wevtutil

Article • 02/03/2023

Enables you to retrieve information about event logs and publishers. You can also use this command to install and uninstall event manifests, to run queries, and to export, archive, and clear logs.

Syntax

```
wevtutil [{el | enum-logs}] [{gl | get-log} <Logname> [/f:<Format>]]
[{sl | set-log} <Logname> [/e:<Enabled>] [/i:<Isolation>] [/lfn:<Logpath>] [/rt:<Retention>] [/ab:
<Auto>] [/ms:<MaxSize>] [/l:<Level>] [/k:<Keywords>] [/ca:<Channel>] [/c:<Config>]]
[{ep | enum-publishers}]
[{gp | get-publisher} <Publishername> [/ge:<Metadata>] [/gm:<Message>] [/f:<Format>]]
[{im | install-manifest} <Manifest>] [/rf:<Path>] [/mf:<Path>] [/pf:<Path>]
[{um | uninstall-manifest} <Manifest>] [{qe | query-events} <Path> [/lf:<Logfile>] [/sq:<Structquery>]
[/q:<Query>] [/bm:<Bookmark>] [/sbm:<Savebm>] [/rd:<Direction>] [/f:<Format>] [/l:<Locale>] [/c:
<Count>] [/e:<Element>]]
[{gli | get-loginfo} <Logname> [/lf:<Logfile>]]
[{epl | export-log} <Path> <Exportfile> [/lf:<Logfile>] [/sq:<Structquery>] [/q:<Query>] [/ow:
<Overwrite>]]
[{al | archive-log} <Logpath> [/l:<Locale>]]
[{cl | clear-log} <Logname> [/bu:<Backup>]] [/r:<Remote>] [/u:<Username>] [/p:<Password>] [/a:<Auth>]
[/uni:<Unicode>]
```

Parameters

Expand table

Parameter	Description
{el | enum-logs}	Displays the names of all logs.
{gl | get-log} <Logname> [/f:<Format>]	Displays configuration information for the specified log, which includes whether the log is enabled or not, the current maximum size limit of the log, and the path to the file where the log is stored.
{sl | set-log} <Logname> [/e:<Enabled>] [/i:<Isolation>] [/lfn:<Logpath>] [/rt:<Retention>] [/ab:<Auto>] [/ms:<MaxSize>] [/l:<Level>] [/k:<Keywords>] [/ca:<Channel>] [/c:<Config>]	Modifies the configuration of the specified log.
{ep | enum-publishers}	Displays the event publishers on the local computer.
{gp | get-publisher} <Publishername> [/ge:<Metadata>] [/gm:<Message>] [/f:<Format>]]	Displays the configuration information for the specified event publisher.
{im | install-manifest} <Manifest> [/{rf | resourceFilePath}:value] [/{mf | messageFilePath}:value] [/{pf | parameterFilePath}:value]	Installs event publishers and logs from a manifest. For more information about event manifests and using this parameter, see the Windows Event Log SDK at the Microsoft Developers Network (MSDN) Web site (https://msdn.microsoft.com). The **value** is the full path to the mentioned file.

