Event Log Crash Browser

by

Software Verify

Software Verify

Troubleshoot your software

Event Log Crash Browser

Easily find crash information in the Windows Event Log.

by Software Verify Limited

Welcome to the Event Log Crash Browser software tool.

Event Log Crash Browser is a software tool that allows you to easily identify crashes in the Windows Event Log and then launch related tools to turn the crash information into symbols, filenames and line numbers you can use for debugging.

We hope you will find this document useful.

Event Log Crash Browser Help

Printed: June 2024 in United Kingdom.

Table of Contents

Foreword 1

Part I How to get Event Log Crash Browser 2

Part II What does Event Log Crash Browser do? 4

Part III Menu 6

1 File 7
2 Settings 7
3 Software Updates 8
4 Help 11

Part IV The user interface 13

Part V SettingsDialog 19

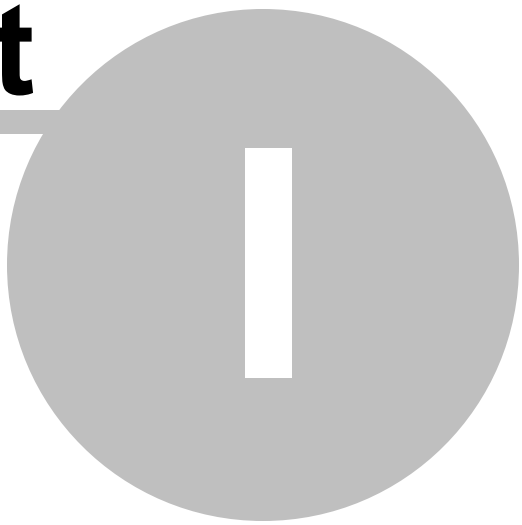
1 Events 20
2 Behaviour 21

Part VI Command Line 24

Part VII Crash Logs 26

Index 0

Part



1 How to get Event Log Crash Browser

Event Log Crash Browser is free for commercial use. Event Log Crash Browser can be downloaded for Software Verify's website at https://www.softwareverify.com/product/event-log-crash-browser/.

This help manual is available in Compiled HTML Help (Windows Help files), PDF, and online.

Windows Help	https://www.softwareverify.com/documentation/chm/eventLogCrashBrowser.chm
PDF	https://www.softwareverify.com/documentation/pdfs/eventLogCrashBrowser.pdf
Online	https://www.softwareverify.com/documentation/html/eventLogCrashBrowser/index.html

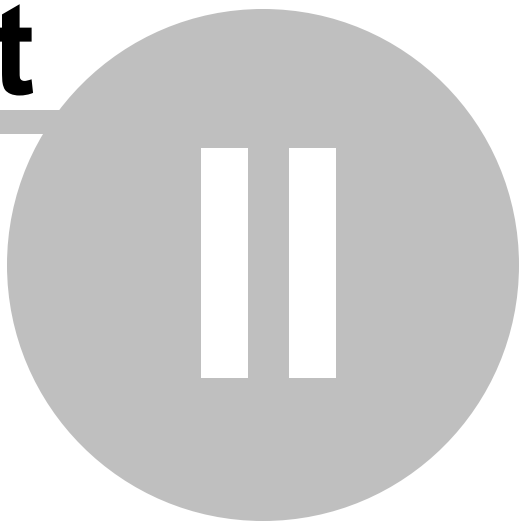
Contact Software Verify at:

Software Verify Limited
Suffolk Business Park
Eldo House
Kempson Way
Bury Saint Edmunds
IP32 7AR
United Kingdom

email sales@softwareverify.com
web https://www.softwareverify.com
blog https://www.softwareverify.com/blog
twitter http://twitter.com/softwareverify

Visit our blog to read our articles on debugging techniques and tools.
Follow us on twitter to keep track of the latest software tools and updates.

Part

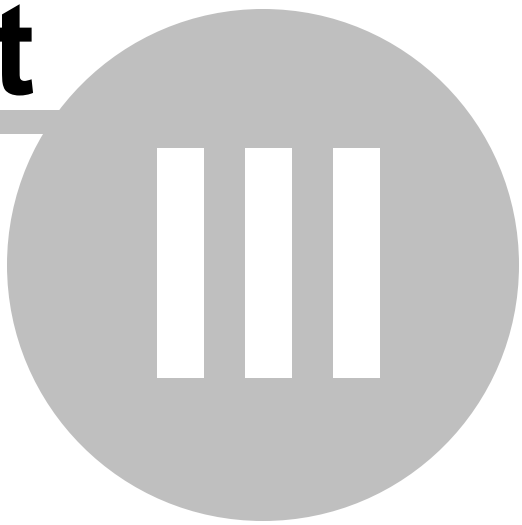


2 What does Event Log Crash Browser do?

Event Log Crash Browser allows you to easily identify crash information in the Windows Event Log.

