



Eclipse Event Log User's Manual

Table of Contents

- 1 Elipse Event Log 1
- 2 Elipse Event Log Viewer 2
 - 2.1 Configuring File Storage 6
 - 2.2 Log Sessions 9
 - 2.3 Viewing Log Files 11
 - 2.4 Merging Log Files 15
 - 2.5 Searching for Events 17
 - 2.6 Filters 18
 - 2.7 Bookmarks 23
- 3 Elipse Event Log Export 28
 - 3.1 Command Prompt Options 30
- 4 Elipse Event Log Collector 32
 - 4.1 Collecting Logs 32
 - 4.2 Contents of CollectedLogs.ezp File 37
- 5 Security Restrictions 38

Eclipse Event Log is a log system developed by Eclipse Software, which integrates some new features for users, and it is available for Windows XP or later. For previous operating systems, logs still work the same way, that is, stored on text files. The main changes incorporated to the system are relative to:

- The format and the way logs are recorded
- The way to view data
- The way to manage files by the system

As for the record format, files are no longer stored as text, but in binary format, which allows more information to be stored by events. This allows a series of new features applied to stored data, such as filters, recording binary messages, sorting, and searching.

As for the recording mode, it is now safer and robust. In case of any failure during the process, logs are always stored on disk, which guarantees that messages are not lost. In addition, new file recording modes were added, allowing sequential and circular files, as well as serialization for backup.

As for ways to view data, the new system now is an ActiveX control, which can be also integrated into an E3 application. In addition, it is possible to export events to a text file. With the new viewer, it is possible to filter, search, and select specific messages.

Finally, there is a new file management, which guarantees maintenance of maximum file size on disk without running out of the available space. The log service, from the moment it is configured and started, constantly monitors the repository folder, controlling files that must be kept on disk, rotating the recent ones and deleting the older ones.

Elipse Event Log Viewer

Elipse Event Log Viewer (from now on, referred only as **Log Viewer**) views messages of a supervisory system stored on files in *Event Trace Logfile* (.etl) format. These logs store information about Elipse systems on user's computer.

Basically, processes store these messages on disk using pre-configured folders, which are created by the log system when it is started. A service running on the system is responsible for managing the size of the files on the log folder, as well as their lifetime. If this service is disabled or is not running, it is not possible to perform a file management.

The main function of Log Viewer is to display system-generated messages to users, by using filter and search functions, making the task of searching for errors easier.

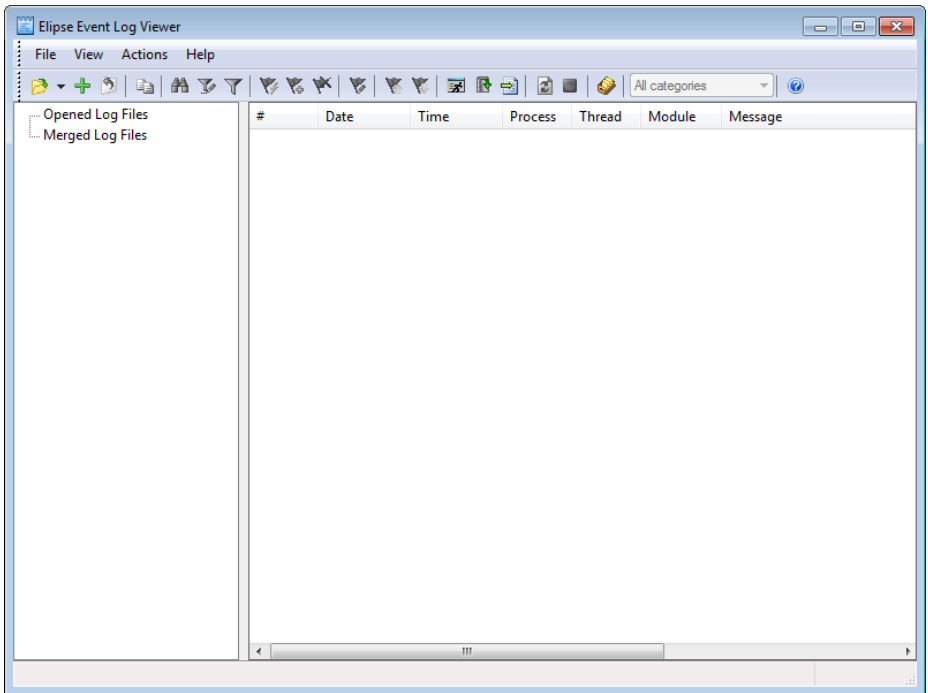
IMPORTANT: These logs are only enabled by users belonging to Windows **Administrator** or **Performance Log Users** groups. For more information, please check the topic **Security Restrictions**.

Log Viewer presents the following features:

- Opens files in ETL format
- Opens more than one file at a time, merging the content of these files
- Searches for messages
- Filters messages by type and by time
- Views log sessions in use
- Exports events to files with tab-separated columns
- Configures view options
- Configures storage options of messages on disk
- Allows selecting and copying events to the Clipboard

To use Log Viewer, follow these procedures:

1. On the **Start** menu, select **Programs - Elipse Software - Elipse Event Log - Log Viewer**. The window on the next figure is opened.















Eclipse Event Log Viewer's main window

The program is divided into two areas: on the left side is the file's viewing area, and on the right side is the event's viewing area. Above them there is a toolbar and below there is a status bar. The available options on this toolbar are described on the next table.

Available options on the toolbar

ICON	COMMAND	ACTION
	Open Event File	Opens a log file.
	Merge Event Files	Opens several files and merges the events chronologically on the same view.
	Close File	Closes the selected file.
	Copy	Copies the selected events to the Clipboard.
	Find	Opens the window to search for messages.
	Filter Editor	Shows the window to edit filters.

ICON	COMMAND	ACTION
	Toggle Filter On/Off	Turns on or off the filters on the events of the selected file.
	Fast Bookmark	Creates a bookmark with a default name Bookmarkn , where n is an automatically-incremented number.
	Add Bookmark	Creates a bookmark, by opening a window to choose its name.
	Remove Bookmark	Removes the selected bookmark.
	Edit Bookmarks	Opens an edition window, which allows removing a bookmark, removing all bookmarks, or locating a bookmark.
	Previous Bookmark	Selects the previous bookmark.
	Next Bookmark	Selects the next bookmark.
	Running Loggers	Shows the active log sessions on the system.
	Collect files	Opens the Elipse Event Log Collector's window.
	Export Events	Opens the Elipse Event Log Export's window.
	Refresh View	Refreshes the view with the last events recorded on disk. If there are events in memory, they are recorded on disk before refreshing.
	Cancel Refresh	Cancels the view refresh with the files on disk.
	Storage Settings	Displays the file storage configuration window .

ICON	COMMAND	ACTION
	Categories	Selects a category to sort the message.
	About	Opens a window with the version of Log Viewer and its components.

The available categories for message sorting are described on the next table.

Available categories for message sorting

NUMBER	CATEGORY	COLOR
0	Log header	Green
10	Error	Red
11	Warning	Yellow
12	Information	Blue
14	Message for general usage	--
15	Statistical and performance data	--
16	Trace	--
17	Additional information about the module	Purple


The status bar of Log Viewer's main window is divided into four areas, shown on the next table.

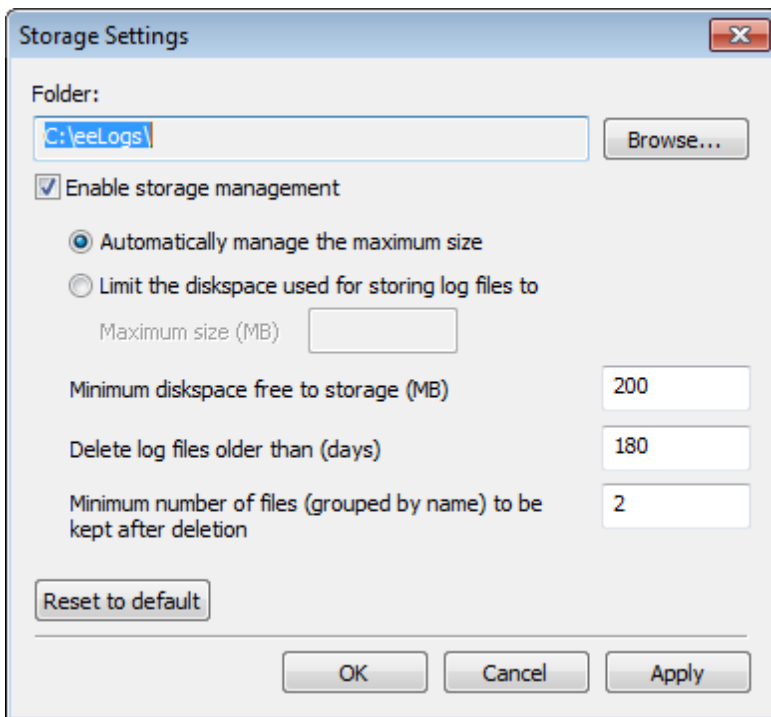
Areas of Log Viewer's status bar

AREA	DESCRIPTION
Number of events	Number of events of the selected file on the viewing area. If there is no file selected, it displays the message "Ready". In case there is any active filter, the displayed value refers to events visible after applying that filter.

