[1. EventLogDemo 2](#_Toc418156099)

[1-1. Description 2](#_Toc418156100)

[1-2. Log Record存续时间 2](#_Toc418156101)

[1-3. Demo 2](#_Toc418156102)

# EventLogDemo

## Description

EventLog lets you access or customize Windows event logs, which record information about important software or hardware events. Using EventLog, you can read from existing logs, write entries to logs, create or delete event sources, delete logs, and respond to log entries. You can also create new logs when creating an event source.

In addition to providing access to individual event logs and their entries, the EventLog class lets you access the collection of all event logs. You can use the static members of EventLog to delete logs, get log lists, create or delete a source, or determine if a computer already contains a particular source.





There are three default event logs: Application, System, and Security. A Security log is read-only.

* Application: Used to track errors or notifications from any application
* Security: Used to track security related problems, used by the OS
* System: Used to track OS events

## Log Record存续时间

One of the potential problems with event logs is that they are automatically overwritten when the maximum set size is reached or after a certain number of days (typically seven days). This means application logs cannot be used to log critical information that need to be retained for a long period of time. Instead, they should be used to track information that is valuable only for a short period of time. For example, the event logs can be used to review errors and diagnose strange behavior immediately after it occurs, say within a couple of days or so.

## Demo

在 EventSource 可以显示的创建，但不显示创建应该也没问题，分别参照Demo1和Demo2

只所以需要显示的创建，是因为只有在CreateEventSource方法中才可以同时创建一个新的log文件。如果不需要新的log文件，完全可以不用创建eventsource，只需在eventlog对象中设置source属性即可，创建时会默认创建在Application这个log下。





