Event Log Explorer

Event Log Explorer Viewer user guide
Event Log Explorer Tools

Table of Contents

1. Introduction

Event Log Explorer is an effective software solution for viewing, analyzing and monitoring events recorded in Microsoft Windows event logs. Event Log Explorer greatly simplifies and speeds up the analysis of event logs (security, application, system, setup, directory service, DNS and others).
Event Log Explorer extends the standard Windows Event Viewer functionality and brings many new features

Main features of Event Log Explorer Viewer

Viewing "live" event logs and event log files
With Event Log Explorer you can open event logs and event log files. You can open modern (EVTX) and legacy (EVT) files.

Event tasks and templates
You can create tasks to quickly get certain events from specific computers or files and display them your in own way. You can also save your tasks as templates or use predefined task templates (e.g. Audit logons).

Merging different event logs into one view
You can unite several event logs (or event log files) in one log view. Such a consolidation view (Merger) may significantly simplify the process of analysis. You can have as many number of different mergers as you wish.

Tabbed-document or multiple-document user interface depending on user preferences
Event Log Explorer provides you with 2 user interface types. Multiple-document interface (MDI) allows you to open different event logs and place them all inside the main window of Event Log Explorer. Tabbed-document interface (TDI) allows you to open f event logs and features the best way of navigation between logs.

Favorites computers and their logs are grouped into a tree
With Event Log Explorer you can view event logs on different computers. For your convenience you can group your computers in a tree. Then you can simply select the desired event log from the desired computer, and it will be opened immediately.

Event descriptions and binary data are in the log window
Unlike standard Windows Event Viewer, Event Log Explorer allows you to view the description and binary data of each event without additional commands. All descriptions are displayed in the Event Description box of log window. You can close this box if you don't need to read event descriptions. You can also display event descriptions in the event list as a column.

Custom columns to display any event data
You can create a custom column to display event details from XML representation of the event. E.g. you can display file name in a column for file system events.

Event list can be sorted by any column and in any direction
Event Log Explorer allows you to sort event list by any column - just click on the column header, and event list will be re-sorted immediately. If you click on the column twice - the event list will be resorted in the backward direction.

Advanced filtering by any criteria including event description text
You can easily filters events in the list by any criteria. The criteria are reusable - you can save them as a file and apply for another event logs.

Quick Filter feature allows you to filter event log in a couple of mouse clicks
It is very easy to filter event log by a single column value. Simply click right mouse button on a cell that will be considered as a filter criteria and you will be prompted to filter on this criteria. E.g. if you click in column "Type" on a cell "Information", you can set a quick filter on Type="Information" criteria.

Log loading filter to pre-filter events
You can pre-filter event log when it's opening. This will increase performance and make log view clear.

Fast search by any criteria
You can easily search for event that meets a certain criteria. Just use Find command to start search. To find a next event that meets this criteria, please use Find Next command.

Fast navigation with bookmarks
Bookmarks allow you to mark an event in Log View and then you can easily return to this event.

Sending Event Log to printer
With Event Log Explorer can print event logs. Print options let you select from several styles of print.

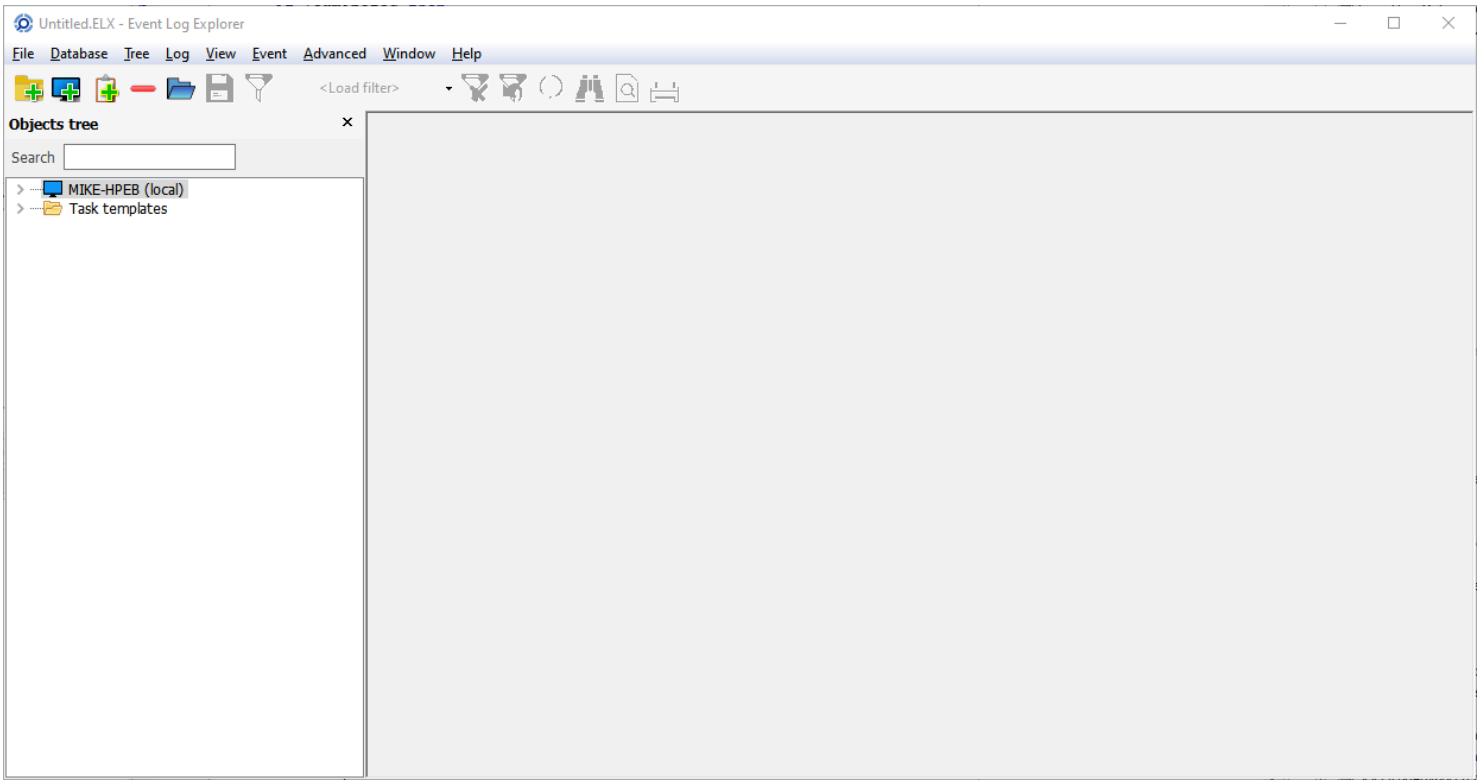
Analytical reports
OLAP cube helps you build different reports for multidimensional analysis and visualize your data in charts.

Export log to different formats
You can export your event logs to other formats e.g. HTML, text or Excel.

2. Quick Start

Opening Event Logs

When you start Event Log Explorer first time, you will see an empty log view area and computer tree with your local computer.



To open an event log from your local computer, click on › near the computer name in the computer tree. This will expand the computer node to show all event logs available. Double click on the log name you want to display - this log will be opened in the log view area.
To open en event log from a remote computer, add this computer to the computer tree. To add a computer to the tree, select **Tree->Add computer** from the main menu or just click  . When the computer appears in the tree, expand it and double click on the required event log.

Opening Event Log Files

To open an event log file select **File->Open Log File** or click  . Browse for your file and click OK.

Viewing Event Properties

To display event properties for a specific event, just double click this event. You will see the Event Properties dialog. Switch to XML tab to display an XML representation of the event. Note that the XML is not available for legacy event log files (EVT).
To close Event Properties dialog, just press Close button. If you close a log view, the corresponding Event Properties dialog will be closed automatically.

Export Event Log to Excel Document

To save current event log view in Excel document, select **File->Export** from the main menu.
Select Excel in **Export to** group and click Export button.

3. Event Log Explorer Concept

Workspaces

Event Log Explorer Viewer has a document-oriented architecture. Event Log Explorer Viewer documents are called workspaces. When you start the application first time, it automatically creates an empty workspace Untitled.
Workspaces store Computers tree and Opened event log views including layout, filters, etc. Workspaces don't store Event Log Explorer Preferences and User credentials. All global options and preferences are stored in the user's registry. Credentials are stored in a separate file shared with the other Event Log Explorer program components (Elodea event collector).
If you maintain a large-scale network, it's a good idea to have different workspaces for different group of servers. To open a certain workspace, use **File->Open Workspace** command. To save workspace use **File->Save Workspace** or **File->Save Workspace As**.

Objects Tree

Objects Tree is designed to provide you with quick access to event logs. You can add any number of computers to the tree and group them for better usability. When you click on the › sing near the computer name, the application displays all event logs available on this computer - double click on the log opens the event log immediately.

Events loading

When you open an event log with Event Log Explorer Viewer, it loads events into an internal local storage and then displays them in a log view. This provides high performance of further operations like filtering, sorting, searching, exporting etc. From the other hand, if new events appeared in the event log after loading, they will not appear on the screen and you will have to refresh the log view to reload events.

Log Views

Log view is a visual representation of event log or event log file. The log view displays a scrollable event list, description box, top lbar and some other controls. You can open as many log views as you wish. Depending on the user interface style, log views are presented either as MDI child windows (for multiply document user interface) or as tabs (for tabbed document user interface). Active log view is the topmost log view (for MDI) or the active tab (for TDI).
All main menu commands for event log management apply to active log view only.

Tasks

Event task is a special entity which defines what events will be picked, which computers from and how they will be displayed. To create a task, use **Tree->Create Task** command. Technically, a task specifies an XML query to get events and a list of computers the events will be collected from. It also defines list of columns to displays, sorting order etc. Tasks are stored in the workspaces and can be saved as files. Event Log Explorer Enterprise Edition lets you schedule export of task events into different formats (PDF, Excel, HTML, Text).