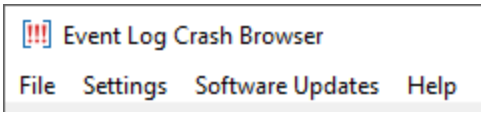
Once the crash information has been identified you can launch various tools to convert the crash address into symbols, filenames and line numbers that you can use for debugging.

Part



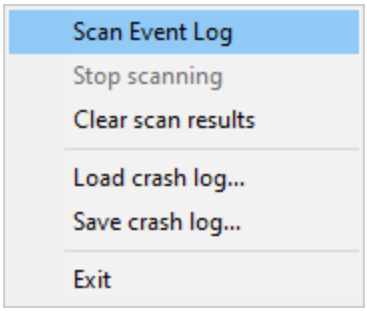
3 Menu

The main menu contains four menus, File, Settings, Software Updates and Help.



3.1 File

The File menu controls the scanning and display of event log crash information.



File menu › **Scan Event Log** › scans the event log for crashes. Any crashes found are shown on the user interface.

File menu › **Stop scanning** › stops scanning the event log for crashes.

File menu › **Clear scan results** › the user interface contents are reset to show no crashes.

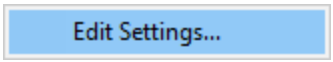
File menu › **Load crash log...** › crash data is loaded from a log file.

File menu › **Save crash log...** › crash data is saved to a log file.

File menu › **Exit** › closes Event Log Crash Browser.

3.2 Settings

The settings menu provides access to the settings.

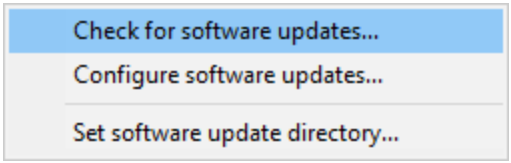


Settings menu › **Edit Settings...** › displays the settings dialog.

3.3 Software Updates

The Software Updates menu controls how often software updates are downloaded.

If you've been notified of a new software release to Event Log Crash Browser or just want to see if there's a new version, this feature makes it easy to update.

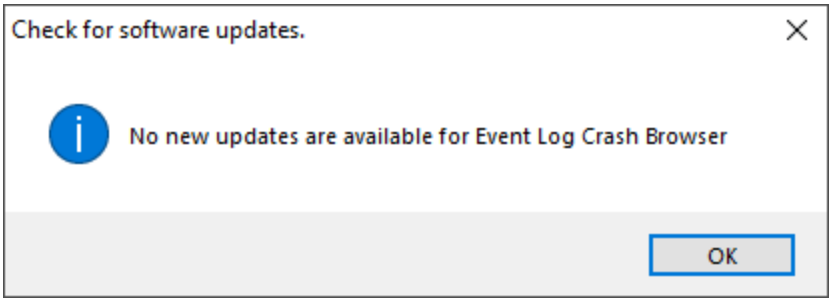


Software Updates menu › **Check for software updates** › checks for updates and shows the software update dialog if any exist

An internet connection is needed to be able to make contact with our servers.

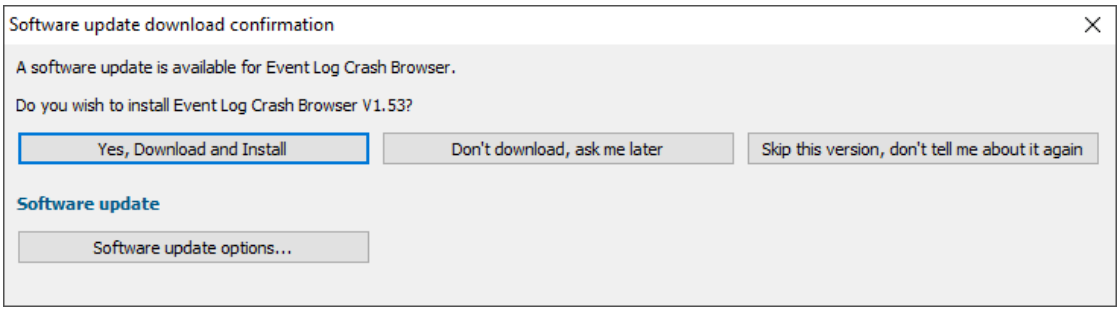
Before updating the software, close the help manual, and end any active session by closing target programs.

If no updates are available, you'll just see this message:

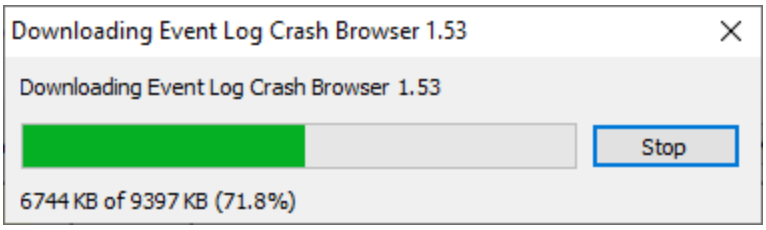


Software Update dialog

If a software update is available for Event Log Crash Browser you'll see the software update dialog.



- **Download and install** › downloads the update, showing progress



  Once the update has downloaded, Event Log Crash Browser will close, run the installer, and restart.

