



python



PowerShell

FPDF Library  
PDF generator

*Full credit is given to the above companies including the OS that this PDF file was generated!*

### **PowerShell Get-Help on command 'Remove-EventLog'**

**PS C:\Users\wahid> Get-Help Remove-EventLog**

#### NAME

Remove-EventLog

#### SYNOPSIS

Deletes an event log or unregisters an event source.

#### SYNTAX

```
Remove-EventLog [-LogName] <System.String[]> [[-ComputerName]
<System.String[]>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

```
Remove-EventLog [[-ComputerName] <System.String[]>] [-Source
<System.String[]>] [-Confirm] [-WhatIf] [<CommonParameters>]
```

#### DESCRIPTION

The `Remove-EventLog` cmdlet deletes an event log file from a local or remote computer and unregisters all its event sources for the log. You can also use this cmdlet to unregister event sources without deleting any event logs.

classic event logs. To get events from logs that use the Windows Event Log technology in Windows Vista and later versions of the Windows operating system, use Get-WinEvent.

> [!WARNING] > This cmdlet can delete operating system event logs, which might cause application failures and > unexpected system behavior.

## PARAMETERS

**-ComputerName <System.String[]>**

Specifies a remote computer. The default is the local computer.

Type the NetBIOS name, an IP address, or a fully qualified domain name of a remote computer. To specify the local computer, type the computer name, a dot ( . ), or localhost.

This parameter does not rely on Windows PowerShell remoting. You can use the ComputerName parameter of `Remove-EventLog` even if your computer is not configured to run remote commands.

**-LogName <System.String[]>**

Specifies the event logs. Enter the log name of one or more event logs, separated by commas. The log name is the value of the Log property, not the LogDisplayName , Wildcard characters are not permitted. This parameter is required.

**-Source <System.String[]>**

Specifies the event sources that this cmdlet unregisters. Enter the source names, not the executable name, separated by commas.

**-Confirm <System.Management.Automation.SwitchParameter>**

Prompts you for confirmation before running the cmdlet.

-WhatIf <System.Management.Automation.SwitchParameter>

Shows what would happen if the cmdlet runs. The cmdlet is not run.

<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>).

---- Example 1: Remove an event log from the local computer ----

```
Remove-EventLog -LogName "MyLog"
```

This command deletes the MyLog event log from the local computer and unregisters its event sources.

---- Example 2: Remove an event log from several computers ----

```
Remove-EventLog -LogName "MyLog", "TestLog" -ComputerName "Server01",  
"Server02", "localhost"
```

This command deletes the MyLog and TestLog event logs from the local computer and the Server01 and Server02 remote computers. The command also unregisters the event sources for these logs.

----- Example 3: Delete an event source -----

```
Remove-EventLog -Source "MyApp"
```

This command deletes the MyApp event source from the logs on the local computer. When the command finishes, the MyApp program cannot write to any event logs.

---- Example 4: Remove an event log and confirm the action ----

Get-EventLog -List

Max(K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	22,923	Application
15,168	0	OverwriteAsNeeded	53	DFS Replication
15,168	7	OverwriteOlder	0	Hardware Events
512	7	OverwriteOlder	0	Internet Explorer
20,480	0	OverwriteAsNeeded	0	Key Management Service
30,016	0	OverwriteAsNeeded	50,060	Security
15,168	0	OverwriteAsNeeded	27,592	System
15,360	0	OverwriteAsNeeded	18,355	Windows PowerShell
15,168	7	OverwriteAsNeeded	12	ZapLog

```
Remove-EventLog -LogName "ZapLog"
```

```
Get-EventLog -List
```

Max(K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	22,923	Application
15,168	0	OverwriteAsNeeded	53	DFS Replication
15,168	7	OverwriteOlder	0	Hardware Events
512	7	OverwriteOlder	0	Internet Explorer
20,480	0	OverwriteAsNeeded	0	Key Management Service
30,016	0	OverwriteAsNeeded	50,060	Security
15,168	0	OverwriteAsNeeded	27,592	System
15,360	0	OverwriteAsNeeded	18,355	Windows PowerShell

The first command lists the event logs on the local computer.

The second command deletes the ZapLog event log.

The third command lists the event logs again. The ZapLog event log no longer appears in the list.

--- Example 5: Remove an event source and confirm the action ---

```
Get-WmiObject win32_nventlogfile -Filter "logfilename='TestLog'" | foreach  
{$_sources}
```

MyApp

TestApp

```
Remove-Eventlog -Source "MyApp"
```

```
Get-WmiObject win32_nventlogfile -Filter "logfilename='TestLog'" | foreach  
{$_sources}
```

TestApp

These commands use the `Get-WmiObject` cmdlet to list the event sources on the local computer. You can use these commands to verify the success of a command or to delete an event source.

The first command gets the event sources of the TestLog event log on the local computer. MyApp is one of the sources.

The second command uses the Source parameter of `Remove-EventLog` to delete the MyApp event source.

The third command is identical to the first. It shows that the MyApp event source was deleted.

## REMARKS

To see the examples, type: "get-help Remove-EventLog -examples".

For more information, type: "get-help Remove-EventLog -detailed".

For technical information, type: "get-help Remove-EventLog -full".

For online help, type: "get-help Remove-EventLog -online"