Event Type

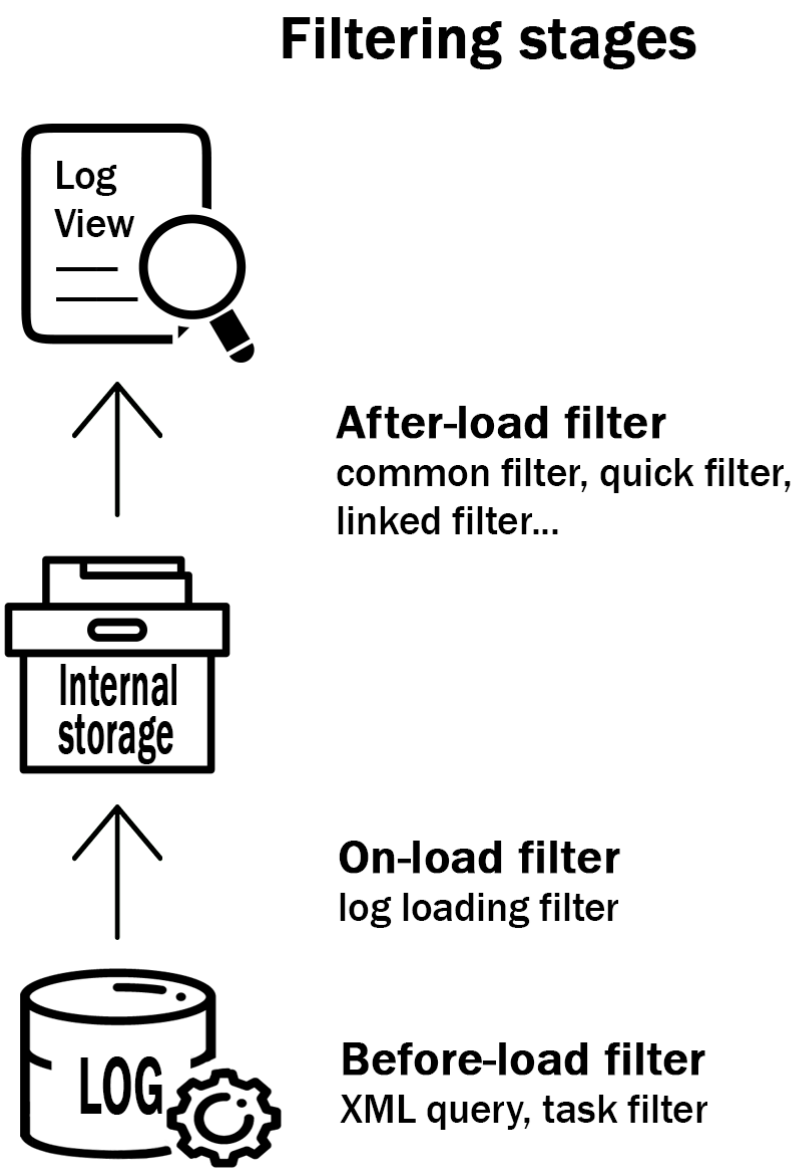
In Windows, Event Type column exists in legacy event logs only. Modern Windows event logs don't have this column. Instead of Event Type, event logs use Level and Keywords columns. However Event Log Explorer still use "virtual" Event Type column as follows:
For security event log, Event Type is either Audit Success or Audit Failure depending on the Keywords value.
For other event logs, Event Type reflects the Level column.

Database

Event Log Explorer Viewer can view events saved by Elodea Event Collector in a database. It lets you manage the database events in a similar way as you manage general events. It also lets you save events into a database without using Elodea Event Collector. For more information about Elodea Event Collector see Event Log Explorer Elodea User's Guide (available for Enterprise Edition users only).

4. Filtering Events

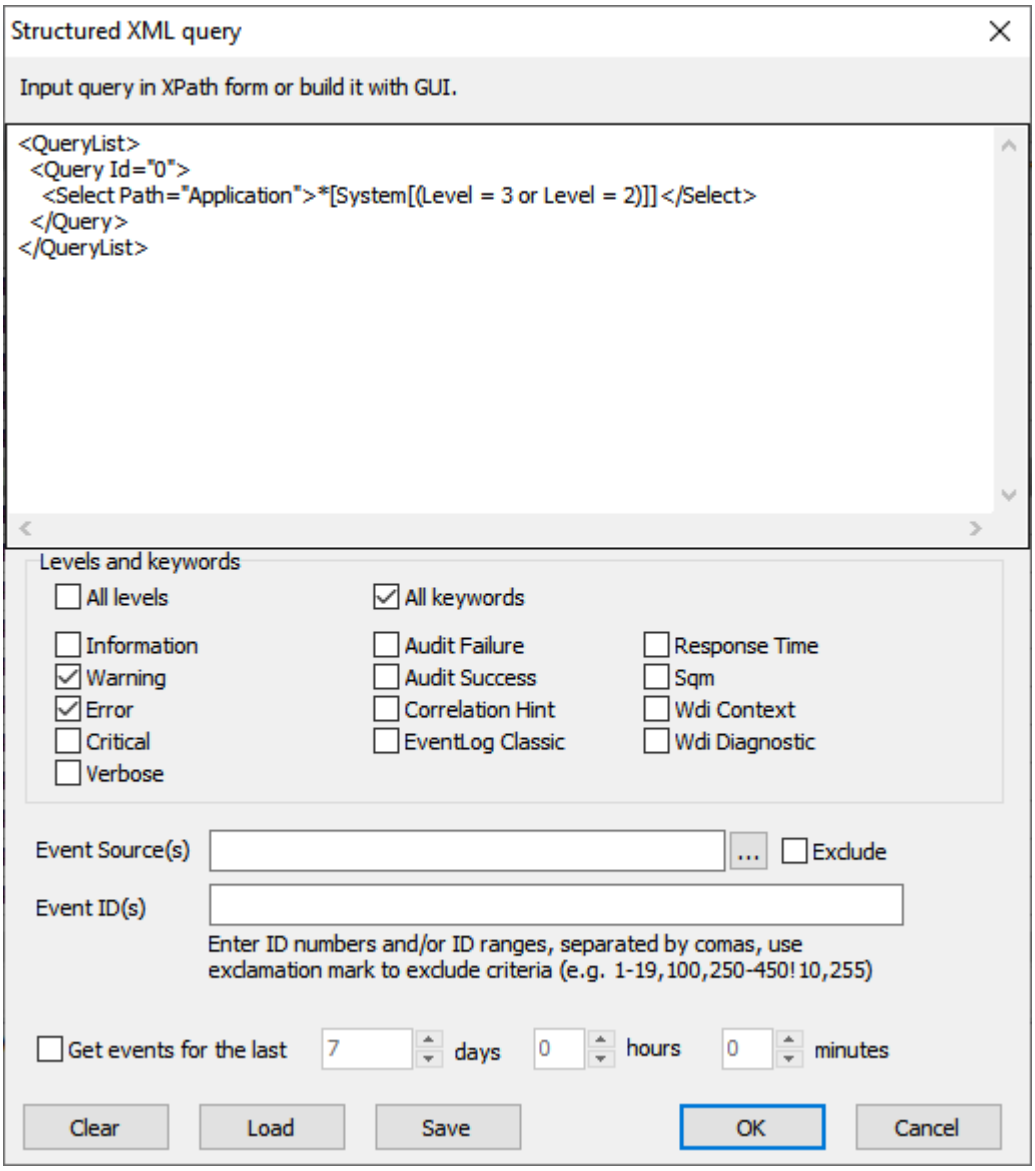
There are several ways to filter events with Event Log Explorer Viewer. You can query only specific events using XML queries, and the filtering will be performed by Windows Event Log Service on the target machine (before-load filter). You can also filter events when it loads events (on-load filter) and you can filter loaded events (after-load filter).



Before-load filter is applied on the target machine and reduces network load.
On-load filter is applied during event loading process - when Event Log Explorer receives events, but before saving the events into the internal storage.
After-load filer is applied to the events saved into the internal storage.

4.1. XML Query Filter

XML Query Filter is a before-load filter.
Select Log->XML Query from the main menu to create or change XML Query filter.

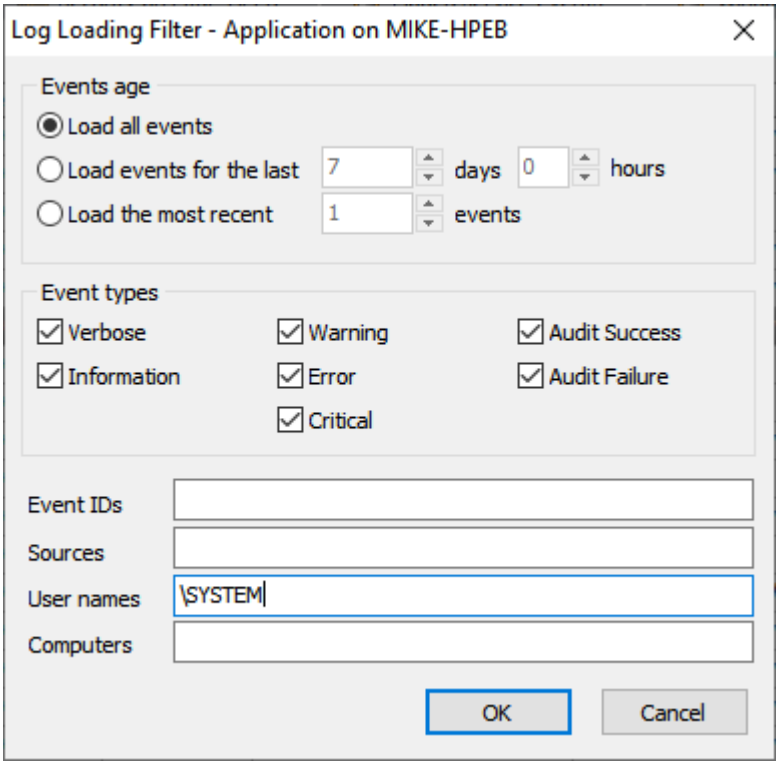


You can input XML query manually or use user interface to build the query.

Load button loads a query from an XML file. If it appears that the loaded XML file is a task or a task template, Event Log Explorer parses this file and loads the XML query from this task.

4.2. Log Loading Filter

Log loading filter is an on-load filter that prefilters events during loading process.
You can pre-filter events by event age, event types, user names and other parameters.
To set/change log loading filter for an active view, select Log->Log Loading Filter from the main menu.



You can also set log loading filter globally. Use Preferences dialog to change log loading filter globally.