AREA	DESCRIPTION
Selection	<p>Displays information about time interval between two events:</p> <ul style="list-style-type: none"> • Timespan between events: Time interval between two events, with a precision of milliseconds • Interval: Amount of existing events between selected events • Average: Time average between two selected events, with a precision of milliseconds <p>In case there are more than two events selected, this area only displays the amount of selected events.</p>
Processing	Displays the percentage of successfully processed events in the selected file.
Filters	Displays whether there is any active filter in the selected file.

2.1 Configuring File Storage

By using the **Storage Settings** option, it is possible to configure automatic management of .etl or .log files recorded by Elipse systems. With it, users can manage where log files are stored, the maximum size of the repository, and the time each file is kept on the repository (based on file's creation date). To use this option, select the **View - Storage Settings** menu, or click .



The image shows a 'Storage Settings' dialog box with a title bar containing a close button. The 'Folder:' label is above a text field containing 'C:\eeLogs' and a 'Browse...' button. Below this is a checked checkbox for 'Enable storage management'. Underneath are two radio buttons: 'Automatically manage the maximum size' (selected) and 'Limit the diskspace used for storing log files to'. The second option is followed by a 'Maximum size (MB)' text field. Below these are three text fields: 'Minimum diskspace free to storage (MB)' with value '200', 'Delete log files older than (days)' with value '180', and 'Minimum number of files (grouped by name) to be kept after deletion' with value '2'. At the bottom left is a 'Reset to default' button, and at the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

Storage Settings window

NOTE: Be careful when disabling the repository with value 0 (zero) in the **Limit the diskspace used for storing log files to** option, because if the **Enable storage management** option is selected, management leaves the repository with a minimum number of files (by name pattern, predefined as 2) as soon as this option is confirmed by clicking **OK** or **Apply**.

The available options on this window are described on the next table.

Available options on Storage Settings window

OPTION	DESCRIPTION
Folder	Shows where logs are stored.
Browse	Allows choosing the folder where logs are stored.
Enable storage management	Enables repository management. When this option is selected, repository management routines are activated.
Automatically manage the maximum size	The log system calculates the available limit based on the partition's free space to manage logs. The rule for allocating space in the automatic mode is using 25% (twenty five percent) of partition's free space.

OPTION	DESCRIPTION
Limit the diskpace used for storing log files to	Specifies the maximum available size for storing logs on disk. If it is specified a size equal to 0 (zero), log files are deleted as soon as they are released by the session.
Minimum diskpace free to storage (MB)	Determines the minimum disk space on a partition to reallocate logs, or to start recording on the repository. This is the lower band limit to be monitored.
Delete log files older than (days)	Specifies the number of days during which the files will be stored. If this value is equal to 0 (zero), management occurs by size or by minimum number of files.
Minimum number of files (grouped by name) to be kept after deletion	Specifies the minimum number of files that must be kept on the repository when excluding files derived from the same name. If this value is equal to 0 (zero), management occurs by size or by minimum size of files. A value greater than zero leaves at least this amount of files for each group of names, as for example E3*.*, E3Server*.*, etc.
Reset to default	Restores default values for fields: <ul style="list-style-type: none"> • Twenty five percent of partition's free space • Automatic management of the space • One hundred eighty days • Two files


NOTE: The following routines and the management only occur when there is a need to release files, because their size is near the configuration limit (the **Limit the diskpace used for storing log files to** option).

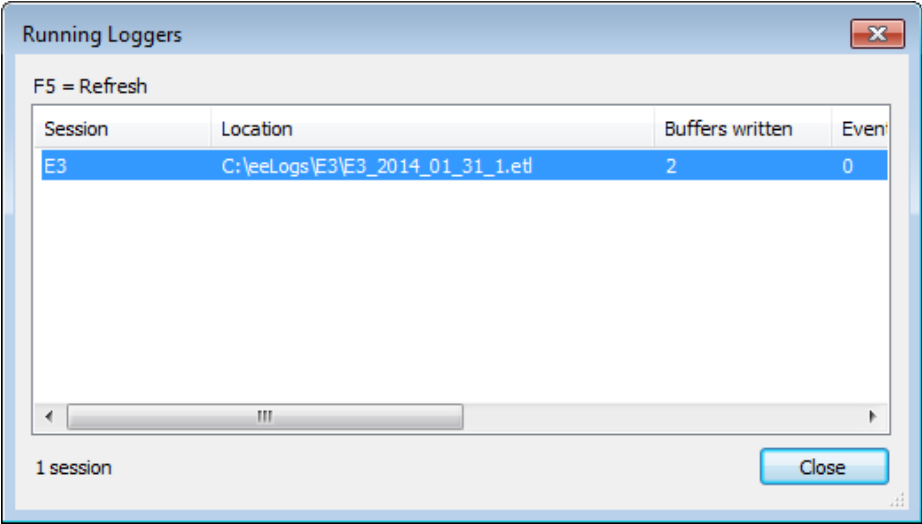
The execution order of repository's file exclusion filters is the following:

1. **Creation date:** When executing the management, all files with a creation date prior to the maximum allowed (the **Delete log files older than (days)** option) are erased, starting from the oldest to the newest ones, as long as the size of the files overrides the repository's maximum quota.
2. **Name pattern:** If even after erasing the oldest files of the repository (the **Delete log files older than (days)** option), still the remaining size is greater than the limit, files are processed by a name filter (the **Minimum number of files** option). In this filter, files are erased up until the control limit is reached, but preserving at least the configured amount of files. This is very useful for establishing a sequence in the regressive analysis of events.
3. **Total size of the repository:** The last filter executed is by total size of the repository. In this case, if still after performing the previous filters the

repository is above the limits, files are erased from the oldest to the newest ones, until reaching the security limit.

2.2 Log Sessions

Another option available on Log Viewer is the visualization of active log sessions being recorded by the system. To open this option, select the **View - Running Loggers** menu, or click . The following window is then opened.



Running Loggers window

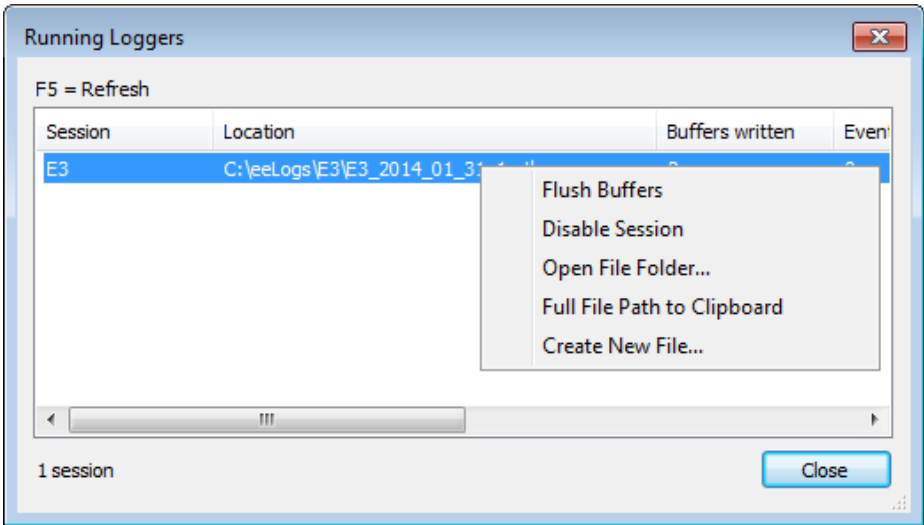
The available columns for viewing are described on the next table.

Available columns on the Running Loggers window

COLUMN	DESCRIPTION
Session	Name of the log session.
Location	Path of log recording.
Buffers written	Buffers written to disk.
Events lost	Indicates events lost (rejected by the system). This counter must always be equal to zero. If this value is greater than zero, it indicates that events were lost, and therefore files do not have all information for debugging.
Log file size (MB)	Size of the files, in megabytes.
Flush timer (s)	If it is equal to 0 (zero), the buffer is only stored on disk when full. If different from 0 (zero), at every x seconds the buffers are automatically written to disk.
Log mode	Recording mode.
Buffer size (KB)	Size of buffers in memory.

It is possible to remove or add columns by right-clicking column names. Only the **Session** column cannot be removed.

It is also possible to select a few actions that can be applied to log sections, by right-clicking the respective row.



Options for editing a specific event of the active session

The available options are described on the next table.

Available options on Running Loggers menu

OPTION	DESCRIPTION
Flush buffers	Stores on disk the events currently in memory.
Enable or Disable Session	Disables event recording, although it does not stop the session. When disabling recording, the session row turns red, indicating that the log is no longer recording events. When enabling this option again, the session restarts event recording.
Open File Folder	Opens a Windows Explorer window, at the directory where log files are stored, configured in the Folder field of the Storage Settings window.
Full File Path to Clipboard	Copies the full path of the selected log session file to the Clipboard.


OPTION	DESCRIPTION
Create New File	Creates a new log file on the selected session. This contextual menu item is disabled in case the recording mode (the Log Mode column) or the session are incompatible with the creation of new files.

The Running Sessions window allows dragging and dropping files to Log Viewer's main window, as well as to an external window (such as Windows Explorer, for example).