  You can stop the download at any time, if necessary.

- **Don't download...** › Doesn't download, but you'll be prompted for it again next time you start Event Log Crash Browser
- **Skip this version...** › Doesn't download the update and doesn't bother you again until there's an even newer update
- **Software update options...** › edit the software update schedule

Problems downloading or installing?

If for whatever reason, automatic download and installation fails to complete:

- Download the latest installer manually from the software verify website.

Make some checks for possible scenarios where files may be locked by Event Log Crash Browser as follows:

- Ensure Event Log Crash Browser and its help manual is also closed
- Ensure any error dialogs from the previous installation are closed

You should now be ready to run the new version.

Software update schedule

Event Log Crash Browser can automatically check to see if a new version of Event Log Crash Browser is available for downloading.

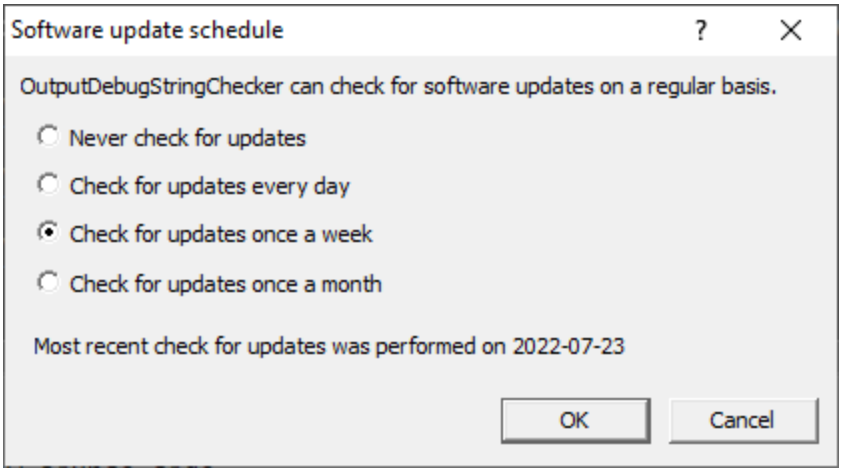
Software Updates menu › **Configure software updates** › shows the software update schedule dialog

The update options are:

- never check for updates
- check daily (the default)

- check weekly
- check monthly

The most recent check for updates is shown at the bottom.

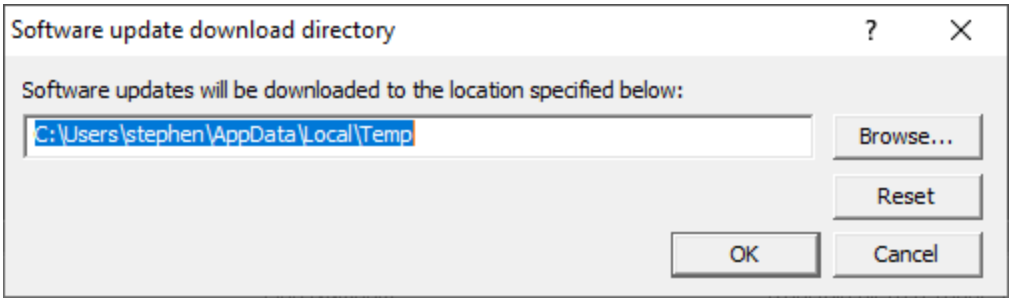


Software update directory

It's important to be able to specify where software updates are downloaded to because of potential security risks that may arise from allowing the `TMP` directory to be executable. For example, to counteract security threats it's possible that account ownership permissions or antivirus software blocks program execution directly from the `TMP` directory.

The `TMP` directory is the default location but if for whatever reason you're not comfortable with that, you can specify your preferred download directory. This allows you to set permissions for `TMP` to deny execute privileges if you wish.

Software Updates menu › **Set software update directory** › shows the Software update download directory dialog



An invalid directory will show the path in red and will not be accepted until a valid folder is entered.

Example reasons for invalid directories include:

- the directory doesn't exist
- the directory doesn't have write privilege (update can't be downloaded)

- the directory doesn't have execute privilege (downloaded update can't be run)

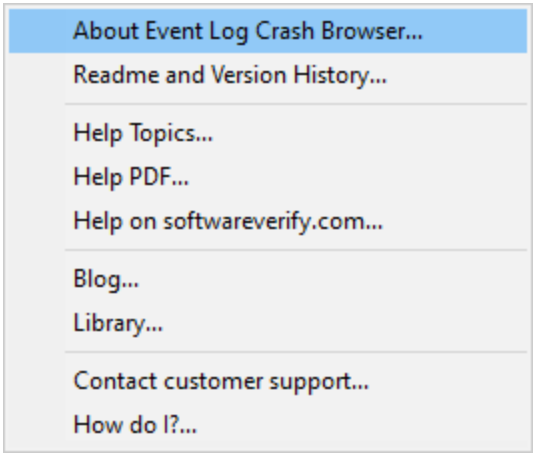
When modifying the download directory, you should ensure the directory will continue to be valid. Updates may no longer occur if the download location is later invalidated.