4.3. General Filter

General filter is a common way to filer events. It is an after-load filter and lets you change filtering conditions without events reloading.
To filter events in an event log view, select Log->Filter from the main menu. This will open Filter/Search window. Enter your criteria in this window and press OK to apply the filter.
You cannot apply general filters one by one. You should change your current filter criteria if you want to narrow displayed event list. To change the filter criteria, open Filter/Search window again and modify the displayed filter criteria.
When you refresh the event list, general filter will be re-applyed after log reloading.
To clear filter, select Log->Clear Filter.

4.4. Quick Filter

Quick Filter is a comfortable way to filter event list by a single criterion.
To set a filter, find an event that meets your criteria, then click right mouse button on the cell of this event that you consider as the "criterion cell". The Event List context menu will appear.
The following quick filter criteria are available:
Column Name = Selected Value
Column Name <> Selected Value
Date >= Date of the current event (option is available if the user pops menu up from the Date column).
Date <= Date of the current event (option is available if the user pops menu up from the Date column).
Date&Time>= Date&Time of the current event (option is available if the user pops menu up from the Time column).
Date&Time <= Date&Time of the current event (option is available if the user pops menu up from the Time column).
You can apply quick filters one by one - this lets you to narrow displayed list easy and clearly.

When you refresh the event list or set a new "non-quick" filter, all quick filters will be cleared!

To clear quick filters, select Log->Clear Quick Filters or Log->Clear Filter.

4.5. Linked Event Filter

Linked event filter helps you to automate linking events by custom fields and filter them.
To start using Linked filter you should add custom columns to the list.
To display Linked Event Filter dialog select Advanced->Linked Event Filter from the main menu.

Example

Sometimes Windows or other software generate several events for one logical operation. E.g. "file delete" operation generates a set of linked events in Windows security event log:
1) Object handle requested;
2) Attempt to access the object;
3) Object Deleted;
4) Object Closed.

If you need to display all Object Deleted events, you should filter Windows security log by Event ID = 4660.
A typical description of Event 4660 is as follows:

An object was deleted.
Subject:
Security ID: S-1-5-21-2153856534-97633110-1224965316-1000
Account Name: Michael
Account Domain: TEST
Logon ID: 0x22183
Object:
Object Server: Security
Handle ID: 0xc04
Process Information:
Process ID: 0x930
Process Name: C:\Windows\explorer.exe
Transaction ID: {00000000-0000-0000-0000-000000000000}

As you can see, it does not list object name, so you don't know what file was deleted.
But it contains Handle ID of the object. Previous events (4663 and 4656) let you resolve object name from handle.
E.g. Event 4656:

A handle to an object was requested.
Subject:
Security ID: S-1-5-21-2153856534-97633110-1224965316-1000
Account Name: Michael
Account Domain: TEST
Logon ID: 0x22183
Object:
Object Server: Security
Object Type: File
Object Name: C:\TEST\File.txt
Handle ID: 0xc04
Process Information:
Process ID: 0x930
Process Name: C:\Windows\explorer.exe
Access Request Information:
Transaction ID: {00000000-0000-0000-0000-000000000000}
Accesses: DELETE
ReadAttributes

Access Reasons: DELETE: Granted by D:(A;ID;0x1301bf;;;AU)

ReadAttributes: Granted by D:(A;ID;0x1200a9;;;BU)

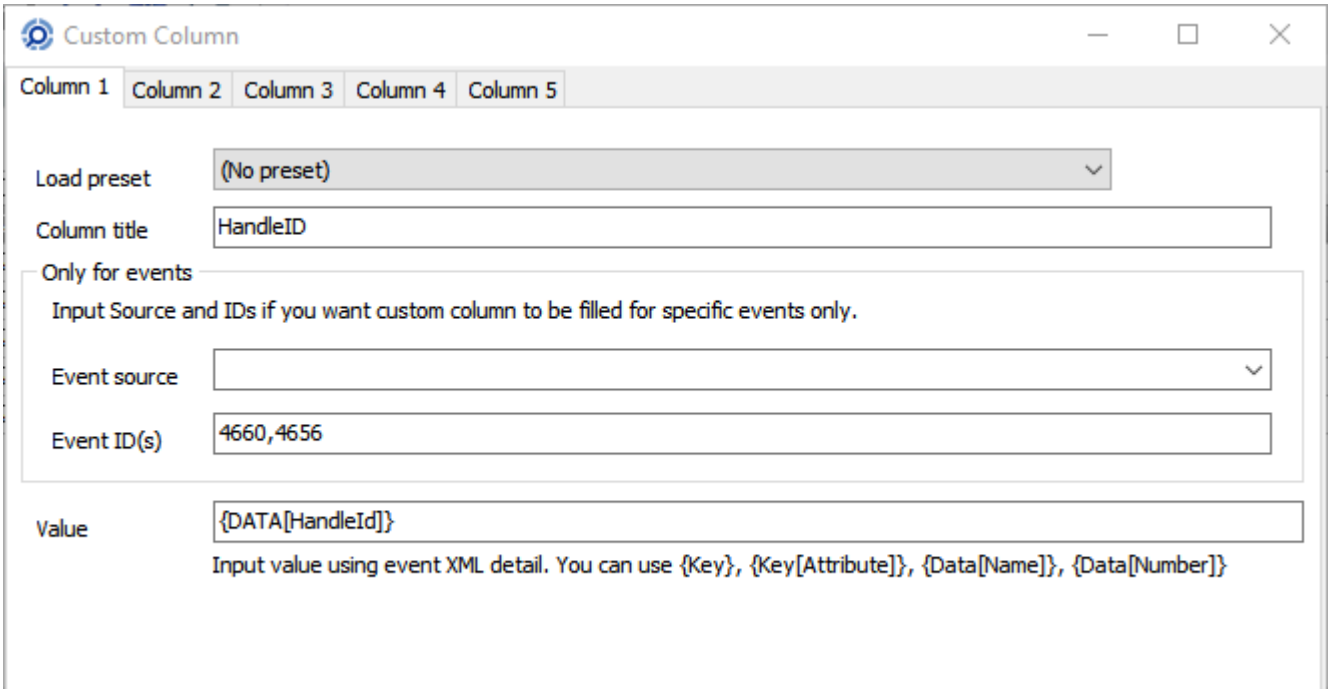
Access Mask: 0x10080
Privileges Used for Access Check: -
Restricted SID Count: 0

Here you can see that Handle ID:0xc04 is "C:\TEST\File.txt"

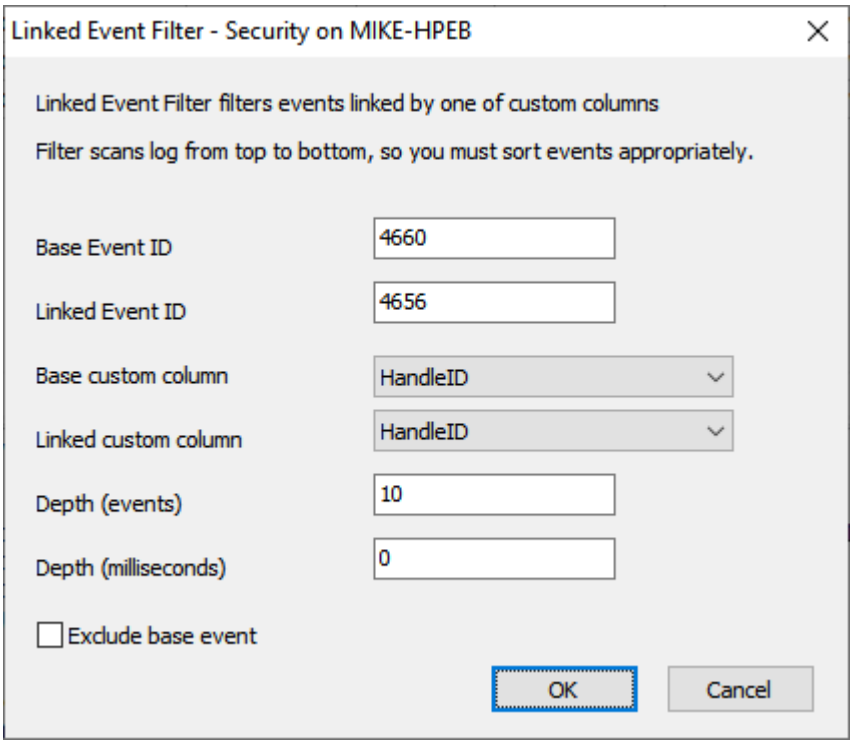
You might notice that event 4663 already contains Accesses: DELETE and you could filter by "Event ID = 4656" and "Description contains "Accesses: DELETE". However you should not rely on 4656 or 4663 events - file system may just prohibit file removal and you will get inaccurate result.

Linked Event Filter helps you to automate linking events by event id and description data and filter them.

First you need to create custom columns for events 4660 and 4656. It is enough to create only one custom field since Handle ID has the same field name (HandeID for both events).



To display Linked Event Filter dialog, select **Advanced->Linked Event Filter** from the main menu.
Base Event ID defines base (bearing) event ID. For the example above, it would be ***4660***.
Linked Event ID defines event ID of linked events. It would be ***4656*** (or 4663) for our example.
Base custom column and **Linked custom column** define custom column names to link. In our example it's the same custom column.
Depth (events) and **Depth (milliseconds)** define scan depth for linked event from the base event. Typically it should not exceed 10 events.
Exclude base event - if enabled, base event will not be displayed in the filtered view (only linked events will be displayed).



How it works

1. Event log view is scanned from top to bottom (this means that commonly you should sort events from newest to oldest).
2. When the **base event** found, the program gets a base value of the base custom column value and starts an inner scan for the linked custom column with the same base value. This inner scan is limited by **depth**.
3. If the linked event was found, it will be displayed in the result set. Base event will be displayed unless **Exclude base event** was checked.

Notes:

Linked event filter works slowly, so you may need to prefilter event list before using linked filter.
Event Log Explorer does not save linked filter into the workspace file.

5. Searching for Events

Search for events is similar to setting a general filter. You use the same Filter/Search dialog to specify search criteria. To open Search dialog, select **Log->Find** command from the main menu (or press Ctrl+F). Type search criteria and press OK. Event Log Explorer starts searching from the current (selected) event. When it finds an event that matches search criteria, it selects this event. To continue searing, select **Log->Find next** from the main menu (or press F3).