Parameter	Description
{um | uninstall-manifest} <Manifest>	Uninstalls all publishers and logs from a manifest. For more information about event manifests and using this parameter, see the Windows Event Log SDK at the Microsoft Developers Network (MSDN) Web site (https://msdn.microsoft.com).
{qe | query-events} <Path> [/lf:<Logfile>] [/sq:<Structquery>] [/q:<Query>] [/bm:<Bookmark>] [/sbm:<Savebm>] [/rd:<Direction>] [/f:<Format>] [/l:<Locale>] [/c:<Count>] [/e:<Element>]	Reads events from an event log, from a log file, or using a structured query. By default, you provide a log name for <Path>. However, if you use the **/lf** option, then <Path> must be a path to a log file. If you use the **/sq** parameter, <Path> must be a path to a file that contains a structured query.
{gli | get-loginfo} <Logname> [/lf:<Logfile>]	Displays status information about an event log or log file. If the **/lf** option is used, <Logname> is a path to a log file. You can run **wevtutil el** to obtain a list of log names.
{epl | export-log} <Path> <Exportfile> [/lf:<Logfile>] [/sq:<Structquery>] [/q:<Query>] [/ow:<Overwrite>]	Exports events from an event log, from a log file, or using a structured query to the specified file. By default, you provide a log name for <Path>. However, if you use the **/lf** option, then <Path> must be a path to a log file. If you use the **/sq** option, <Path> must be a path to a file that contains a structured query. <Exportfile> is a path to the file where the exported events will be stored.
{al | archive-log} <Logpath> [/l:<Locale>]	Archives the specified log file in a self-contained format. A subdirectory with the name of the locale is created and all locale-specific information is saved in that subdirectory. After the directory and log file are created by running **wevtutil al**, events in the file can be read whether the publisher is installed or not.
{cl | clear-log} <Logname> [/bu:<Backup>]	Clears events from the specified event log. The **/bu** option can be used to back up the cleared events.

Options

Expand table

Option	Description
/f:<Format>	Specifies that the output should be either XML or text format. If <Format> is XML, the output is displayed in XML format. If <Format> is Text, the output is displayed without XML tags. The default is Text.
/e:<Enabled>	Enables or disables a log. <Enabled> can be true or false.
/i:<Isolation>	Sets the log isolation mode. <Isolation> can be system, application or custom. The isolation mode of a log determines whether a log shares a session with other logs in the same isolation class. If you specify system isolation, the target log will share at least write permissions with the System log. If you specify application isolation, the target log will share at least write permissions with the Application log. If you specify custom isolation, you must also provide a security descriptor by using the **/ca** option.
/lfn:<Logpath>	Defines the log file name. <Logpath> is a full path to the file where the Event Log service stores events for this log.
/rt:<Retention>	Sets the log retention mode. <Retention> can be true or false. The log retention mode determines the behavior of the Event Log service when a log reaches its maximum size. If an event log reaches its maximum size and the log retention mode is true, existing events are retained, and incoming events are discarded. If the log retention mode is false, incoming events overwrite the oldest events in the log.

Option	Description
/ab:<Auto>	Specifies the log auto-backup policy. <Auto> can be true or false. If this value is true, the log will be backed up automatically when it reaches the maximum size. If this value is true, the retention (specified with the **/rt** option) must also be set to true.
/ms:<MaxSize>	Sets the maximum size of the log in bytes. The minimum log size is 1048576 bytes (1024KB) and log files are always multiples of 64KB, so the value you enter will be rounded off accordingly.
/l:<Level>	Defines the level filter of the log. <Level> can be any valid level value. This option is only applicable to logs with a dedicated session. You can remove a level filter by setting <Level> to 0.
/k:<Keywords>	Specifies the keywords filter of the log. <Keywords> can be any valid 64-bit keyword mask. This option is only applicable to logs with a dedicated session.
/ca:<Channel>	Sets the access permission for an event log. <Channel> is a security descriptor that uses the Security Descriptor Definition Language (SDDL). For more information about SDDL format, see the Microsoft Developers Network (MSDN) Web site (https://msdn.microsoft.com).
/c:<Config>	Specifies the path to a configuration file. This option will cause log properties to be read from the configuration file defined in <Config>. If you use this option, you must not specify a <Logname> parameter. The log name will be read from the configuration file.
/ge:<Metadata>	Gets metadata information for events that can be raised by this publisher. <Metadata> can be true or false.
/gm:<Message>	Displays the actual message instead of the numeric message ID. <Message> can be true or false.
/lf:<Logfile>	Specifies that the events should be read from a log or from a log file. <Logfile> can be true or false. If true, the parameter to the command is the path to a log file.
/sq:<Structquery>	Specifies that events should be obtained with a structured query. <Structquery> can be true or false. If true, <Path> is the path to a file that contains a structured query.
/q:<Query>	Defines the XPath query to filter the events that are read or exported. If this option is not specified, all events will be returned or exported. This option is not available when **/sq** is true.
/bm:<Bookmark>	Specifies the path to a file that contains a bookmark from a previous query.
/sbm:<Savebm>	Specifies the path to a file that is used to save a bookmark of this query. The file name extension should be .xml.
/rd:<Direction>	Specifies the direction in which events are read. <Direction> can be true or false. If true, the most recent events are returned first.
/l:<Locale>	Defines a locale string that is used to print event text in a specific locale. Only available when printing events in text format using the **/f** option.
/c:<Count>	Sets the maximum number of events to read.
/e:<Element>	Includes a root element when displaying events in XML. <Element> is the string that you want within the root element. For example, **/e:root** would result in XML that contains the root element pair <root>.
/ow:<Overwrite>	Specifies that the export file should be overwritten. <Overwrite> can be true or false. If true, and the export file specified in <Exportfile> already exists, it will be overwritten without confirmation.
/bu:<Backup>	Specifies the path to a file where the cleared events will be stored. Include the .evtx extension in the name of the backup file.