- **Reset** › reverts the download location to the user's `TMP` directory

  The default location is `c:\users\[username]\AppData\Local\Temp`

3.4 Help

The Help menu controls displaying this help document and displaying information about Event Log Crash Browser.



Help menu › **About Event Log Crash Browser...** › displays information about Event Log Crash Browser.

Help menu › **Readme and Version History...** › displays the readme and version history.

Help menu › **Help Topics...** › displays this help file.

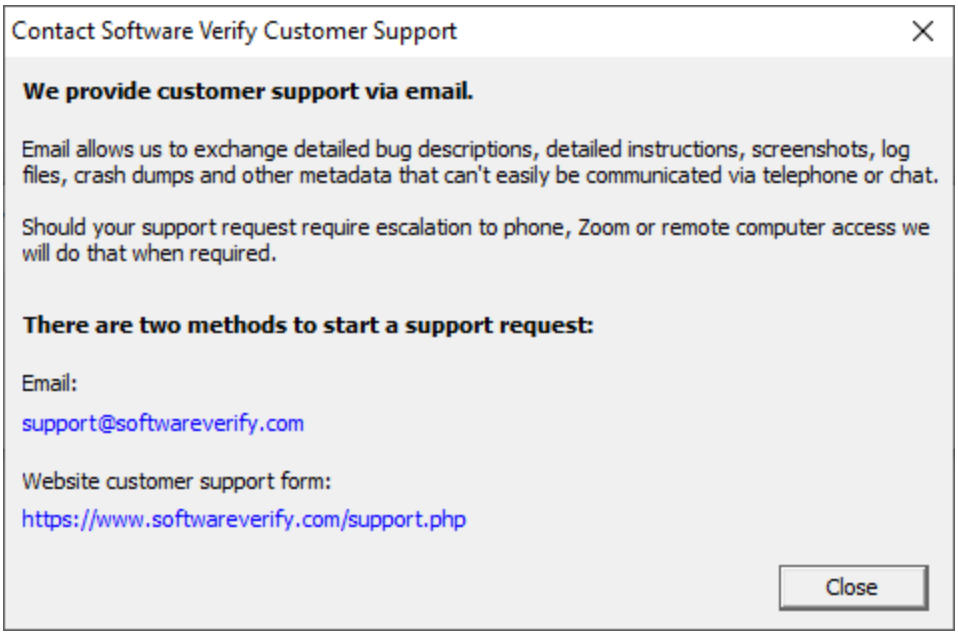
Help menu › **Help PDF...** › displays this help file in PDF format.

Help menu › **Help on softwareverify.com...** › display the Software Verify documentation web page where you can view online documentation or download compiled HTML Help and PDF help documents.

Help menu › **Blog...** › display the Software Verify blog.

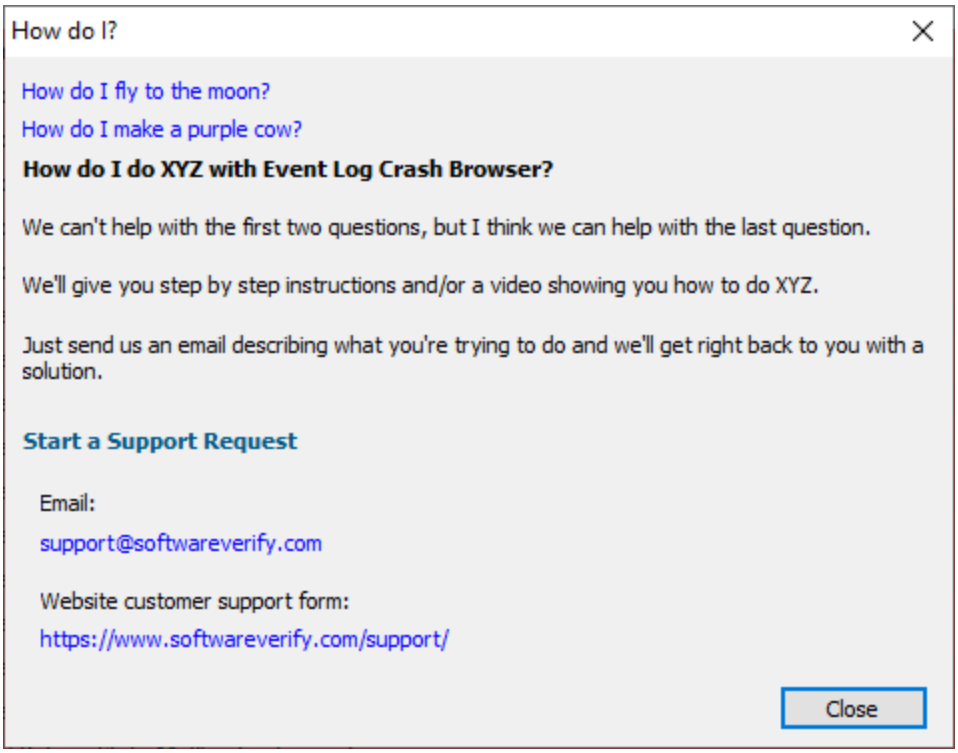
Help menu › **Library...** › display the Software Verify library - our best blog articles grouped by related topics.