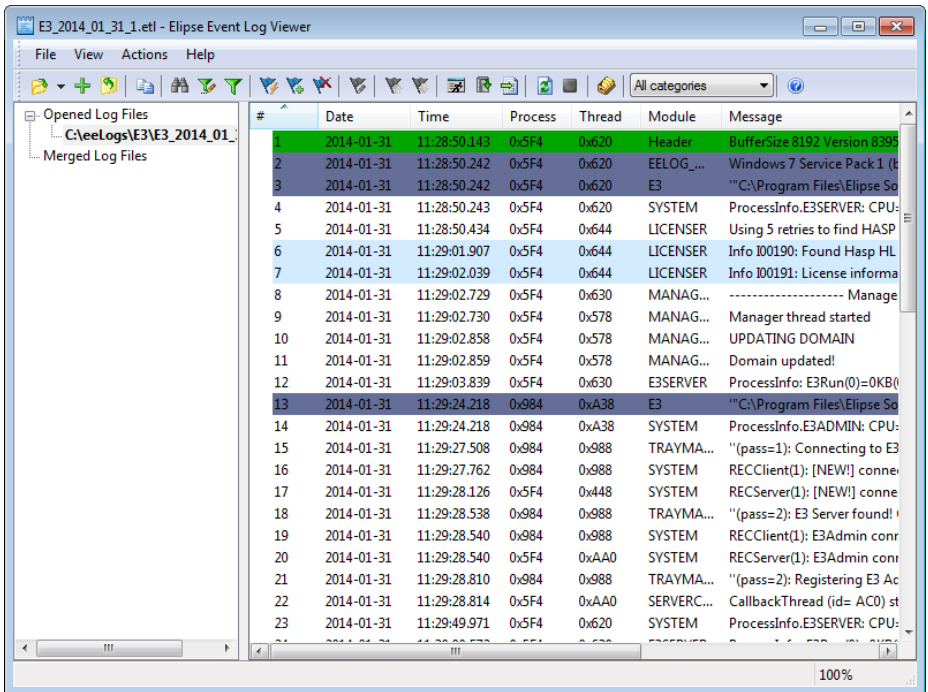
In case of Log Viewer's main window, the behavior of this feature is the following: if the file is dragged and dropped onto the **Merged Log Files** item, it is added to this item. If the file is dropped onto any other area of the main window (the default behavior), the file is added to the **Opened Log Files** item. In case of a file being dragged outside Log Viewer's main window, a copy of the file is then created on the destination where it is dropped.

2.3 Viewing Log Files

Log Viewer allows opening one or more files at the same time, merging information of these files and monitoring log sessions. Log files with an .etl extension can be opened by Log Viewer in three ways:

- By using the **File - Open Event File** menu
- By using the  icon on the toolbar
- By dragging a file to the window

The result is a window similar to the one on the following figure.



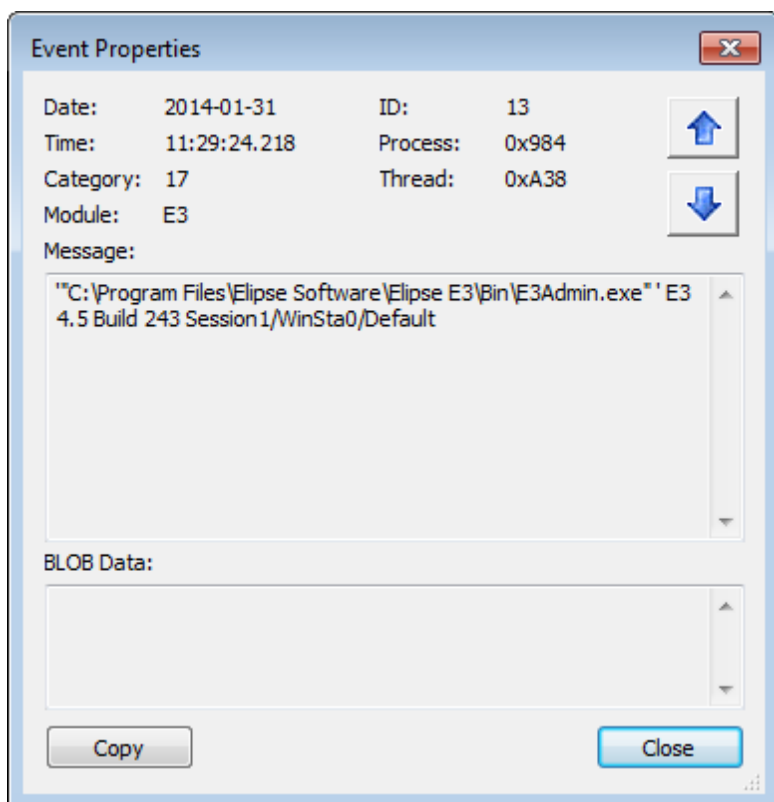
Opening a log file

On the event viewing area, files are sorted chronologically, one event by row. Messages in green are information about the structure of log files, and are not part of messages of the process that recorded events on the session.

The status bar, on the lower part of the window, always indicates the number of selected events (in this example, 88), the percentage of processed ones (in this example, 100%), and the status of search filters (in this example, the search was not affected by filters).

When right-clicking the header of the event list, it is possible to select, on its contextual menu, which columns are visible or invisible to users.

To view message details, select the corresponding row and type ENTER or double-click the message. The window on the next figure is then displayed.





Log message details

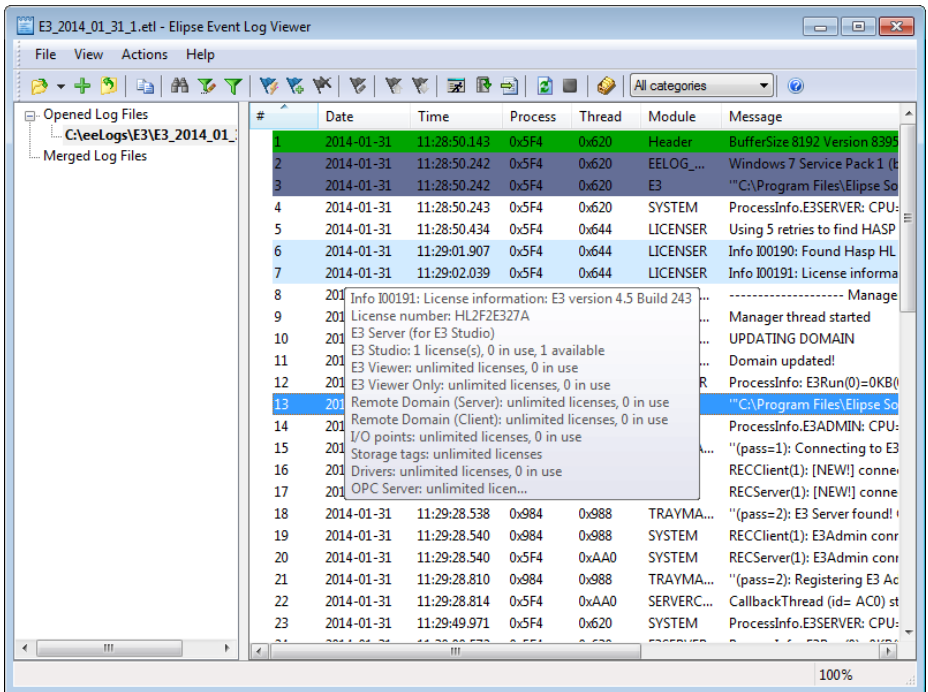
The available options on this window are described on the following table.

Available options on the Event Properties window

OPTION	DESCRIPTION
Date	The event date, in YYYY-MM-DD format.
ID	A unique identifier for every event.
Time	The event time, in HH:MM:SS.000 format.
Process	Identifier of the process generating the event. This value can be displayed in hexadecimal or decimal format, depending on the selection performed in the Process and Thread as Hexadecimal option of the event's contextual menu.
Category	Event category, according to the table at the beginning of this chapter.

OPTION	DESCRIPTION
Thread	Identifier of the thread generating the event. This value can be displayed in hexadecimal or decimal format, depending on the selection performed in the Process and Thread as Hexadecimal option of the event's contextual menu.
Module	Identifies the module, function, or area name inside the process or thread responsible for generating information about the event.
 and 	Allows navigating through the previous and next events relative to the selected event.
Message	Text of the event message.
BLOB Data	Shows whether along with the event there is binary data (<i>Binary Large Objects</i>) attached, which complements information given by the event's Message field. This field is optional and therefore it may not have data associated.
Copy	Allows copying the selected event to the Clipboard.
Close	Closes this window.

When mouse pointer remains over an event for some time, a tooltip appears displaying the message, as in the next figure.



Information about a log message

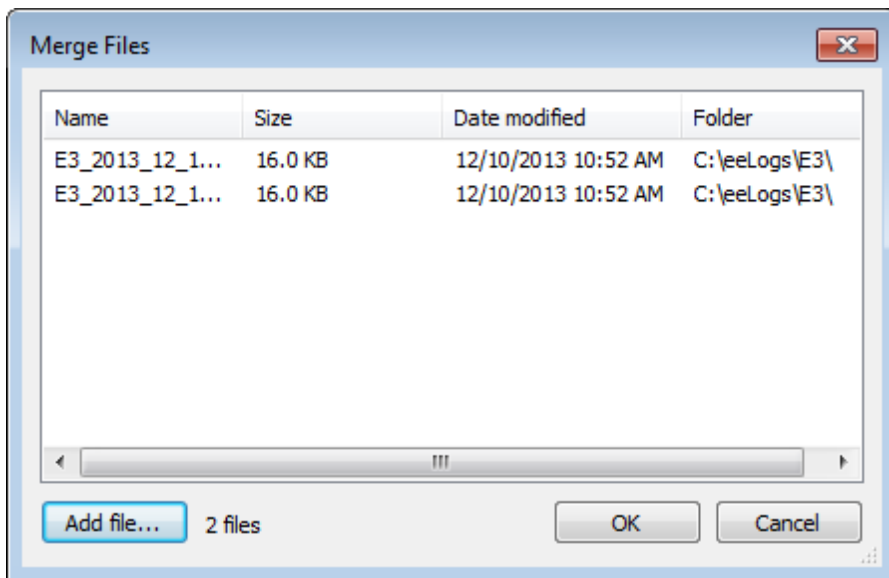
When right-clicking a file, the following options are displayed on its contextual menu:

- **Close All Files:** Closes all open files
- **Close File:** Closes only the selected file
- **Merge File:** Adds the selected file to the **Merged Log Files** node
- **Open File Folder:** Opens the directory where log files are stored

2.4 Merging Log Files

With Log Viewer, it is also possible to open more than one file at the same time and merge their information as if they were a single file. Events are sorted chronologically, which allow an analysis of cause and consequence events among different machines or different files. In this example, events from two files are merged.