Option	Description
/r:<Remote>	Runs the command on a remote computer. <Remote> is the name of the remote computer. The **im** and **um** parameters do not support remote operation.
/u: <Username>	Specifies a different user to log on to a remote computer. <Username> is a user name in the form domain\user or user. This option is only applicable when the **/r** option is specified.
/p:<Password>	Specifies the password for the user. If the **/u** option is used and this option is not specified or <Password> is *, the user will be prompted to enter a password. This option is only applicable when the **/u** option is specified.
/a:<Auth>	Defines the authentication type for connecting to a remote computer. <Auth> can be Default, Negotiate, Kerberos or NTLM. The default is Negotiate.
/uni: <Unicode>	Displays the output in Unicode. <Unicode> can be true or false. If <Unicode> is true then the output is in Unicode.

Remarks

- Using a configuration file with the sl parameter

  The configuration file is an XML file with the same format as the output of wevtutil gl <Logname> /f:xml. To shows the format of a configuration file that enables retention, enables autobackup, and sets the maximum log size on the Application log:

```
<?xml version=1.0 encoding=UTF-8?>
<channel name=Application isolation=Application
xmlns=https://schemas.microsoft.com/win/2004/08/events>
<logging>
<retention>true</retention>
<autoBackup>true</autoBackup>
<maxSize>9000000</maxSize>
</logging>
<publishing>
</publishing>
</channel>
```

Examples

List the names of all logs:

```
wevtutil el
```

Display configuration information about the System log on the local computer in XML format:

```
wevtutil gl System /f:xml
```

Use a configuration file to set event log attributes (see Remarks for an example of a configuration file):

```
wevtutil sl /c:config.xml
```

Display information about the Microsoft-Windows-Eventlog event publisher, including metadata about the events that the publisher can raise:

```
wevtutil gp Microsoft-Windows-Eventlog /ge:true
```

Install publishers and logs from the myManifest.xml manifest file:

```
wevtutil im myManifest.xml
```

Uninstall publishers and logs from the myManifest.xml manifest file:

```
wevtutil um myManifest.xml
```

Display the three most recent events from the Application log in textual format:

```
wevtutil qe Application /c:3 /rd:true /f:text
```

Display the status of the Application log:

```
wevtutil gli Application
```

Export events from System log to C:\backup\system0506.evtx:

```
wevtutil epl System C:\backup\system0506.evtx
```

Clear all of the events from the Application log after saving them to C:\admin\backups\a10306.evtx:

```
wevtutil cl Application /bu:C:\admin\backups\a10306.evtx
```

Archive the specified (*.evtx*) log file in a self-contained format. A subdirectory (LocaleMetaData) is created and all locale-specific information is saved in that subdirectory:

```
wevtutil archive-log "C:\backup\Application.evtx" /locale:en-us
```

Related links

- Command-Line Syntax Key