6. Custom Columns

Custom columns allow you to add your own columns to the event list.
This feature is mostly helpful for Security event logs when you need to display some information from the event description, e.g. Account name, User logon name, file name, process name etc.
To display Custom column dialog box, select **View->Custom Columns** from the main menu of the program or right click on a column title in the event list and then select Custom Columns.
Just click on **Colmn#** (# is a column number) in the top of the dialog to add a specific column.
Load preset fills the column from a saved preset.
Column title. Input the display name of the column.
Event source, Event ID(s). Input source name and Event IDs for which custom column will be calculated. If you leave these fields empty, Event Log Explorer will try to calculate custom column for each event.
Value. Input how Event Log Explorer will calculate value of the custom column. **Value Helper** helps you to select the right value from the list of available values.
You should use column identified from the event XML representation.

Let's take an event sample:

- **System**
  - **Provider**
    - [**Name**] Microsoft-Windows-Security-Auditing
    - [**Guid**] {54849625-5478-4994-a5ba-3e3b0328c30d}
  - **EventID** 4660
  - **Version** 0
  - **Level** 0
  - **Task** 12800
  - **Opcode** 0
  - **Keywords** 0x8020000000000000
  - **TimeCreated**
    - [**SystemTime**] 2021-04-24T20:46:25.3457085Z
  - **EventRecordID** 838914
  - **Correlation**
  - **Execution**
    - [**ProcessID**] 4
    - [**ThreadID**] 2256
  - **Channel** Security
  - **Computer** MIKE-HPEB
  - **Security**
- **EventData**
  - **SubjectUserSid** S-1-5-21-2670916313-2975000581-3514835237-1001
  - **SubjectUserName** Michael
  - **SubjectDomainName** MIKE-HPEB
  - **SubjectLogonId** 0x1bb7b8
  - **ObjectServer** Security
  - **HandleId** 0x1144
  - **ProcessId** 0x259c
  - **ProcessName** C:\Windows\explorer.exe
  - **TransactionId** {00000000-0000-0000-0000-000000000000}

To get fields under the System node, just use the key name in the curly brackets {}. E.g. to get Keywords, just use **{Keywords}**. To get values of the keys with attributes, add the attribute name in the square brackets []. E.g. to get ProcessID, use **{Execution[ProcessID]}**.

To get fields under EventData or UserData nodes, use **{DATA[Index]}** where Index is either a number of the value under EventData/UserData node or a value name under EventData node. E.g. to get ProcessName in the example below, use **{DATA[8]}** or **{DATA[ProcessName]}**.

You can get several parameters in one field. E.g. if you want to display user name as DOMAIN\ACCOUNT NAME, you should input the following Value:

{DATA[SubjectDomainName]}\{DATA[SubjectUserName]}
or
{DATA[3]}\{DATA[2]}

Formula (available in the Forensic or Enterprise editions of Event Log Explorer).
If checked, the value will be processed by the script engine. E.g. in the sample above, you the **ProcessName** specifies the full path to the process. If you want to see only file names in the event list, input the following Value:
ExtractFileName('{DATA[ProcessName]}')
This process works in 2 steps:
1. It resolves values in the curly braces, resulting in:
ExtractFileName('C:\Windows\Explorer.exe')

2. This line is then processed in the script engine.
The function ExtractFileName is defined as:
function ExtractFileName(FileName : String) : String;
It extracts the name of the parameter passed to this function. So it will return ***'Explorer.exe'***.

If you need a more complex script, define your own functions in file "\ProgramData\Event Log Explorer\Scripts\cfformulas.pas" and use them.

Refer to 'Scripting Reference' for more information about scripts.
Be aware that processing processing scripts is time-consuming, so calculating the custom columns with formulas may take long time for large logs.

Treat value as defines the type of the custom column value:

• **Text** - returns the value as is. Always use it when the result is a text-based or the value type is uncertain.
• **Integer** - Interprets the value as an integer. If the value cannot be converted to an integer, an empty value will be displayed.
• **Float** - Interprets the value as a floating-point number. If the value cannot be converted to a float, an empty value will be displayed.
• **Date & Time** - Interprets the value as a date & time value in the ISO 8601 format (e.g., yyyy-mm-ddThh:mm:ss.sssZ). While not all ISO 8601 variations are supported (e.g., 20240101), using a space instead of the 'T' delimiter (e.g., 2024-01-01 10:10:10) is allowed. Event Log Explorer displays such dates in the default date & time format. If the value cannot be converted to date & time, an empty value will be shown.

Test - calculates the custom column value for the current event and displays it.

You can also use a legacy custom column format from Event Log Explorer 4.x that based on event descriptions.
E.g., if you have an event description:

```
Special privileges assigned to new logon.

Subject:
    Security ID:        S-1-5-19
    Account Name:       LOCAL SERVICE
    Account Domain:     NT AUTHORITY
    Logon ID:           0x3E5

Privileges:             SeAssignPrimaryTokenPrivilege
                        SeAuditPrivilege
                        SeImpersonatePrivilege
```

To display **Account Name** in a custom column, use **{Subject\Account Name}**.

7. Tasks and Templates

Event task is a special entity which defines what events will be picked, which computers from and how they will be displayed. The tasks are stored in the workspace.
Task template is similar to task, but it doesn't define the computers to get events from. Templates are stored as files. Templates default location is "C:\ProgramData\Event Log Explorer\TaskTemplates". Event Log Explorer comes with a number of predefined templates.

7.1. Tasks

Technically, a task specifies an XML query to get events and a list of computers the events will be collected from. It also defines list of columns to displays, sorting order etc. Tasks are stored in the workspaces and can be saved as files. Event Log Explorer Enterprise Edition lets you schedule export of task events into different formats (PDF, Excel, HTML, Text).

To create a task, use **Tree->Create Task** command. The task wizard will appear.
Use Next and Back buttons to specify task parameters:

General page defines base task parameters: name, description, type of the task (event log or log file task), and the location of the task in the tree.
Computers page (available for event log tasks) defines the list of computers from from which you will get the events. If the list is empty, the local computer will be implied.
Logs page (available for event log tasks) defines the list of event logs from which you will get the events.
Log files page (available for event log file tasks) defines the list of evtx files from which you will get the events. You can add a folder to the list as well - in this case, Event Log Explorer will add all evtx files from this folder.
Filter page defines XML query. You can use UI to build query or just type the query manually.
Columns page defines the list of columns to display. You can also add custom columns to the list.
Start page lets you start the task when you click Finish button. It also suggests how to schedule the task to export events.

7.2. Task Templates

Task templates are very similar to tasks, but they don't contain computer list or log file list. Templates are stored separately as files in "C:\ProgramData\Event Log Explorer\TaskTemplates\" folder. Task templates are intended to create new tasks quickly based on the template.
To create a template, start creating a task. When the task is ready, click Save button arrow and select **Save as template**.

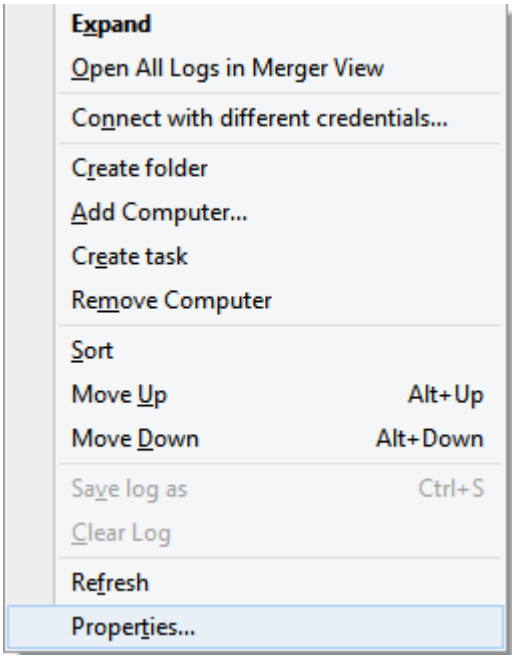
Task templates are listed in the Tree under Task templates node. When you double click on a template, Event Log Explorer creates a new task based on this template. You can also test a template without creating tasks. Click right mouse button on the template name and select **Test template locally**. This will run the task on your local computer.

8. Merging Events

Sometimes you may need to join events from different event logs in one log view. Event Log Explorer provides 2 ways of joining events:
1. Using tasks - create a task and specify which logs and from which computers are to be joined. See more in the Tasks chapter.
2. Using merger. Open an event log or event log file. Then click right mouse button on another log (log file) in the Tree and select **Merge with Current View** or select event logs (files) in the Tree, click right mouse button and select **Merge into a New View**.
This will create a new log view (Merger). On the log view top bar, you will see a merger icon (a stack of logs ) . When you hover mouse over this icon, you will see log names in the merger. Double click on the item displays Merger Properties dialog.

9. Tree Object Properties

When you click the right mouse button on an object in the Object tree, you can select Properties from the pop-up menu. Event Log Explorer displays Properties dialog depending on the type of object.



9.1. Computer Properties

To display Computer properties dialog, select the computer in the tree, click right mouse button on it and select Properties from the context menu.

Name - name of the computer. You can rename your computer in the tree by clicking on Rename button.
Description - description of the computer. The description will appear in the tree near the computer name in parentheses.
Folder - a tree folder that contains this computer.
Display event time in defines how Event Log Explorer will display event time.

9.2. Log Properties

To display the log properties dialog, select the log in the tree, click right mouse button on it and select Properties from the context menu. Alternatively click the right mouse button on the log view and select Log Properties.

Log file name - name of the log file and its location.
File size - size of the log file in kilobytes (and bytes).
File created - when the log file was created.
File modified -when the log file was modified. Note that due to caching you can see events generated after this time.
File accessed - when the log file was accessed.
Maximum log size - log file size will not exceed this value.
When maximum log size is reached:
Overwrite events as needed - when the log is full, the newest events will replace the oldest.
Do not overwrite events (clear log manually) - if the log is full, you should clear it manually. Note that non-administrative users will not be able to logon if the log is full.
Backup log automatically - log will be saved as a file and the emptied.
Clear Log - empties event log.