1. Click **+**, or use the **File - Merge Event Files** menu. The window on the next image is then opened.



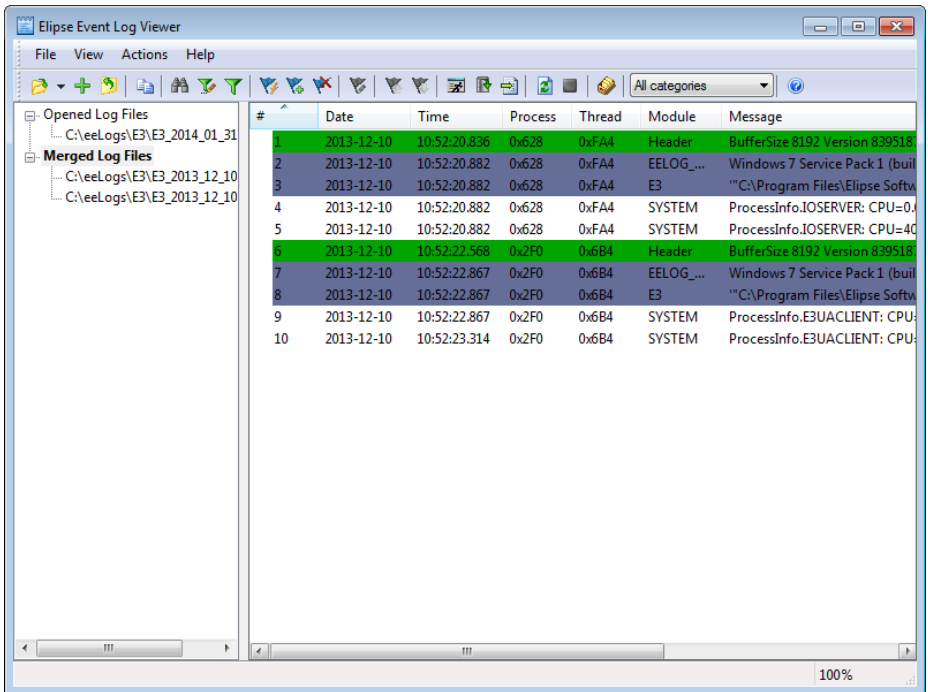
Merge Files window

The available columns to view files for merging are described on the next table.

Available options on Merge Files window

OPTION	DESCRIPTION
Name	The name of the file.
Size	The size of the file.
Date modified	The date when the file was last modified.
Folder	The path of the file.

2. Select the files to merge, by clicking **Add File**.
3. Events are opened already sorted by time, such as in the next figure.




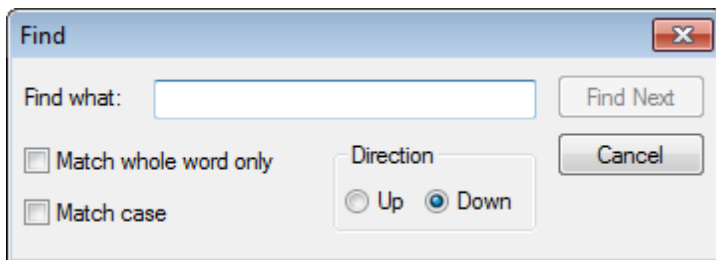
Window with files for merging

Another option is selecting a file from the **Opened Log Files** node, right-clicking it, and then selecting the **Merge File** option. That file is automatically added to the **Merged Log Files** node.

The status bar informs the total amount of events of all files opened as a set. These files are on the left area, below **Merged Log Files**. If the whole node is selected, events from all files of this node are viewed. However, when selecting each file individually, only its own events are displayed.

2.5 Searching for Events

Log Viewer offers search and filter functions, which makes it easy to search for specific events inside a file. To use this option, click the **Actions - Find** menu, or click . The window on the next figure is then opened.



Find window

The available options are described on the next table.

Available options on Find window


OPTION	DESCRIPTION
Find what	Message to search for.
Match whole word only	Searches for the value as a word or a whole phrase, and not as a part of other messages.
Match case	Differentiates between upper and lower case.
Direction	Searches for the next occurrence up or down the currently selected example.
Find Next	Searches for the next occurrence of the currently selected value.
Cancel	Cancels the operation.

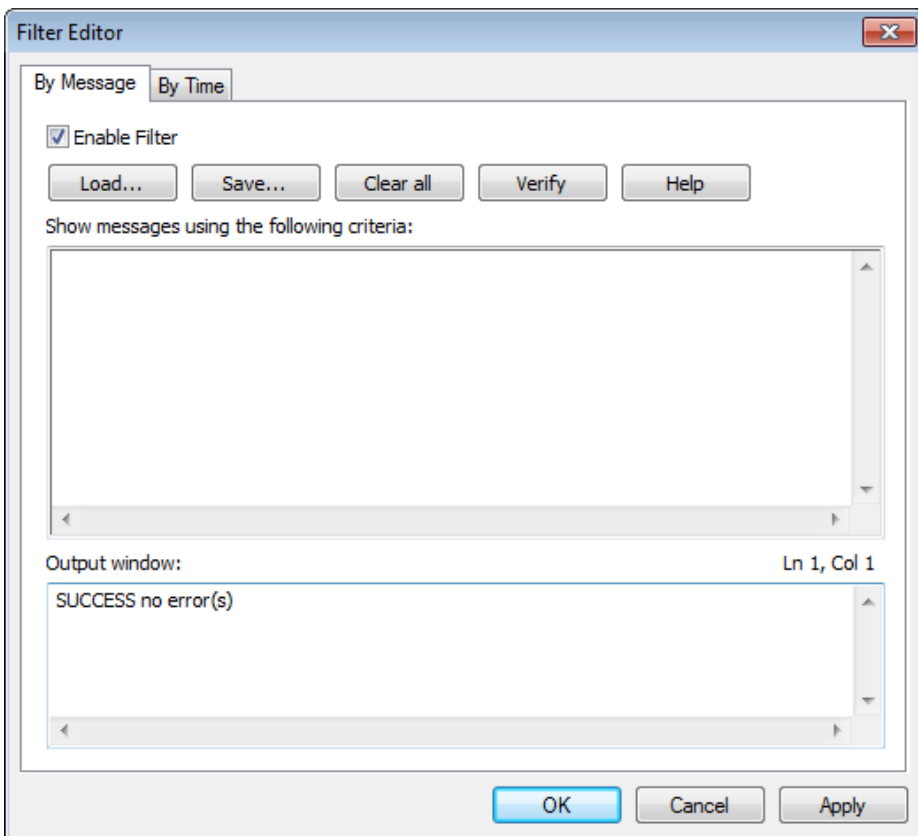
After searching the whole file (according to the selected direction), the search is then finished.

2.6 Filters

Filters are an option to refine event viewing. In Log Viewer, there are two independent types of filters: by **Message** or by **Time**.

2.6.1 Message Filter

A **Message Filter** allows restricting an event interval, by selection the type of message to display. To use this option, select the **Actions - Filter Editor** menu or click , and then select the **By Message** tab. The window on the next window is displayed.



By Message tab of the Filter Editor window

The available options are described on the next table.

Available options on the By Message tab

OPTION	DESCRIPTION
Enable Filter	Enables the usage of a By Message filter.
Load	Loads a saved filter.
Save	Saves a filter to a file with an .sfi extension.
Clear all	Clears the selected filter.
Verify	Checks whether there are errors on filter's syntax.
Help	Shows the correct syntax to build a filter.
Show messages using the following criteria	Edits scripts of the selected filters.
Output Window	Displays the help for the selected option on Functions , or else the error messages after check using the Verify option.

When clicking **Help**, a window is displayed with the correct syntax for each valid keyword, such as the next figure.



Window with help on correct keyword syntax

When more than one value is used on a keyword, they must be separated by commas.

The filter script restricts event viewing, therefore if no event matches the specified criteria, the resulting list of events remains empty.

Filter elements or keywords are: **Thread**, **Process**, **Message**, **Category**, and **Module**. Users can choose between the equal to (==) and different from (!=) operators.