Help menu › **Contact customer support...** › displays the options for contacting customer support.



Click a link to contact customer support.

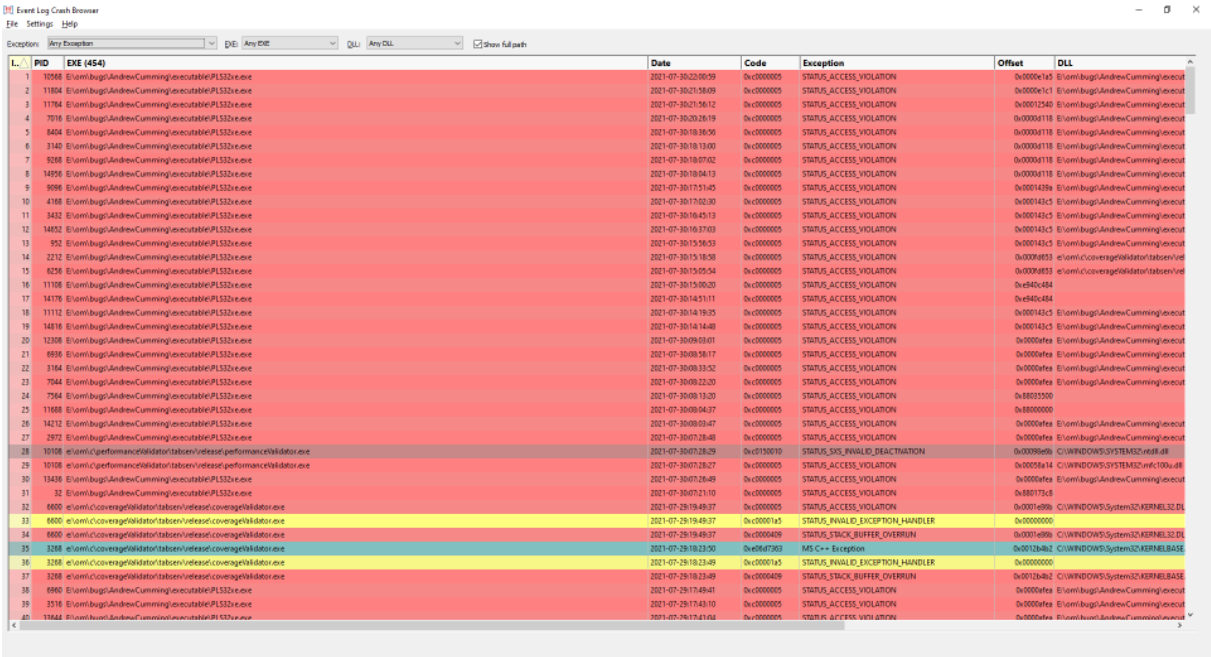
Help menu › **How do I?...** › displays the options for asking us how to do a particular task.



Part

4 The user interface

The Event Log Crash Browser user interface is shown below.



The display shows one event log crash per line. The most recent event is shown first.

Each line displays the process id, the crash executable, the crash exception code, a text version of the exception code, the crash offset and the crash DLL (the DLL that the crash occurred inside of) and the name of the company that build the DLL. The DLL field will be empty if the crash does not occur inside a DLL. The company name will only be displayed if there is a DLL name specified with a full path (some DLL names are specified without a path).

The display can be sorted by each column. Click the column header to choose which column to sort. Click the same column header again to reverse the sorting direction.

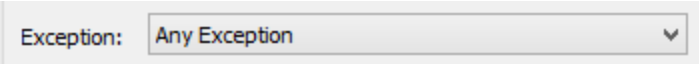
The display is colour coded according to the type of exception. This colour coding can be enabled or disable from the settings.

EXE and DLL paths are shown with full paths by default, but path information can be hidden if you wish - use the show full path checkbox.

Filters

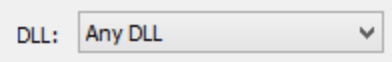
Three filters are provided: Exception, EXE and DLL.

Exception



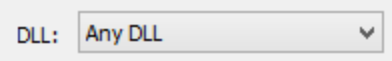
Any Exception allows any event to be displayed, whereas other selections will only display an event that has that exception type.

EXE



Any EXE allows any event to be displayed, whereas other selections will only display an event that has that executable.

DLL

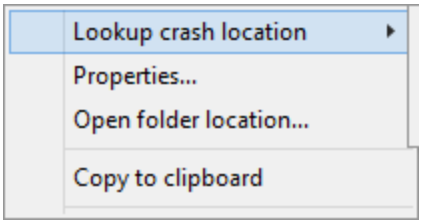


Any DLL allows any event to be displayed, whereas other selections will only display an event that has that crash DLL.