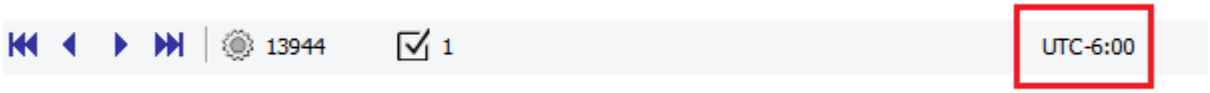
10. Merger Properties

Merger properties dialog lets you view and manage event logs in the merger. To display Merger properties, click right mouse button on a merger view and select Log Properties from the context menu.
Merger properties lists all the logs in the merger.
To remove specific logs from the merger, select them and press Remove button.
See also: Merging Events

11. Time Correction

By default, Event Log Explorer displays event time in your local time zone. In some cases, you may need to view event time in the other time zones. To change the time zone for a log view, select **Log->Time Correction** from the main menu.
You can also change the timezone for a computer - using Computer Properties dialog or for all event log files using Preferences dialog->Log Files.

Event Log Explorer always displays a current time zone in the top bar of the log view.



12. Color Coding

Color coding allows you to easily distinguish between different events.
To display Color Coding dialog box, select **View->Color Coding** from the main menu of the program.
Each event can be displayed with a certain foreground color, background color and a certain font style.
Use **Add** button to add a new color code, **Change** - to Change the code, **Remove** - to remove selected color code from the list and **Remove All** to clear the list of color codes.
Load button loads color codes from a file.
Save button saves the current color codes to a file.

13. Description Server

Event Log Explorer allows you to set a place where it will read event descriptions from.
By default Event Log Explorer reads event descriptions from the computer where the event log is located. Sometimes you may want to change the default location of the description server: when descriptions are not available from the default location or if getting the event descriptions from a remote server affect the performance.
To set the description server, select **Log->Description server**.
Default location - descriptions will be read from the default location (where the event log is located)
Local computer - descriptions will be read from the local computer (this ensures the best performance).
Another computer - descriptions will be read from a certain location.
Imaged computer - descriptions will be read from an imaged computer. This option is available only in Forensic Edition.

14. Connect with Different Credentials

When you try to open event log from a remove computer, Event Log Explorer uses your current credentials to access this log.
Sometimes you may need to connect a remote computer with different credentials.
If you have not enough permissions, Event Log Explorer displays Access-denied error and will prompt you to input the other credentials (user name and password).
You can also explicitly connect a remote computer with non-default credentials. Select the required computer in the tree, click the right mouse button and select **Connect with different credentials**.

See also: Credential Manager

15. Credential Manager

Credential manager is intended to store user names and passwords.
To open Credential manager, select **Advanced -> Credentials** from the main menu.
To add a new credential, click **Add** and input machine name, user name and user password.
To change an existing credential, click **Edit** button. To change several existing credentials, select several items in the list, then click **Edit** button.
To remove selected or all credentials, click **Remove** or **Clear all** respectively.
Whenever you connect a remote computer, Event Log Explorer will check if you assigned an alternative credential for this computer. If you did, it will try to apply this credential.

Event Log Explorer stores credentials globally (in "C:\ProgramData\Event Log Explorer\Globals\Credentials.xml"), so the credentials persists when you create a new workspace with Event Log Explorer. Elodea Event Collector also uses the same credentials.

See also: Connect with Different Credentials

16. Bookmarking Events

Bookmarking is a handy way to navigate between events in log view. You can mark events in a log view with bookmarks and then quickly navigate between bookmarked events.
Bookmarked events are distinguished from others by their blue color.
To create or remove a bookmark on event highlight the event in the log view, then select **Event -> Bookmarks -> Toggle Bookmark** from the main menu.
To jump to a bookmarked event select **Event -> Bookmarks -> Next Bookmark** or **Event -> Bookmarks -> Previous Bookmarks**.
To remove all bookmarks select **Event -> Bookmarks -> Clear Bookmarks**.
You can bookmark events that match a certain criteria. Use **Event -> Bookmarks -> Bookmark by Criteria**.This will open Filter/Search window and let you input your own bookmark criteria.

17. Analytical Reports

Analytical reports serve to summarize events by a certain criteria and display data as a summary (pivot) table or a pivot chart.
To open Analytical Reports window select **Advanced->Analytical Reports** from the main menu.
Report lets you select report type.
Export To lets you to export summary (pivot) table to a file (HTML, Excel or Word).
Reconcile refreshes your summary table to reflect the latest changes of the original log view.
Summary table tab displays the summarized data as a pivot table
Pivot chart tab displays the summarized data as a pivot chart

18. Command Line Options

Event Log Explorer allows you to open event logs from the command line:
Usage:
ELEX.EXE Workspace
or
ELEX.EXE [/CLEAN] [/OPENLOG lognames] [/OPENFILE filenames] [/OPENTASK tasknames] [/SETFILTER filtername] [/RUNSCRIPT|/RUNSCRIPTCONSOLE scriptname [script_parameters]]

Workspace - workspace to open with Event Log Explorer
/CLEAN - do not restore saved event log windows
/OPENLOG - open event logs *lognames*
/OPENFILE - open event log files *filenames*
/OPENTASK - starts tasks saved in an XML file. You can specify a task template file and it will start it as a task on a local computer
/SETFILTER - applies a saved filter to the event logs. The filter will be applied to event logs listed before this option. *You can set only one filter*
/RUNSCRIPT - start script scriptname, the script may access script_parameters
/RUNSCRIPTCONSOLE - start script scriptname and display scripting console, the script may access script_parameters

/RUNSCRIPT and /RUNSCRIPTCONSOLE are available in Forensic and Enterprise editions.

Examples:
elex.exe C:\Data\MyLogs.elx - opens MyLogs.elx workspace
elex.exe /clean /openlog system \\server\security - opens 2 log files in a new workspace system from the local machine and \\server\security
elex.exe /openlog system application security - opens 3 local logs: system, application and security
elex.exe /openfile C:\backup\system.evtx "C:\app backup.evtx" \\server\c$\eventlogs\sysback.evtx - opens 3 event log files
elex.exe /openlog system application /setfilter filter1.elc /openlog security - opens 3 local logs: system, application and security and applies filter1 to system and application
elex.exe /openlog server\security server\system /openfile C:\backup\system.evtx /clean - opens 1 event log and one event log file
elex.exe /opentask "C:\ProgramData\Event Log Explorer\TaskTemplates\Administrative\Admin events.xml" - starts a task saved in Admin events.xml file.
elex.exe /runscript myscript.pas MSSQLSERVER Administrator - starts script myscript.pas and passes parameters into the script.

19. Working with Database

You can read events stored in a database and you can upload events into a database table.
Event Log Explorer Viewer support Microsoft SQL Server databases.
First you should connect the database. To do so, select **Database->Connect** from the main menu.
You cannot connect more than one database simultaneously. If you want to connect another database, you should disconnect the connected database before establishing a new connection.
To disconnect from the database, select **Database->Disconnect** from the main menu.

Load events from table
If you use Event Log Explorer Enterprise Edition and collect events using Elodea Event Collector, you already have event tables as Elodea feeds.
To load events select **Database -> Load from table**.
Select the required table name and click OK.
Event Log Explorer Viewer will display events from the database table as a native windows event log.

Create database
You can create a new database and upload your own logs directly from Event Log Explorer Viewer.
Although it's recommended to create new databases from special tools like SQL Server Management studio, you create a new database directly from Event Log Explorer Viewer.
To create a database, select **Database->Connect** and click **Create New Database** in Database Connect dialog, type server name and your credentials and click Connect button. Then type database name, its file parameters and review or modify database creation script. Click Create button to start the creation script.

Upload events into table
To upload events into a table from the active event view, select **Database->Upload to Table** from the main menu.In Upload to table dialog, type table name and if required select **Append if table exists** option. If checked Event Log Explorer will append events to the existing table. If not checked and the table exists, Event Log Explorer will delete all events from the table before upload.

20. Backing up Event Logs

Save Event Log As File

To save current event log into event log file, select **File -> Save Event Log (backup)** from the main menu. To backup unopened event log, browse for the log in the computers tree, click right mouse button on it and select **Save Log As** from the drop-down menu.
By default Windows Event Log service doesn't allow backups across the network. It means that if you need to backup System log on \\Server, you can only backup it to \\Server.
When you backup event logs with Event Log Explorer, you can save logs to any computer across the net. In this case Event Log Explorer will backup event log locally to Windows\Temp folder, and move the backup file to the target computer.

Automatic Event Log Backup

Event Log Explorer helps you to automatically back up event logs. To do so, open Event Log Properties dialog (**File->Log Properties** for the current event log) and enable option: **Backup log automatically**. When this option is enabled and the event log size reaches **Maximum log size** value, Windows Event Log service will automatically save the log into Windows\System32\winevt\Logs and clear the log. The name of the backup file is a concatenation of the log file name and the date and time (in coordinated universal time, or UTC). The name has this format:
LogName-year-month-day-hour-minute-seconds-millisecond.evt
You must make sure to move or delete the backup log files from the System volume. If you do not, the volume may become full.
You can find extra information about auto auto-archiving at Microsoft's website