All filter parameters inside parenthesis are evaluated as an **OR** for that filter keyword or element. Example:

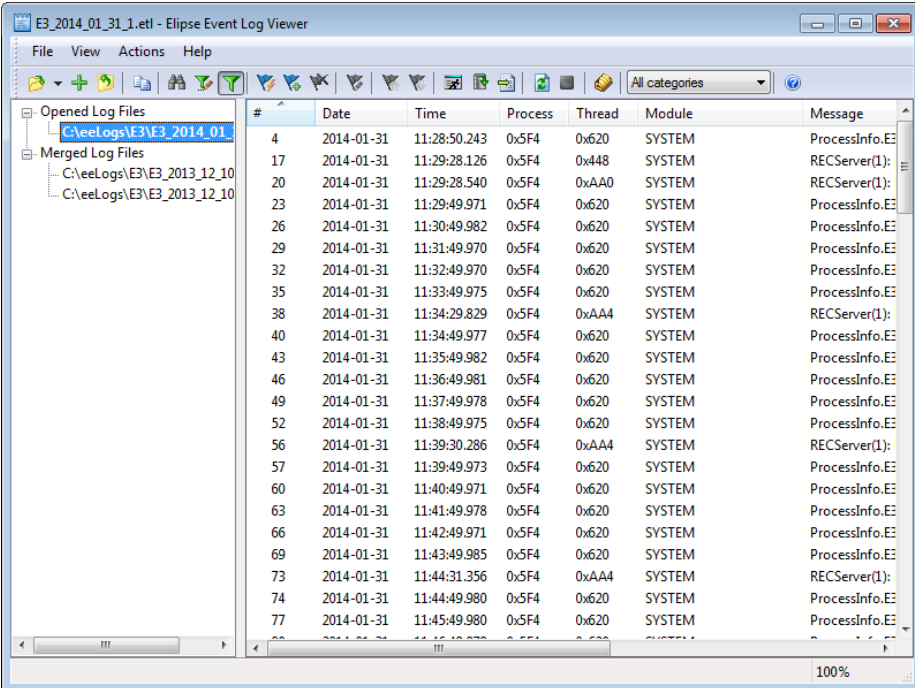
```
Process == (0x5F4);
```

```
Module == ("SYSTEM");
```

This means that only events that match the following logical equation are displayed:

```
(Process == 0x5F4) AND Module == SYSTEM
```

To turn the filter on, click  on the toolbar. For the filter on the previous example, the result is similar to the one displayed on the next figure.




The screenshot shows the Elipse Event Log Viewer interface. The left pane displays a tree view of log files, with 'C:\eeLogs\E3\E3_2014_01' selected. The main pane shows a table of filtered events. The table has columns for #, Date, Time, Process, Thread, Module, and Message. The filter 'Module == ("SYSTEM");' is applied, and the results show only events where the Process is 0x5F4 and the Module is SYSTEM. The messages are truncated in the screenshot.

#	Date	Time	Process	Thread	Module	Message
4	2014-01-31	11:28:50.243	0x5F4	0x620	SYSTEM	ProcessInfo.E3
17	2014-01-31	11:29:28.126	0x5F4	0x448	SYSTEM	RECServer(1):
20	2014-01-31	11:29:28.540	0x5F4	0xAA0	SYSTEM	RECServer(1):
23	2014-01-31	11:29:49.971	0x5F4	0x620	SYSTEM	ProcessInfo.E3
26	2014-01-31	11:30:49.982	0x5F4	0x620	SYSTEM	ProcessInfo.E3
29	2014-01-31	11:31:49.970	0x5F4	0x620	SYSTEM	ProcessInfo.E3
32	2014-01-31	11:32:49.970	0x5F4	0x620	SYSTEM	ProcessInfo.E3
35	2014-01-31	11:33:49.975	0x5F4	0x620	SYSTEM	ProcessInfo.E3
38	2014-01-31	11:34:29.829	0x5F4	0xAA4	SYSTEM	RECServer(1):
40	2014-01-31	11:34:49.977	0x5F4	0x620	SYSTEM	ProcessInfo.E3
43	2014-01-31	11:35:49.982	0x5F4	0x620	SYSTEM	ProcessInfo.E3
46	2014-01-31	11:36:49.981	0x5F4	0x620	SYSTEM	ProcessInfo.E3
49	2014-01-31	11:37:49.978	0x5F4	0x620	SYSTEM	ProcessInfo.E3
52	2014-01-31	11:38:49.975	0x5F4	0x620	SYSTEM	ProcessInfo.E3
56	2014-01-31	11:39:30.286	0x5F4	0xAA4	SYSTEM	RECServer(1):
57	2014-01-31	11:39:49.973	0x5F4	0x620	SYSTEM	ProcessInfo.E3
60	2014-01-31	11:40:49.971	0x5F4	0x620	SYSTEM	ProcessInfo.E3
63	2014-01-31	11:41:49.978	0x5F4	0x620	SYSTEM	ProcessInfo.E3
66	2014-01-31	11:42:49.971	0x5F4	0x620	SYSTEM	ProcessInfo.E3
69	2014-01-31	11:43:49.985	0x5F4	0x620	SYSTEM	ProcessInfo.E3
73	2014-01-31	11:44:31.356	0x5F4	0xAA4	SYSTEM	RECServer(1):
74	2014-01-31	11:44:49.980	0x5F4	0x620	SYSTEM	ProcessInfo.E3
77	2014-01-31	11:45:49.980	0x5F4	0x620	SYSTEM	ProcessInfo.E3

Example of a result after applying filters

It is possible to check filter results using the **Process** and **Module** columns.

2.6.2 Time Filter

A **Time Filter** allows restricting a message interval, by selecting the start and end date and time to display. To use this option, select the **Actions - Filter Editor** menu or click , and then select the **By Time** tab. The window on the next figure is displayed.

By Time tab of the Filter Editor window

The available options are described on the next table.


Available options on the By Time tab

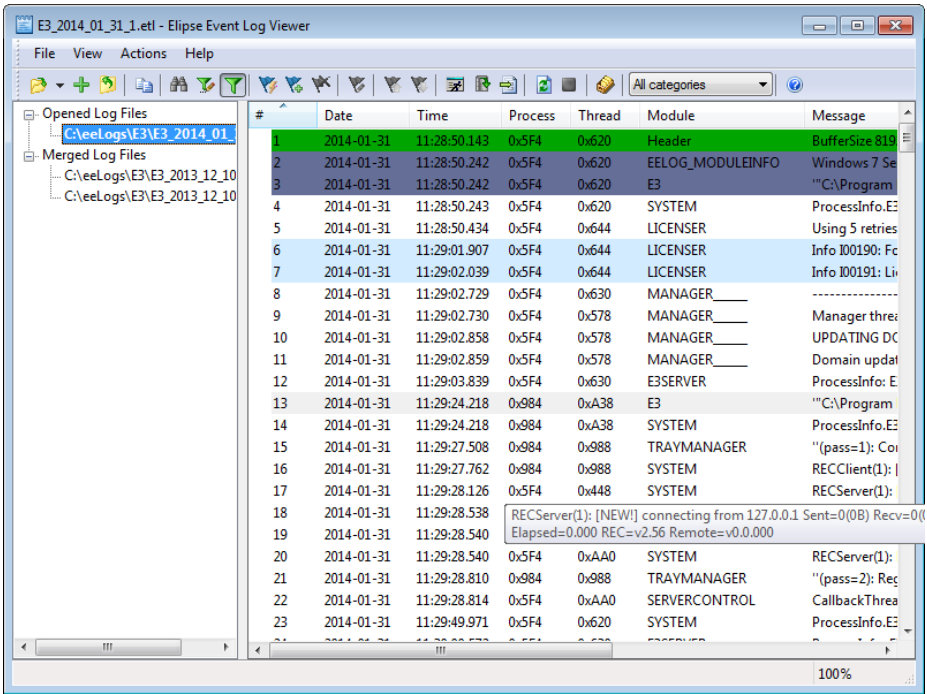
OPTION	DESCRIPTION
Enable Filter	Enables the usage of a By Time filter.
Start	Selects the starting date and time for the filter.
End	Selects the ending date and time for the filter.

Whenever the final date and time are previous to the start date and time, or the final time interval is previous to the start time interval, the filter is automatically disabled.

On a **By Time** filter, the start time is included, but the final one is excluded. That is, a filter between **09:30:47** and **09:35:47** displays only events up to the second **46**. Therefore, it is not allowed a **By Time** filter using the same dates and times.


Notice that, although it is possible to select the starting and ending time by message number, the milliseconds of the interval are zeroed. Therefore, when selecting a specific starting second, all its events are listed, since the first millisecond.