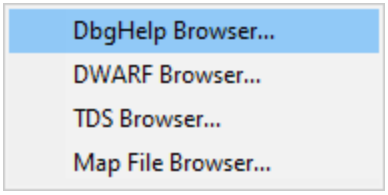
The filters combine with each other, so that you can go from displaying all events to displaying only a specific exception that happens in a specific DLL when used as part of a specific EXE.

Context Menu

There is a context menu which you can access by right clicking on any crash event. This provides options for various Software Verify debugging tools that can turn the crash offset into a symbol, filename and line number.



- **Lookup crash location**



- **DbgHelp Browser...**

DbgHelp Browser is launched to open the PDB symbols associated with the crash DLL. The symbol at the crash offset is then highlighted.

- **DWARF Browser...**

DWARF Browser is launched to open the DWARF symbols in the crash DLL. The symbol at the crash offset is then highlighted.

- **TDS Browser...**

TDS Browser is launched to open the TDS symbols associated with the crash DLL. The symbol at the crash offset is then highlighted.

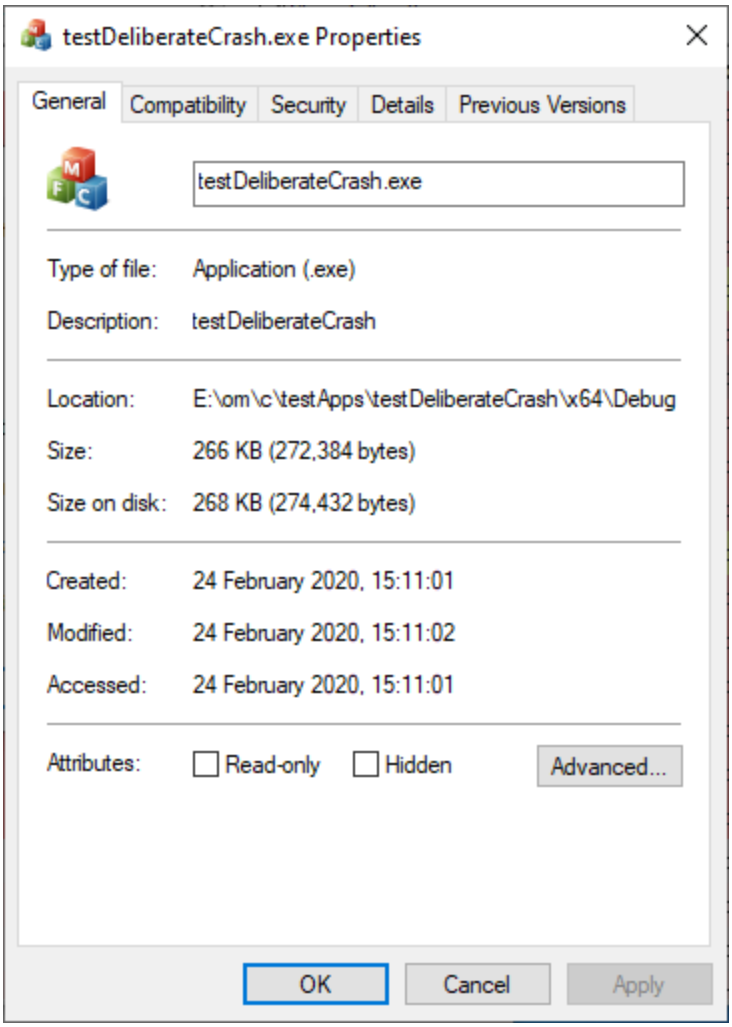
- **MAP File Browser...**

Map File Browser is launched to open the MAP file associated with the crash DLL. The symbol at the crash offset is then highlighted.

If a tool is chosen that is not installed a prompt will be displayed to download the tool.

- **Properties...**

Windows explorer is used to open a properties dialog for the crash DLL.



- **Open folder location...**

Windows explorer is used to open a folder view at the location of the crash DLL.

- **Copy to clipboard**

Crash information is copied to the clipboard in an XML format that can be used with DbgHelp Browser, TDS Browser and Map File Browser.

The format is similar to the event log XML format for Windows Error Reporting "APPCRASH", but with some of the fields left blank because we don't use them.