20.1. Backup batch

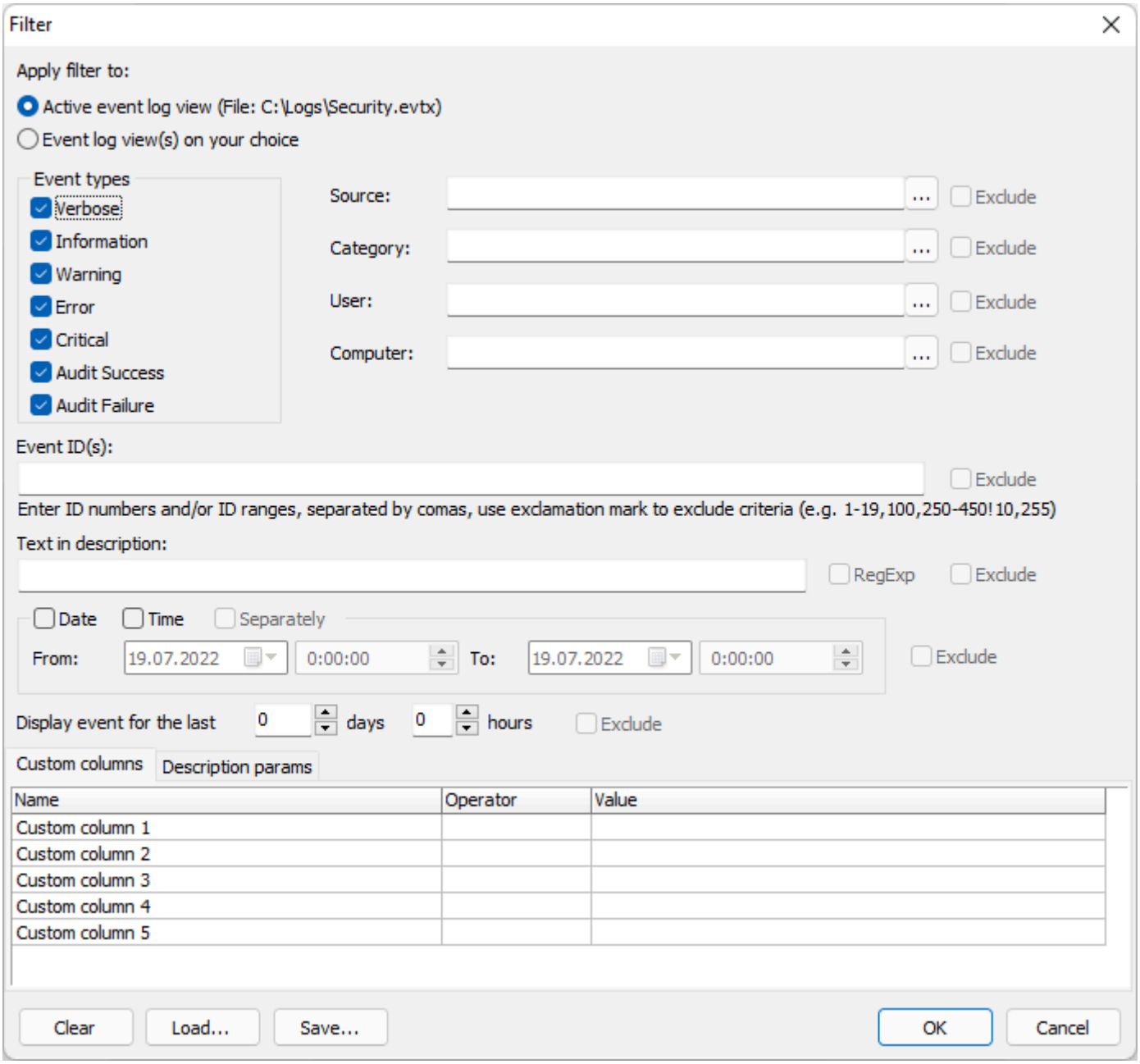
You can automate creation of event log backup batch from Event Log Explorer.
To export Event Log Explorer computers tree to the backup batch, select **Tree->Export** to backup batch from Event Log Explorer main menu.
Backup folder - type the name of the destination folder or /NOBACKUP options.
In the **Computers** box, select the computer names which logs will be backed up, then select log names to backup.
Clear logs after backup adds /CLEAR option to Backup batch lines - this will force ELBACK.EXE to clear event logs after backup.
Review Backup batch and press **Save** button to save batch to file.

21. Exporting Event Logs

Event Log Explorer allows you to export current log view to different formats. Current version exports to Html documents, tab separated text files and Microsoft Excel documents.
To export current log view select **File->Export** from the main menu.
In Export Log dialog box select target file format and export scope.
Enable **Export event description** to add event descriptions to the export file.
Enable **Close this dialog when export is done** to close Export dialog right after export procedure is complete.

22. Filter/Search Window

Using this dialog window, you can specify the criteria for Filter, Find and Bookmark by Criteria command.



Apply filter to defines the views the filter will affect.
Active event log view - if checked, the filter will be applied to the active event log view only.
Event log view(s) lets you select event views to filter.
Event Types defines a list of event types in the criteria. If you uncheck all, any event type will match this criteria.
Source, **Category**, **User**, **Computer** - define lists of sources/task categories/users/computers in the criteria.
Event IDs defines event IDs in the criteria. Refer to Event ID Condition for more information.
Text in description lets you get events that contains the specified text in the event description. Tick RegExp checkbox if Text in description is a regular expression.
Date - if checked, Event Log Explorer will get events logged between From and To dates.
Time - if checked, Event Log Explorer will get events logged between From and To times.
Separately - if not checked, Event Log Explorer will use a single time interval From Date Time and To Date Time. If checked, Event Log Explorer will get events that fall into date interval (from From Date to To Date) and also fall into time interval (from From Time to To Time). This is helpful for example, when you want to get the events that were generated during the working time.

Last dd days yy hours - Event Log Explorer will get the recent events logged during the last DD days and yy hours. Set these values to 0 to display all events.
Custom columns lets you get events based on custom column values. You can build condition by any custom columns. E.g. if you ran a task based on "Service Installed" task template, you may want to view the list of drivers installed in the system that start automatically with the system. You can set such a condition to fulfill this goal:

Name	Operator	Value
Custom column 1		
Custom column 2	Equal	kernel mode driver
Custom column 3	Equal	system start
Custom column 4		
Custom column 5		

Description params lets you create conditions based on formatted description parameters.
E.g. - you have an event (eventid: 4688) with description:

```
A new process has been created.
Subject:
     Security ID:          S-1-5-21-1388292303-2233603710-2753204785-1005
     Account Name:          Bob
     Account Domain:          FSPRO
     Logon ID:          0x1af38
Process Information:
     New Process ID:          0x23b0
     New Process Name:     C:\Program Files (x86)\Microsoft Office\Office15\EXCEL.EXE
     Token Elevation Type:     TokenElevationTypeLimited (3)
     Creator Process ID:     0x8fc
```

Let's say that we want to get all events where user Bob starts Excel.
In this case our filter by params should look like:

Name	Operator	Value
Subject\Account Name	Equal	Bob
Process Information\New Process Name	Contains	excel.exe

The description params filter works only with the descriptions formatted like the descriptions of security events. It is recommended to use Custom columns filter instead of Description params filter.

Case sensitive - if checked, Event Log Explorer will perform a case-sensitive comparison for event description, custom columns and description params. Note that this feature doesn't affect regular expression matching. If you wish to enable case-sensitive regular expression matching, use the regular expression syntax: "**(?-i)**".
Case sensitive is not available for MS SQL Server tables.

23. Event ID Condition

In the most dialog windows which prompt you to input Event ID condition (like filter, search, XML query etc.) you can input multiple event ids.

If you want to specify several event IDs, you can use coma as a delimiter.
E.g. **`10,20,30`** means that events with Event Id = 10 or 20 or 30 will match the condition.

Event Log Explorer provides a handy way to specify event ranges and exception ranges.
To specify a range of IDs, use "**-**" (minus).
E.g. **`10-50,100-200`** means that events with Event ID from 10 to 50 or from 100 to 200 will match the condition.

You can use "!" to specify the exception list of events. All events and event ranges following "!" will be considered as exceptions.

E.g.
`!100,101` means all events except 100 and 101.

`10,100-1000,2000-5000!250,500-600,3000-3200` is equal to
`10,100-249,251-499,601-1000,2000-2999,3201-5000`.

24. Preferences

Preferences dialog window allows you to change default Event Log Explorer parameters.
Top open Preferences dialog, select **File->Preferences** from the main menu.
Changes you made in this dialog are stored into the user's registry, so they are global for different workspaces.

General

User interface defines which user interface will be used.
In **Multiple document interface** (MDI) all event log views will reside under the main window.
In **Tabbed document interface** (TDI) all event log views will be contained within the main window, but only one of them is visible at the time.
Display taskbar tabs enables Event Log Explorer to display tabs in Windows taskbar for each event view.
Click items as follows defines the controls behavior on single or double click.
Do not display empty logs in the tree hides empty logs in the Objects tree**.**
Minimize to notification area hides When Event Log Explorer from Windows task bar and displays Event Log Explorer icon in the system tray when the program is minimized.
Font defines the default font and for main Event Log Explorer window and event log views.
Scale defines the user interface scale.
Visual Style defines Event Log Explorer visual style.

Advanced

Event description rendering method defines how Event Log Explorer will get the description of events.
Undocumented way provides the fastest method of getting descriptions, however in some rare cases, it may display not the same result as Windows Event Viewer displays. **Documented API** generates the same result as Event Viewer does, but log loading performance is not so fast as Undocumented approach.

SQL server database options define how Event Log Explorer will query events from SQL server tables.
Event Log Explorer Viewer may work as an SQL Server client to read events saved by Elodea Event Collector or exported by Event Log Explorer Viewer.
When querying SQL tables, SQL server creates a cursor - a special temporary set of records. Event Log Explorer lets you store this cursor either on the server side or on the client (local computer) side. Server-side cursors are handy for a large amount of records you queried (e.g. more than 100 000 records). Client-side cursors are the best choice for a small number of records.
In most cases, you don't need to query all the data in one log view. With Event Log Explorer you can limit a number of records selected from the database.

Example:
Let's say you have a database table with 1 million events. As a rule, you don't need to view all these events. So you can set SQL Server database options to display only 25 000 events (and use Client-side cursor). When opening the table, Event Log Explorer will display only 25 000 events. Then you may want to display e.g. only Error events. Set filter to type = Error and check the result. If the total number of errors is less than 25 000, it will display them all. If the total number of error events is more than 25 000, you can refine your filter or increase the limit.

Date and time format defines how Event Log Explorer will display event dates. It uses system date and time format by default, but you can change it to your own format.
Pay attention that "n" stands for minutes while "m" stands for months.

Maximum custom columns number (available in Forensic and Enterprise editions only) lets you increase the maximum number of the custom columns available for each log view. By default, Event Log Explorer allows you to use up to 5 custom fields. You can enable up to 15 custom fields by using this option. Setting more custom columns may affect the performance of Event Log Explorer, so change this value only when you need it.

Log View Defaults

These settings will be applied to new log views, created with Event Log Explorer. They will not affect existing log views.