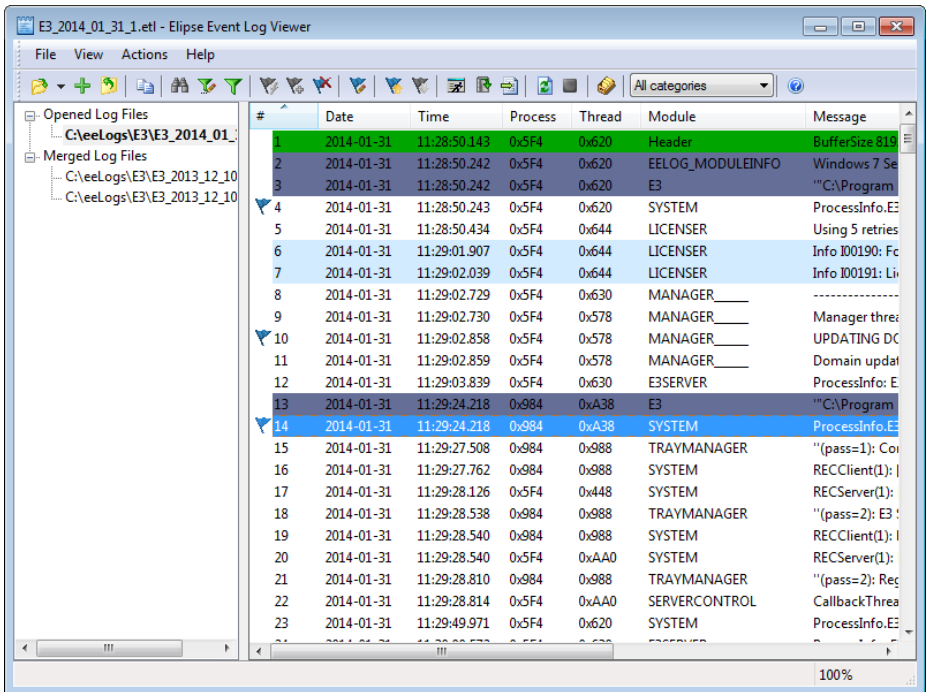
To turn the filter on, click  on the toolbar. The result is similar to the one showed on the next figure (for messages in the interval between **2014-01-31 11:28:50** and **2014-01-31 13:06:49**).



Example of a filter by time

2.7 Bookmarks

Bookmarks are tags that can be linked to one or more events in a file. On event viewing area there is a column named **Bookmarks**, which displays events that have a linked bookmark. In these cases, an icon  is placed near the event ID.




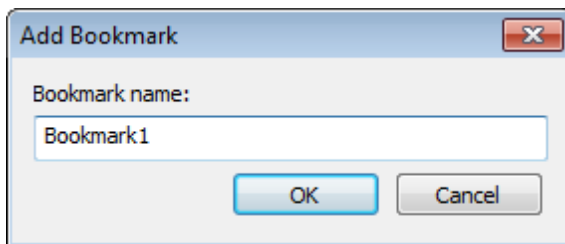
Elipse Event Log Viewer window with bookmarks linked to events

The available option on the bookmarks toolbar are described on the next table.


Available options for the bookmark toolbar

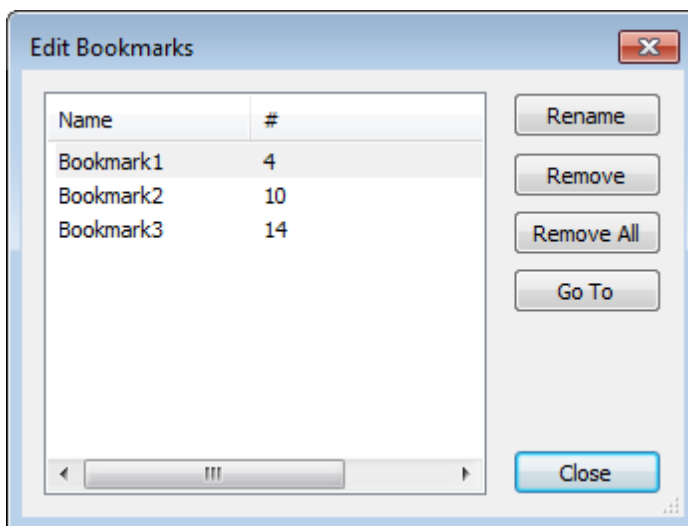
ICON	OPTION	DESCRIPTION
	Fast Bookmark	Adds a bookmark with an automatically generated name for all selected events.
	Add Bookmark	Opens a window to ask for a name for the bookmark, and adds it to all selected events.
	Remove Bookmark	Removes the bookmarks from the selected events.
	Edit Bookmarks	Opens a window for bookmark edition.
	Previous Bookmark	Selects the previous bookmark.
	Next Bookmark	Selects the next bookmark.

When clicking , the window on the next figure is then displayed.



Add Bookmark window

In the **Bookmark name** field, users must inform a name for the bookmark. If there is already a bookmark with this name, then the selected event is added to a list of events linked to that bookmark. If it does not exist, then a new bookmark is created and the selected event is linked to it. When clicking , the window on the next figure is then displayed.



Edit Bookmarks window

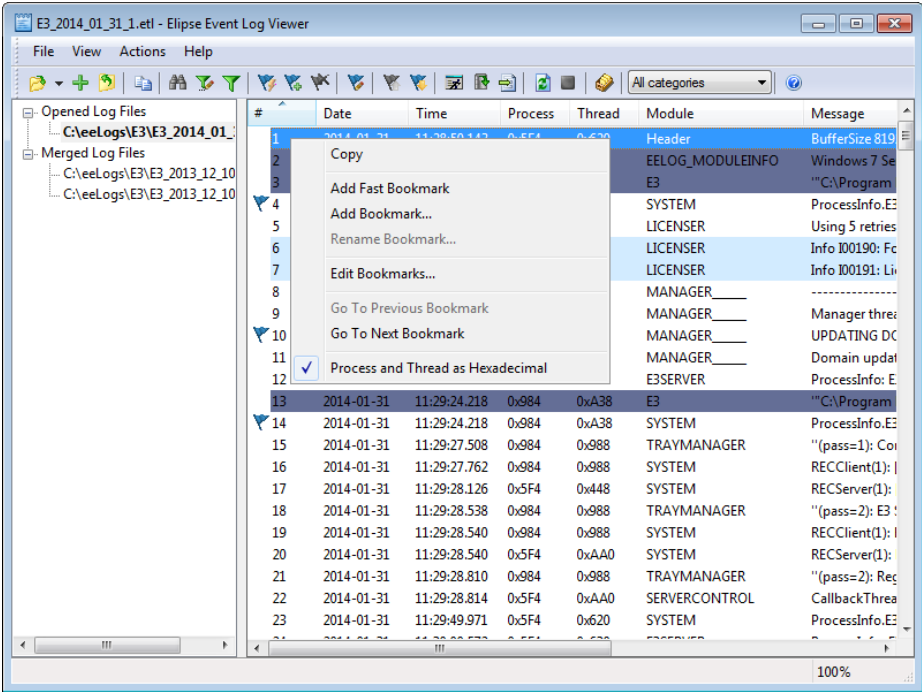
This window displays a list with all existing bookmarks and the events linked to them. The available options on this window are described on the next table.

Available options on the Edit Bookmarks window

OPTION	DESCRIPTION
Rename	Renames the selected bookmark on the list displayed on the window. A window asking for a new name is then displayed.
Remove	Removes the selected bookmark on the list displayed on the window.
Remove All	Removes all bookmarks.

OPTION	DESCRIPTION
Go To	Selects the event linked to the selected bookmark, on the event viewing area, without closing the edition window.
Close	Closes the bookmark's edition window.

All operations performed on this window are automatically applied. When right-clicking an event, a contextual menu is displayed with the options displayed on the next figure.



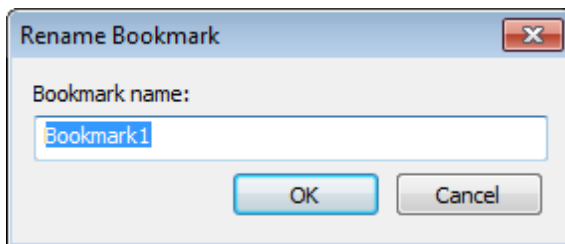
Contextual menu of an event

Contextual menu options of an event

OPTION	DESCRIPTION
Copy	Copies the selected events to the Clipboard. The selection performed in the Process and Thread as Hexadecimal is kept during the copy operation.
Add Fast Bookmark	Adds a bookmark with an automatically generated name to all selected events.
Add Bookmark	Opens a window to ask for a bookmark name, and adds it to all selected events.
Rename Bookmark	Renames the selected bookmarks.
Edit Bookmarks	Opens a window to edit the bookmarks.

OPTION	DESCRIPTION
Go To Previous Bookmark	Selects the previous bookmark.
Go To Next Bookmark	Selects the next bookmark.
Process and Thread as Hexadecimal	Allows selecting whether the view of Process and Thread columns is displayed in hexadecimal (default) or decimal format. This option is preserved per user and it is also used when exporting events .

When clicking the **Rename Bookmark** option, the window on the next figure is displayed.




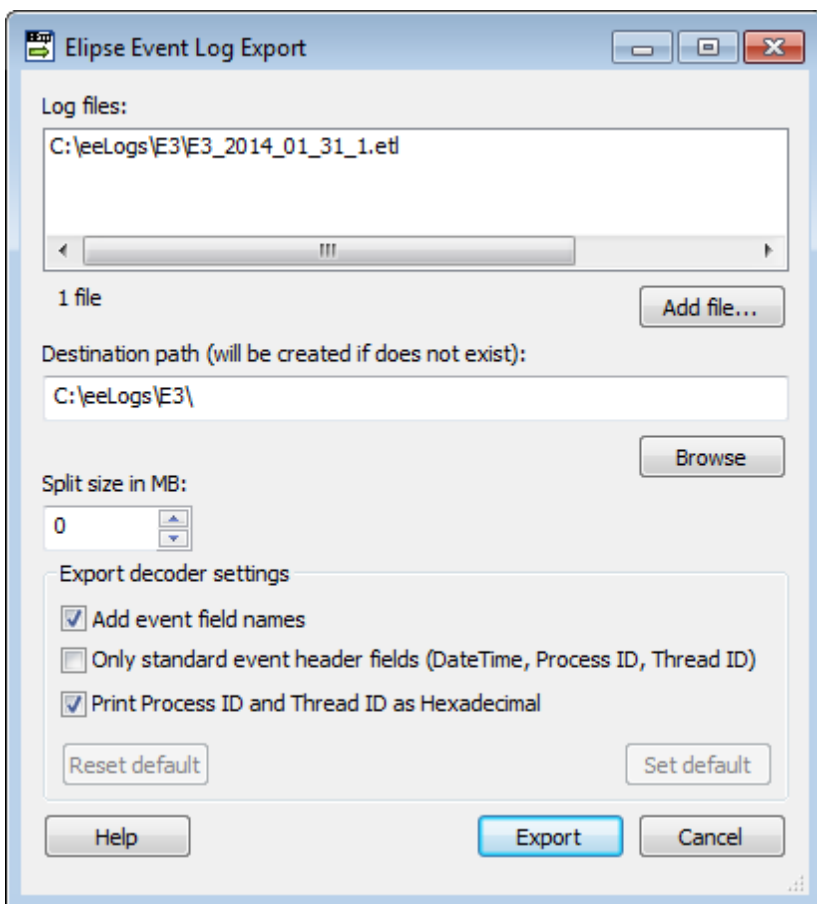
Rename Bookmark window

In the **Bookmark name** field, users must type a new name for the bookmark. This option is valid for single and for multiple selections, allowing several events to be grouped under the same bookmark name.