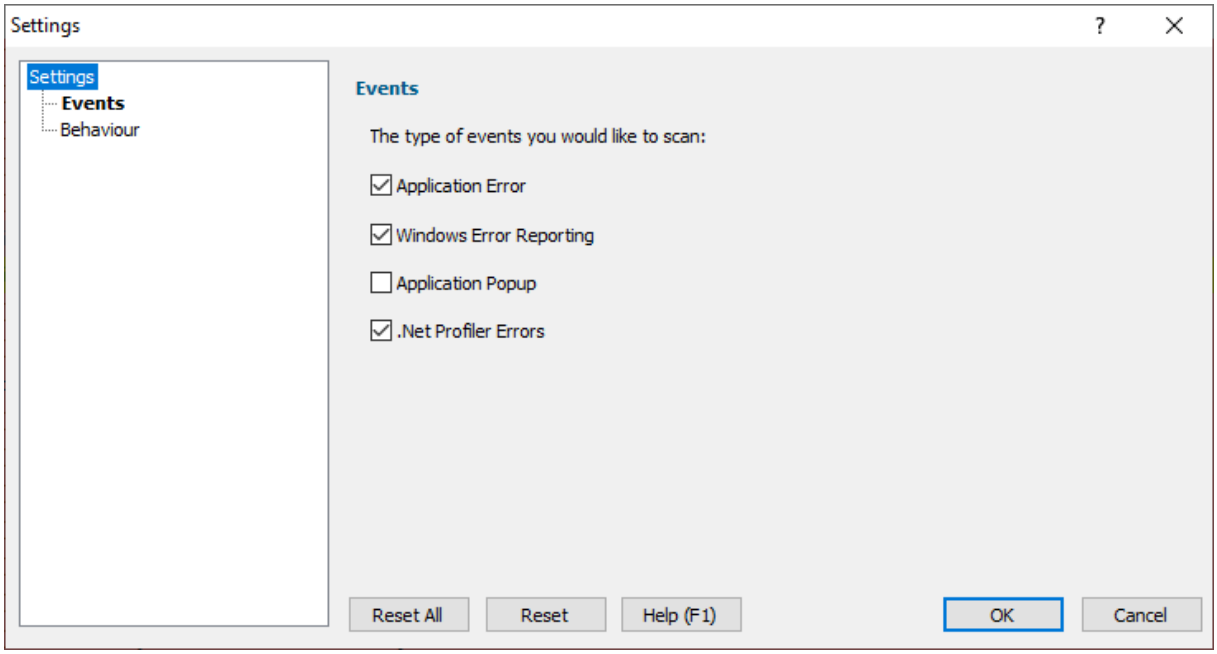
For example:

```
<Event>
  <System>
    <Provider Name="Windows Error Reporting">
  </System>
  <EventData>
    <Data></Data>
    <Data></Data>
    <Data>APPCRASH</Data>
    <Data></Data>
    <Data></Data>
    <Data>E:\om\c\testApps\testDeliberateCrash\x64\Debug\testDeliberateCrash.exe</Data>
    <Data></Data>
    <Data></Data>
    <Data>E:\om\c\testApps\testDeliberateCrash\x64\Debug\testDeliberateCrash.exe</Data>
    <Data></Data>
    <Data></Data>
    <Data>0xc0000005</Data>
    <Data>0x00001e6c</Data>
    <Data></Data>
    <Data></Data>
    <Data>STATUS_ACCESS_VIOLATION</Data>
    <Data>OK</Data>
    <Data>TODO: <Company name></Data>
  </EventData>
</Event>
```

Part V

5 SettingsDialog

The Settings dialog allows you to change what event types are searched for and how those events are displayed.

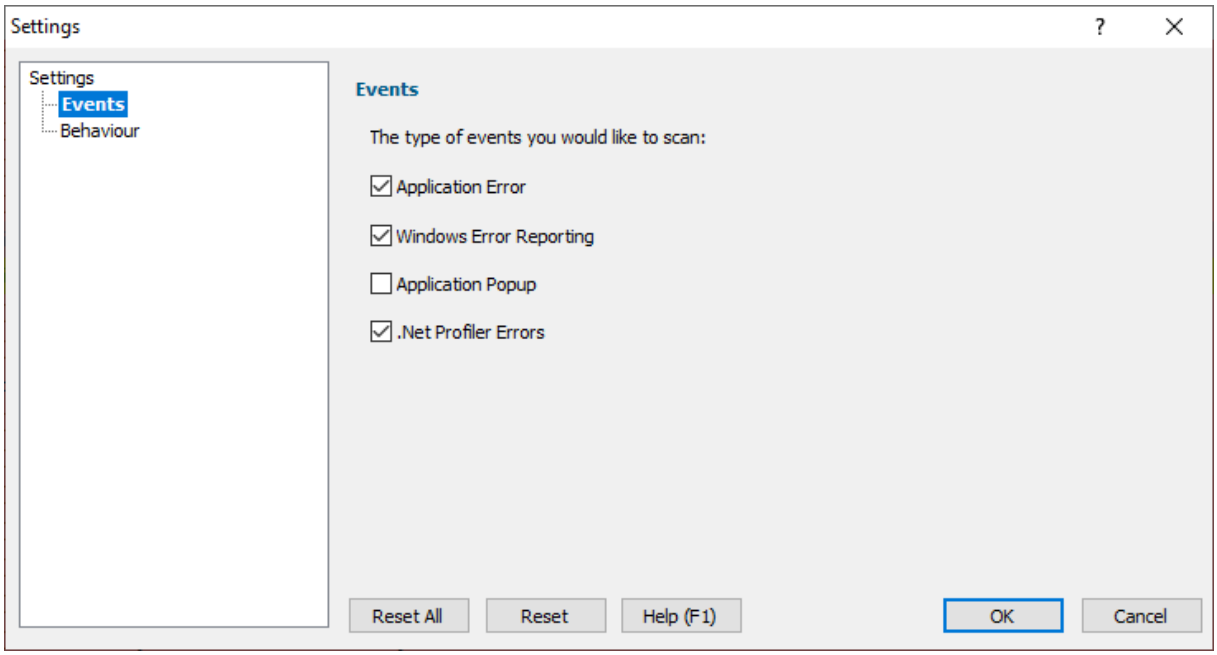


Reset

If you make a mess of the settings and wish to go back to the defaults, you can always Reset the settings.