Enable auto-refresh force Event Log Explorer to reread event logs every **Default auto-refresh** interval.
Default sort order defines a default criteria (column) the event list will be sorted by. Enable **Descending** if you want to sort the event list in descending order. We recommend you to set **Newest first** sorting criteria - this will increase event log loading process.
Description server defines server name where Event Log Explorer will get descriptions by default. E.g. you can set this field to LOCALHOST, and Event Log Explorer will try to get description from your local computer.
Color coding file defines the default color coding file for all new event views. See also: Color Coding

Log Loading Filter

Event age allows you to pre-filter event log by events age.
Event types allows you to pre-filter event log by event type.
Event IDs allows you to pre-filter event log by events IDs. If you want to specify multiple IDs, please use coma as a delimiter. To specify a range of IDs, use "**-**".
You can use "!" to specify the exception list of events. All events and event ranges following "!" will be considered as exceptions. E.g. ***10,100-1000,2000-5000!250,500-600,3000-3200*** will be equal ***10, 100-249,251-499,601-1000, 2000-2999,3201-5000***
User names allows you to pre-filter event log by user name. To specify multiple user names, please use coma as a delimiter.
Computers allows you to pre-filter event log by computer name. To specify multiple computer names, please use coma as a delimiter.
We highly recommend you to pre-filter events by age and/or by type - this will force to load logs partially, reduce memory consumption and increase the performance.

Appearance

Display grid lines - if checked, event list will be displayed with grid lines.
Details box location defines where the description box will be displayed (event description, hex data and other event details).
Description in line - if checked, event list will be displayed with description column. Muiti-line descriptions will be converted into single-line once. Very long descriptions could be truncated in this column.
Autofit columns after loading - if checked, Event Log Explorer will adjust columns width when you load or refresh event logs. Unlike all other Log View Defaults, this option is applied even to already opened log views.

Workspace

On program start
Open last used workspace - if checked Event Log Explorer will start with last used workspace.
Open empty workspace - if checked Event Log Explorer will create UNTITLED workspace at start.
On new workspace defines the program behavior when creating a new workspace.
Add local computer to the tree - if checked, your computer will be automatically added as a first computer in the computers tree.
Restore from workspace file defines which kind of data should be restored from the workspace file.

Confirmations

Confirmations define when Event Log Explorer will display warning messages.
When closing event log window - if checked, the program will not warn you when you close event log window.
When closing all event log windows - if checked, the program will not warn you when you use File / Close All command.
When quitting the program - if checked, the program will not warn you when you quit it.
When closing the workspace - if checked, the program will not warn you when you close the workspace:

- **Auto save the workspace** - it will save the workspace file automatically;
- **Do not save the workspace** - all unsaved changes to the workspace will be lost.

Log Files

Associate Event Log Explorer with .EVT files. Enable this option if you want Event Log Explorer to open .EVT files when you click on them in Windows Explorer.
Associate Event Log Explorer with .EVTX files. Enable this option if you want Event Log Explorer to open .EVTX files when you click on them in Windows Explorer.

Automatically add log files to tree. If checked, Event Log Explorer will add event log files you open to the tree.
Put log files to group defines group name to which event log files will be added.
Default timezone for log files defines in which time zone Event Log Explorer will display event data and time.

Print

These options define the default print layout.
Report title - defines report header.
Page footer - defines text messages that will be displayed in the left, center and right part at the bottom of each report page.
Striped report - if checked, the report will be displayed or printed with horizontal stripes - this will highly increase report readability.
Restore defaults - resets report layout defaults.
Reporting variables:
[LogName] - name of the event log.
[CompName] - name of the computer.
[Page#] - Report page number.
[TotalPages] - Number of pages in the report.
[Program] - Name of this program (Event Log Explorer).
[Date] - Date of print.
[Time] - Time of print.
[IsFiltered] - Will display "Filtered" if the log view is filtered.
[IsFiltered2] - Will display "Filtered: xx of xxxx event(s)" if the log view is filtered.

User Files

Location of criteria files (filters) defines a default path where Event Log Explorer will store event filter files. When Event Log Explorer starts, it loads filter names from this folder and displays them in **Load Filter** menu in the toolbar.

Updates

Automatically poll for updates - Event Log Explorer will be checking for updates automatically every (**Polling interval**) days.
Last poll - the date of the last check for updates.
Do not display warning message before connecting the Internet - if unchecked Event Log Explorer will display a dialog box notifying you about connecting the Internet.

25. Forensic Edition

Event Log Explorer Forensic Edition extends the features of Standard Edition. Event Log Explorer Viewer runs non-elevated by default, so it doesn't require admin permissions. To access the local logs which require admin permissions (e.g. Security log), you can start it elevated (use Run as Administrator command in Windows). You can access the forensic features of the program using Forensics item in the main menu.

25.1. Imaged Computer

Event Log Explorer Forensic Edition simplifies working with disk images. When you examine logs from a disk image without using Event Log Explorer Forensic Edition, you should either extract files located in \Windows \System32\winevt\Logs\ from the image or mount this image and access these files. In both cases, you open evtx files, but you see only the information saved in this evtx files. The viewer may not display event descriptions, task categories or user names unless it can render it locally. E.g. if you open a security log file, your local computer commonly contains the required components to render the task category and event description. As for the user name, it is commonly set to N/A for Security log.
However, if you open an application or other event logs, you can find that event description for some events could not be found, task category displays a number in parentheses and user name displays a user SID e.g. S-1-5-21-2251232950-2328508685-887570584-1001.
To fix these rendering problems, Event Log Explorer lets you access your disk as you access a live computer. First, if you work with a disk image, you should mount your image as a disk.
To add Imaged Computer to the tree, select Forensics->Add imaged computer from the main menu.
Windows root folder - specify the path to Windows folder on the examined disk. Event Log Explorer tries to detect this path automatically.
Friendly name of PC - specify the name of the PC as it will be displayed in the tree.

The new imaged computer will be added to the tree and you can work with it exactly like you work with a local computer. When you work with the imaged computer, Event Log Explorer will emulate Event Log Service and resolve description, category and user name.

25.2. Open Files with Forensic Edition

Event Log Explorer Forensic Edition provides more features to work with EVTX files.
The standard menu item File->Open Log File still works, but we recommend using **Forensics->Forensic Open File** menu command.
Add, **Remove** and **Clear** buttons let you select event log file(s) to open.
File access method - Standard access method - Event Log Explorer will open files using Windows API. This is a recommended file access method. Event Log Explorer Forensic Edition will work the same way as the Standard Edition does.
File access method - Direct access method - Event Log Explorer will open files without using Windows API. This lets you open damaged EVTX files. Use this option if the Standard method fails.
Note: If you have a damaged EVT file, you should try the standard command: File->Open Log File - damaged EVT files can be opened even in the Standard Edition.
Multiple files open - open each file in separate views - If you add several EVTX files to the list, Event Log Explorer each file in a new log view.
Multiple files open - merge all files in one view - Event Log Explorer will merge all files into one view.
Get event description, task and user names, text parameters from - Default location - Event Log Explorer will render event description and other event details based on the locally installed components.
Get event description, task and user names, text parameters from - Imaged computer - Event Log Explorer will render event description and other event details using the components installed on the imaged computer.
Check log files for deleted events - Event Log Explorer will try to detect if the event log files was forged by removing events. This option may not work when you open files using Direct method.

25.3. Deep Scan

Deep Scan lets you extract events from any file or disk. You can use it to find events in highly damaged event log files, deleted log files, logical or physical disks or disk images you cannot to mount. Event Log Explorer scans file or disk byte by byte and looks for the Event Log Chunk signature (ElfChnk). When it finds ElfChnk signature, it verifies if the next 65536 bytes of the scanned source represent an event chunk and tries to extract events from it. This lets you extract events from virtually any source provided that it is not encrypted. When you want to scan a logical or a physical drive, you may need to start Event Log Explorer elevated or you may get the Access-denied error. If you have an encrypted disk or image, you should either decrypt it or mount it to get access to the disk content.

To start scanning of a file or a disk, select Forensics->Deep Scan from the main menu.
Scan file - input name of the file to scan. It could be evtx file or any other file including disk image.
Scan disk - input a logical or a physical name of the disk to scan.
Event loading criteria - lets you filter events by scanning. E.g. if you want to scan only for Security events, click Events matching criteria click Add near the Channel names box and type Security in the Input channels name dialog.

If you scan an entire disk or a disk image, this operation may take long time.

25.4. Snapshots

Snapshots lets you save events into a local file and then load and work this file like you work with event logs.
Taking snapshots is similar to making backups, but provides extra features:
You can snap visible or specific (bookmarked) events;
You don't need to have special permissions to snap;
The snapshot contains rendered event descriptions, categories and user names;
The snapshot can optionally contain extra event details like a timezone and custom columns.

To take snapshot of the event view, select **Forensics->Take snapshot** from the main menu.
Event scope - select whether you want to save all visible events or only bookmarked events.
Include custom columns definition - if your event log view has custom columns, their definitions will be saved in the snapshot. When loading, Event Log Explorer will create custom columns and calculate them.
Save timezone - if checked, current timezone will be saved in the snapshot. In the other case, the snapshot will be saved without the timezone. When loading, Event Log Explorer will use the default timezone.
Open snapshot after saving - Event Log Explorer will load the snapshot after saving into a new log view.

To load snapshot, select **Forensics->Load snapshot** from the main menu. Select the name of the snapshot file and press Open button. Event Log Explorer will load the snapshot into a new log view.

26. Scripting

Event Log Explorer comes with scripting support provided by FastScript/PascalScript (https://www.fast-report.com/en/product/fast-script/). Scripting support is available in Forensic and Enterprise Editions of Event Log Explorer.
To open Script console select **Script->Script Console** from the main menu.
New - clears the script console - make sure to save your current script before starting a new one.
Load - loads a saved script.
Save - saves the script console.
Run - runs the script typed in the console.
Break - tries to break the running script. This will stop the script, but will not break the current scripting operation, e.g. if you click Break when log is loading, this will not stop the loading operation (you may need to press Stop button near the loading progress to break the loading).
Clear - clears the debug output window.

Refer to the Event Log Explorer Scripting Reference to get to know how to make your own scripts.

27. Event Log Explorer Tools

Event Log Explorer comes with a set of command-line utilities to automate your work. You can find these utilities in the Event Log Explorer application folder.

Event Log Backup utility (elbackx.exe)
Event Log Backup utility lets you quickly save event logs from different locations in one place. You can find elback.exe in Event Log Explorer application folder.
ELBACKX BatchFile
runs **BatchFile** to backup logs.

ELBACKX DestDir EventLogs [/clear]
backups **EventLogs** to **DestDir** with optional clear option.