Eclipse Event Log Export

It is possible to export files in .etl format to a text file for printing, as well as for manipulation by another program. This is performed by using a tool called **Eclipse Event Log Export**. To use this option, follow these procedures:

1. In Log Viewer, select the **Actions - Export Events** menu, click , or else directly select the **Start - Programs - Eclipse Software - Eclipse Event Log - Log Export** menu. If the **Merged Log Files** node is selected, all data from open events is exported in this option.
2. The window on the next figure is then displayed.



Window for exporting events

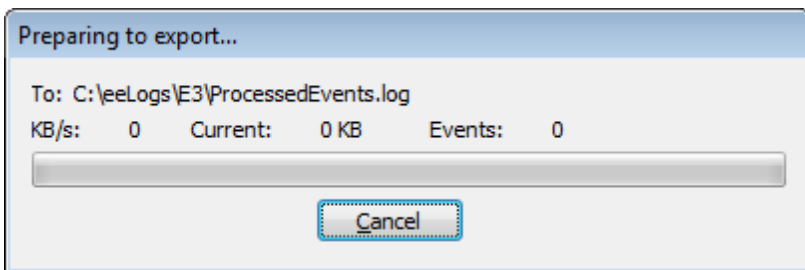
The available options are described on the next table.

Available options for exporting events

OPTION	DESCRIPTION
Log files	Lists the selected files for export. To delete any of them, select it and press the DELETE key.
Add file	Allows adding other files to the list for export.
Destination path (will be created if does not exist)	Determines the destination folder for export. This folder is created if it does not exist. If no directory is specified, the current path of log files is used.
Browse	Allows selecting another destination folder.
Split size in MB	Splits the final file into several files, according to the selected size.
Add event field names	The events are exported in full mode, containing event's name and value. The default value of this option is selected.
Only standard event header fields (DateTime, Process ID, Thread ID)	Only the most important fields are exported. The default value of this option is not selected (all fields are exported).
Print Process ID and Thread ID as Hexadecimal	Allows selecting whether Process and Thread columns are exported in hexadecimal or decimal format. The default value of this option is selected.
Reset default	Returns the export configurations back to their default (the Add event field names field selected, the Only standard event header fields field not selected, and the Print Process ID and Thread ID as Hexadecimal field selected).
Set default	Saves the current export configurations.

When more than one file is selected for export, the name of the file is ProcessedEvents.log. When only one file is selected for export, the name of the file is the same, but its extension changes to .log.

After configuring this option, click **Export**. The window on the next figure is opened when event export starts.



Export events progress window

Depending on the size of the files to export, this may be a time-consuming task, because files are read from the beginning to the end and then sorted before the export process of events starts.

3.1 Command Prompt Options

Elipse Event Log Export can be used on a command prompt. The usage format of the program is the following:

```
> eeLogExport.exe [- | /] [function | command] <arguments>
```

The options for the *function* parameter are described on the next table.

Available options for the function parameter

FUNCTION	DESCRIPTION
s <file1.etl; file2.etl>	File or files to export. Files separated by semicolons are merged.
d <folder>	Specifies an output folder for the exported log files. If this folder does not exist, it is created. If this parameter is omitted, the current path of log files is used.
x <schema.xml>	Uses a file in XML Schema format with the specification of the export format.
split <n>	Splits the results of log export into several files, decoded with <i>n</i> megabytes.
splitb <n>	Splits an .etl file into several files with <i>n</i> megabytes each, without decoding them.
p <n>	Stops splitting a file when reaches the <i>n</i> value, which is the amount of files to create. This option can only be used together with the <i>splitb</i> parameter.
fts <dd/MM/yyyy HH:mm:ss>	Starting date of the events to export.
fte <dd/MM/yyyy HH:mm:ss>	Ending date of the events to export.
stop <LoggerName>	Closes a log section, specified by the <i>LoggerName</i> argument.

FUNCTION	DESCRIPTION
stoplogdir <directory>	Recursively stops all open log sessions, starting at the path indicated by <i>directory</i> . NOTE: This action cannot be undone.

The options for the *command* parameter are described on the next table.

NOTE: Some of the following commands, to be executed, need a user belonging to the Windows group **Administrator** for Windows XP and Windows Server 2003 operating systems. For Windows Vista or later operating systems, this process must be executed with higher privileges, by using the **Run as Administrator** option.

Available options for the command parameter

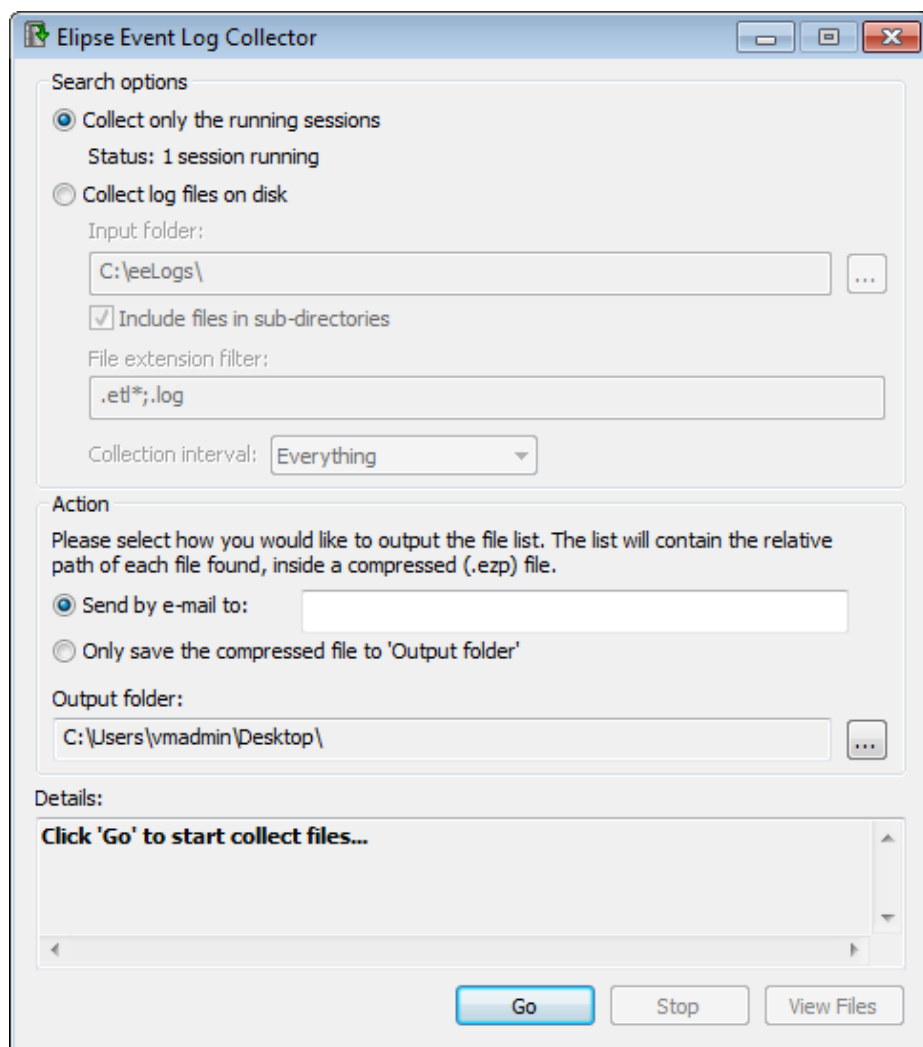
COMMAND	DESCRIPTION
? or help	Displays a message box with a help text about the command line options.
show	Forces a display of Elipse Event Log Export settings window.
install	Links files with .etl extension to Elipse Event Log Export, so that these files can be opened in Windows Explorer by double-clicking them. This must be executed as Administrator.
uninstall	Removes the Elipse Event Log Export link to files with an .etl extension. This must be executed as Administrator.
q	Quiet mode. It does not display a dialog box with error messages.
queryall	Displays a window with all active log sessions. Selecting the check box near the name of the session and clicking Stop allows closing that session. This must be executed as Administrator. When right-clicking a session, the Session Name to Clipboard (copies the session name to the Clipboard) and Full File Path to Clipboard (copies the full path of the session file to the Clipboard) options are presented.
singleton	Avoids that several instances of the same process in which Elipse Event Log Export is running are opened.

