<SwitchParameter>]

Gets the AppLocker policy from the local GPO.

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

-Xml [<SwitchParameter>]

Specifies that the AppLocker policy be output as an XML-formatted string.

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.AppLockerPolicy
AppLockerPolicy

System.String
```

NOTES

----- Example 1: Get an AppLocker policy -----

```
PS C:\> Get-AppLockerPolicy -Local

Version RuleCollections RuleCollectionTypes
-----
1 {} {}
```

This example gets the local AppLocker policy as an AppLockerPolicy object.

----- Example 2: Get the AppLocker policy for a GPO -----

```
PS C:\> Get-AppLockerPolicy -Domain -LDAP "LDAP://DC13.Contoso.com/CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=Contoso,DC=com"
```

This example gets the AppLocker policy of the unique GPO specified by the LDAP path as an AppLockerPolicy object.

----- Example 3: Get the effective policy -----

```
PS C:\> Get-AppLockerPolicy -Effective -Xml | Set-Content ('c:\temp\curr.xml')
```

This example gets the effective policy on the computer, and then sends it in XML-format to the specified file on an

existing path.

----- Example 4: Get and test an AppLocker policy -----

```
PS C:\> Get-AppLockerPolicy -Local | Test-AppLockerPolicy -Path C:\Windows\System32\*.exe -User Everyone
```

This example gets the local AppLocker policy on the computer, and then tests the policy using the Test-AppLockerPolicy cmdlet to test whether the .exe files in

C:\Windows\System32 will be allowed to run by the Everyone group.

RELATED LINKS

Online

Version:

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

Get-AppLockerFileInformation

New-AppLockerPolicy

Set-AppLockerPolicy

Test-AppLockerPolicy