5.1 Events

The Events settings allows you to change what event types are searched for.



Event types

Four types of events can be searched for in the event log.

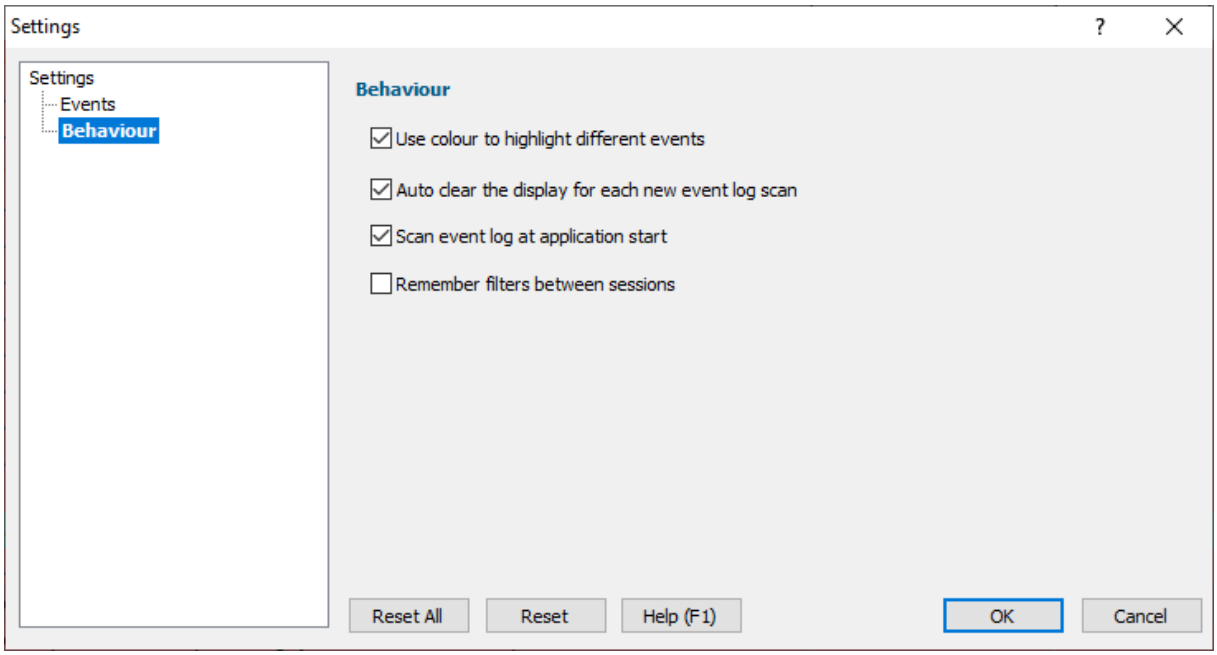
- Application Error
- Windows Error Reporting
- Application Popup
- .Net Profiler Errors

Reset

If you make a mess of the settings and wish to go back to the defaults, you can always Reset the settings.

5.2 Behaviour

The Behaviour settings allows you to change how events are displayed.



Behaviour

Colour

Colour is used to highlight different event types. By default this is enabled. If you don't want this you can turn it off.

Auto Clear

Typically we clear the display when a new event log scan is started, but if you're performing multiple searches with different event criteria you may wish to keep the results from previous scans by not enabled auto clearing of the display.

Automatic Scan

Scans are normally manually initiated, but if you always want to scan automatically you can do that. This is useful if you're using Event Log Crash Browser to quickly see what the most recent crash value is.

Filter Persistence

If you're interested in a particular crash that is repeating you may wish to set up a specific filter configuration to go with the automatic scan.

Reset

If you make a mess of the settings and wish to go back to the defaults, you can always Reset the settings.

Part VI

6 Command Line

The command line support in Event Log Crash Browser is very simple.

/export

The **/export** command takes one argument, a filename.

/export e:\crash.elcbl

Example command line

```
eventLogCrashBrowser.exe /export e:\crash.elcbl
```

The above command line will cause the list of events normally displayed on the user interface to be written to the file `e:\crash.elcbl`

This file could then be inspected at a later date, on the same computer or a different computer.

Part VII

7 Crash Logs

Event log crash information can be saved to a log file which can then be inspected at a later date on the same computer or a different computer. The Save crash log and Load crash log menu items provide support for this.

A scenario we imagine is using Event Log Crash Browser on a customer machine to save all the events to a crash log which is sent to customer support where the crash log is inspected for information related to the application under development.

There is also command line support for this style of usage.