Elipse Event Log Collector was created to automate the process of sending logs to Elipse. With the collector, users need almost no configuration, since the program already executes all the necessary steps, according to the type of file to collect (.etl, .log, or any other file extension) and generating at the end of the collect process a compressed file, supported by any program that decompresses files in ZIP format.

NOTE: Starting with version 4.5 build 60 of Elipse Event Log Collector, users must install **Elipse Event Log Tools**.

4.1 Collecting Logs


When executing Elipse Event Log Collector, the dialog box on the next figure is opened.




Elipse Event Log Collector's main window

The available options on this window are described on the next table.

Available options for Elipse Event Log Collector

OPTION	DESCRIPTION
Search options	<p>Allows selecting how files are collected:</p> <ul style="list-style-type: none"> • Collect only the running sessions: Log collection is performed only on open log sessions • Collect log files on disk: Allows selecting log files to collect, by using the Input folder option <p>Regardless the selected mode, collected files are serialized (if supported by the API and by the log session) to the next value on the daily sequence.</p>
Input folder	<p>Informs the directory from where the log files must be retrieved. It is initially filled in with parameters configured on log storage, so that it is possible to determine where logs are currently generated. To select a directory, click  or use the key combination ALT + I.</p>
Include files in sub-directories	<p>Indicates if the collect process must be performed by searching files on sub-directories.</p>
File extension filter	<p>Informs what file extensions must be collected.</p>
Collection interval	<p>Allows selecting a time interval to collect logs. The available options on this combo box are the following:</p> <ul style="list-style-type: none"> • Everything (all logs) • Last 24 hours • Last 7 days • Last 30 days • Last 365 days • Custom range (logs from a specific date) <p>When selecting the Custom range option, users can choose a specific date to collect the logs.</p>
Action	<p>Informs the output type of the log collector. If the selected option is Send by e-mail to, the result of the log collect, after saved to the output folder, is sent by e-mail to the address informed on this option. If the option is Only save the compressed file to 'Output Folder', the generated file is only saved to the output folder.</p>

OPTION	DESCRIPTION
Output Folder	Indicates the output directory where the compressed log file is saved. Regardless of the option selected in Action , a copy of the compressed file is always saved to that directory. To select a directory, click  or use the key combination ALT + O.
Details	Shows information about the progress of the process of collecting log files.
Go	Starts collecting log files.
Stop	Stops collecting log files.
View Files	Allows viewing what log files were found, according to the Input file options and File extension filter options. If compression is successful, this list matches the list of compressed files.

NOTE: Changes on the parameters of the **Input file options** option must be performed carefully, because this action determines from where the collector retrieves those files. It is only advised to change these values under technical recommendation by Elipse Software.

When collecting files with an .etl (*Elipse Trace Logs*) extension that are in use, the program automatically flushes in-memory events (flush of event buffers), preventing loss of information.

Flushing in-memory events to disk only happens when the files to collect are on the same computer where Elipse Event Log Collector is running. A collecting executed on remote computers has no way to perform flushing events on the other computer, although they are collecting files written to disk. The generated output file is always named CollectedLogs.ezp. When starting a new collect process, if there were a previous file on the same output directory named CollectedLogs.ezp, this file is erased and a new one is created.

If the disk unit where the CollectedLogs.ezp file is generated has less than or equal to 5 MB free space, the collector does not start the collect process. If collecting has already begun, it is stopped when reaching this limit.

If the **Send by e-mail to** option is selected, at the end of the collect process a window is opened to send the e-mail. The collected file is then attached to it.

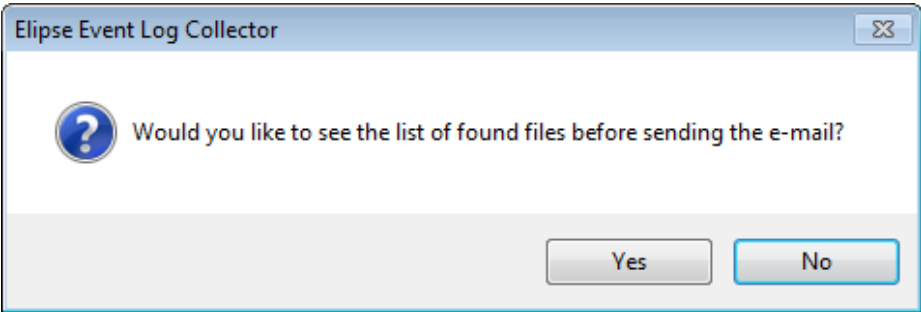
If there is no e-mail client configured or compatible, or any other error has occurred while preparing the message, the file is not sent. In this case, users must send this file manually using an e-mail client (or a webmail). Depending on the size of the generated file, it may be necessary to send it via physical media, such as a CD or DVD, to Elipse Software.

NOTE: For Elipse Event Log Collector to open an e-mail message, users must have an e-mail client compatible with Microsoft Simple MAPI (*Microsoft Simple Message API*), a protocol used by the collector to create a call to an e-mail client that generates the message.

Any error due to search option parameters, access rights to output folders, insufficient disk space (less than 5 MB), users aborting the collect process, or any other error, prevents the CollectedLog.ezp final file to be generated.

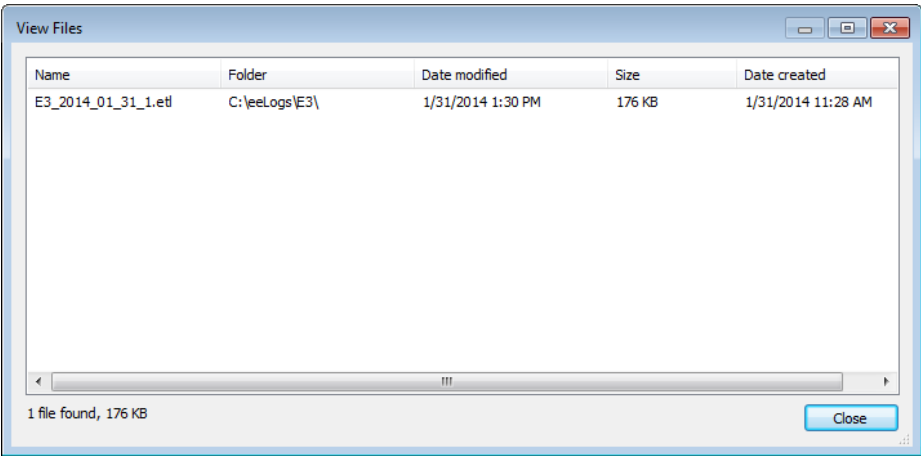
While the collect process is running and the output file is being generated, its name has a __tmp suffix, therefore it is named CollectedLogs.ezp__tmp. This file is renamed at the end of the collect process to CollectedLogs.ezp.

If the option to send by e-mail was selected, a message is displayed asking whether the list of collected files should be displayed before sending it.



Message asking to display a list of collected files

By clicking **Yes**, a list is displayed with all files added to the file CollectedLogs.ezp.



List of added files

Next, the e-mail is configured to be sent, using the default e-mail client of the machine where Elipse Event Log Collector is installed.

4.2 Contents of CollectedLogs.ezp File

The CollectedLogs.ezp file is generated using the PKZIP format, and can be opened by any program that also decompress the ZIP format.

At least there is one eeLogCollector_Readme.txt file inside the CollectedLogs.ezp file. This file contains all records of the executed collect process, even if the collect process did not find or add files. This is important to inform what was collected.

For operating systems beginning with Windows XP, Elipse Event Log, since version 4.0, creates a user on the local machine during the installation process, named **eeLogs**, and adds it to the **Performance Log Users** group. This user is needed by Elipse Event Log to control log sessions created by processes without administrator privileges on the machine. These new policies comply with Microsoft recommendations to allow granting special rights to processes or users without privileges, aiming to improve system security against malicious users.

But if this user is modified (that includes deleting or editing its parameters), possibly the logs may not have access to session control, because of the differences between edited and required configurations, thus leading to event losses. Therefore, it is not advisable to change these settings.

To restore default user settings, users can force the creation of a user by running the log service installation, eeLogSvc.exe, on a command prompt using the **eeLogSvc.exe /i** command.

For security reasons regarding the computer in which the Elipse Event Log user was created, this user is as limited as possible, granting only the minimum privileges needed for logs. The following grant restrictions are applied to the **eeLogs** user:

- **Deny access to this computer from the network**
- **Deny log on locally**
- **Deny log on through Remote Desktop Services**



Headquarters

Rua 24 de Outubro, 353 - 10º andar
90510-002 Porto Alegre
Phone: (+55 51) 3346-4699
Fax: (+55 51) 3222-6226
E-mail: elipse-rs@elipse.com.br

Taiwan

9F., No.12, Beiping 2nd St., Sanmin Dist.
807 Kaohsiung City - Taiwan
Phone: (+886 7) 323-8468
Fax: (+886 7) 323-9656
E-mail: evan@elipse.com.br

Check our website for information about a representative in your city or country.

www.elipse.com.br

kb.elipse.com.br

forum.elipse.com.br

www.youtube.com/elipsesoftware

elipse@elipse.com.br



Gartner, Cool Vendors in Brazil 2014, April 2014.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability of fitness for a particular purpose.

Microsoft Partner
Gold Independent Software Vendor (ISV)