BatchFile format:
; - comment line
DestDir EventLogs [/clear]

DestDir - specifies a destination folder (or /NOBACKUP option).
If the destination folder name contains spaces, it must be enclosed in quotes.
EventLogs - specifies a particular event log or group of event logs which you want to backup to **DestDir**.
Event logs must be separated by spaces. If event log name contains spaced, it must be enclosed in quotes.
Remote event logs are specified as \\ComputerName\LogName. You can use wildcard characters (*) to specify all event logs (\\ComputerName*).
/clear - optionally clears **EventLogs** after backup.

Sample BatchFile with comments:
```
====================
;backup to C:\Backup Application and system from Server, then clear
C:\Backup\ Server\Application Server\System /Clear
;Backup all logs from Server2 to C:\My Backup, without clearing.
"C:\My Backup\" Server2\*
;Clear all logs from 192.168.1.11
/Nobackup \\192.168.1.11\* /clear
====================
```

You can automate BatchFile creation from Event Log Explorer tree. More information is available in Export to backup batch.

Examples:

```
run batchfile.elb batch to backup logs:
ELBACKX batchfile.elb
backup Security log from Serv01 to C:\Backup:
ELBACKX C:\Backup Security Serv01\Security
backup all logs from Serv01, Serv02 and Serv03 to C:\My Backup, then clear them:
ELBACKX "C:\My Backup" \\Serv01\* \\Serv02\* \\Serv03\* /Clear
backup Directory Service from Serv01 to C:\My Backup:
ELBACKX "C:\My Backup" "\\Serv01\Directory Service"
```

Event Log Database Export utility (eldbx.exe)

This utility is available only in the Enterprise Edition.

Event Log Backup utility lets you quickly save event logs from different locations into a database table. You can find eldbx.exe in Event Log Explorer application folder.

Usage

```
eldbx [OPERATION] /OPTION:VALUE [/OPTION:VALUE] ...
```

Operations:
Export Export events into database table
CreateDB Create database

Export:

```
eldbx EXPORT [/DBMS:mssql] /DBSERVER:<server_name> [/DBAUTH:{windows|server}]
[/DBUSER:<db_user_name>] [/DBPASSWORD:<db_password>]
/DBNAME:<db_name> /TABLE:<table_name> [/TABEXTTS:{date|datetime}]
[/TXA:{fail|append|overwrite}] [/HOST:<host_name>] [/USER:<user_name>]
[/PASSWORD:<password>] [/LOGNAME:<log_name>] [QUERY:<query_file_name>]
[/EDR:{all|ri|render|no}] [/CLEARLOG:{no|yes|tolerate}]
[/VERBOSE:{0|1|2|3}]
```

Option	Value	Description
/DBMS	{mssql}	Specifies database management system. Values: mssql - Microsoft SQL Server. Optional. Default value: mssql.
/DBSERVER	<server_name>	Specifies database server name (instance name). Mandatory. For SQL Server, the default instance is the computer name. For SQL Server Express, the default instance is named <computer_name>\sqlexpress
/AUTH	{windows|server}	Specifies authentication method windows - uses Windows authentication. server - uses SQL server authentication. Optional. Default value: windows.
/DBUSER	<db_user_name>	SQL server user name. Optional.
/DBPASSWORD	<db_password>	SQL server user password.
/DBNAME	<db_name>	Specifies Database name. Mandatory
/TABLE	<table_name>	Specifies table name. Mandatory
/TABEXTTS	{date|datetime}	Specifies table extension timestamp. Values: date - adds current date to table name as -yyyy-mm-dd. datetime - adds current date and time as -yyyy-mm-dd-hh-mm-ss. Optional.
/TXA	{fail|append|overwrite}	Specifies what to do if table already exists. Values: fail - quit application with error. append - append events to the table.

		overwrite - delete existing and write new. Optional. Default value: fail.
/HOST	<host_name>	Specifies host name to read events from. Optional. Localhost is implied.
/USER	<user_name>	Specifies user name to access logs on host. Optional.
/PASSWORD	<password>	Specifies user password to access logs. Optional.
/LOGNAME	<log_name>	Specifies log name to export. Mandatory if /QUERY not specified.
/QUERY	<query_file_name>	Specifies file containing XML query to get events for export. Mandatory if /LOGNAME not specified.
/EDR	{all|ri|render|no}	Specifies event description rendering options. Values: no - do not render event description. render - render event description. ri - use event RenderingInfo. all - try RenderingInfo, if not available, render description. Optional. Default value: all.
/CLEARLOG	{no|yes|tolerate}	Option to clear event log after export. Values: no - do not clear event log. yes - clear event log. tolerate - clear event log, do not report error if clearing fails. Optional. Default value: no. NOTE. "Export&clear" is not an atomic operation! There is a chance that some events appear after export and before clearing!
/VERBOSE	{0|1|2|3}	Specifies verbosity level. Values: 0 - display all information. 1 - display event message rendering issues, warnings and errors. 2 - display warning and errors. 3 - display errors only. Optional. Default value: 2.

CreateDB:

```
Eldbx CREATEDB [/DBMS:mssql] /DBSERVER:<server_name> [/AUTH:{windows|server}]
[/DBUSER:<db_user_name>] [/DBPASSWORD:<db_password>] /DATABASE:<db_name>
[/DBSIZE:init_db_size] [/DBGROW:db_grow] [/LOGSIZE:init_log_size]
[/LOGGROW:log_grow] [/VERBOSE:{0|1|2|3}]
```

Option	Value	Description
/DBMS	{mssql}	Specifies database management system. Values: mssql - Microsoft SQL Server. Optional. Default value: mssql

/DBSERVER	<server_name>	Specifies database server name (instance name). Mandatory. For SQL Server, the default instance is the computer name. For SQL Server Express, the default instance is named <computer_name>\sqlexpress
/AUTH	{windows|server}	Specifies authentication method windows - uses Windows authentication. server - uses SQL server authentication. Optional. Default value: windows.
/DBUSER	<db_user_name>	SQL server user name. Optional.
/DBPASSWORD	<db_password>	SQL server user password.
/DBNAME	<db_name>	Specifies Database name. Mandatory
/DBSIZE	<init_db_size>	Initial size of the database data file (in MB) Optional. Default value: 25.
/DBGROW	<db_grow>	Specifies the automatic growth increment of the database data file in percent. Optional. Default value depends on SQL Server.
/LOGSIZE	<init_log_size>	Initial size of the database log file (in MB). Optional. Default value: 10
/LOGGROW	<log_grow>	Specifies the automatic growth increment of the database log file in percent. Optional. Default value depends on SQL Server.
/VERBOSE	{0|1|2|3}	Specifies verbosity level. Values: 0 - display all information. 1 - not used with CreateDB command. 2 - display warning and errors. 3 - display errors only. Optional. Default value: 2.

Examples:

Create database Events:

```
eldbx CREATEDB /DBSERVER:Server /DBNAME:Events
```

Export local Application log into table app_events:

```
eldbx EXPORT /DBSERVER:Server /DBNAME:Events /TABLE:app_events /
LOGNAME:Application
```

Append System log from Host into app_events providing specific credentials:

```
eldbx EXPORT /DBSERVER:Server /DBNAME:Events /TABLE:app_events /TXA:append /
HOST:Host /LOGNAME:System /USER:Administrator /PASSWORD:password
```

Event Log Export utility (logexport.exe)

This utility is available in Enterprise and Forensic editions of Event Log Explorer.

Log Export utility lets you export event logs into different document formats. You can find logexport.exe in Event Log Explorer application folder.

Usage

```
logexport /OPTION:VALUE [/OPTION:VALUE] ...

logexport [/TASK:<task_file_name>]
          [/HOST:<host_name>]
          [/USER:<user_name>]
          [/PASSWORD:<password>]
          [/LOGNAME:<log_name>]
          [/EDR:{all|ri|render|no}]
          [/TARGET:{EXCEL|CSV|HTML|PDF}]
          [/TDIR:<target_dir_name>]
          [/TFILE:<target_file_name>]
          [/VERBOSE:{0|1|2|3}]
```

Option	Value	Description
/TASK	<task_file_name>	Specifies path to xml file name that describes the task. Mandatory if /LOGNAME not specified
/HOST	<host_name>	If /TASK not specified, /HOST defines the host name to read events from. If no /TASK and no /HOST specified, localhost implied.
/HFT	{fail|tolerate}	Host fail tolerance. Defines the behavior when the task lists several hosts and logs from one of the hosts are not available. Values: fail - terminate if the logs unavailable. tolerate - ignore the host and continue with the others. Optional. Default value: tolerate.
/USER	<user_name>	Specifies user name to access logs. Optional.
/PASSWORD	<password>	Specifies user password to access logs. Optional.
/LOGNAME	<log_name>	Specifies log name or log file name to export. Mandatory if /TASK not specified. For a log file, you must provide a full path in double quotes.
/EDR	{all|ri|render|no}	Specifies event description rendering options. Values: no - do not render event description. render - render event description. ri - use event RenderingInfo. all - try RenderingInfo, if not available, render description. Optional. Default value: all.
/TARGET	{Excel|ODS|CSV|HTML|PDF}	Specifies the target file type. Excel - Microsoft Excel (XLSX file). ODS - Open Office spreadsheet format.

		CSV - coma separated text. HTML - HTML format. PDF - Adobe PDF fornat. Optional. Default value: Excel.
/TDIR	<target_dir_name>	Specifies the location (folder) of the target file. Optional. Default value: Current_Folder.
/TFILE	<target_file_name>	Specifies name of the target file. Optional. If not specified, will be named automatically. If a full path is specified TDIR will be ignored. If TARGET is HTML, TFILE specifies name of the folder in which html files will be created.
/VERBOSE	{0|1|2|3}	Specifies verbosity level. Values: 0 - display all information. 1 - display event message rendering issues, warnings and errors. 2 - display warning and errors. 3 - display errors only. Optional. Default value: 2.

Examples:

Export local Application log into Excel file:

```
logexport /LOGNAME:Application /TFILE:App.xlsx
```

Export Security log from Server into PDF file and autoname this file:

```
logexport /HOST:Server /LOGNAME:Security /TARGET:PDF
```

Export log file into HTML files:

```
logexport /LOGNAME:"C:\LogFiles\sys.evtx" /TARGET:HTML /TFILE:"C:\LogFiles
\Exported"
```

Export Event Log Explorer task into Excel file and autoname it:

```
logexport /TASK:"C:\Tasks\mytask1.xml"
```