



Welcome to Event Log Explorer Help

This help system is a place to find information about Event Log Explorer.

[Introduction](#)

[Concept](#)

[Event Log Explorer basics](#)

[License agreement](#)

© 2005-2018 FSPro Labs. All rights reserved.

Introduction

Event Log Explorer is a software for viewing, monitoring and analyzing events recorded in Security, System, Application and other logs of Microsoft Windows operating systems. It extends standard Event Viewer monitoring functionality and brings new features.

Main features of Event Log Explorer:

- » Multiple-document or tabbed-document user interface depending on user preferences
- » Favorites computers and their logs are grouped into a tree
- » Viewing event logs and event logs files
- » Merging different event logs into one view
- » Archiving event logs
- » Event descriptions and binary data are in the log window
- » Event list can be sorted by any column and in any direction
- » Advanced filtering by any criteria including event description text
- » Quick Filter feature allows you to filter event log in a couple of mouse clicks
- » Log loading options to pre-filter event logs
- » Switching between disk and memory for temporary data storing
- » Fast search by any criteria
- » Fast navigation with bookmarks
- » Compatibility with well-known event knowledgebases
- » Sending event logs to printer
- » Export log to different formats

Multiple-document or tabbed-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 unlimited number of event logs and place them all inside the main window of Event Log Explorer. Tabbed-document interface (TDI) allows you to open unlimited number of 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.

Viewing event logs and event log files

With Event Log Explorer you can open event logs as event log files. To open an event log file, just select **File / Open Log File**.

Merging different event logs into one view

You can unite several event logs (or event log files) in one log view. Such consolidation view (Merger) may significantly simplify process of analysis. You can have unlimited number of mergers in Event Log Explorer workspace.

Archiving event logs

Archiving event logs is very important task. Very large event logs affect system performance, but administrators must be able to analyze past events. The appropriate solution is to limit the size of event logs, and backup event logs on regular basis. Event Log Explorer allows you to save opened event log as an event log file manually or automatically.

Event descriptions and binary data are in the log window

Unlike standard 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.

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 filter 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 options to pre-filter event logs

You can pre-filter event log when it's opening. This will reduce memory consumption, increase performance and make log view clear.

Switching between disk and memory for temporary data storing

You can choose where to load event logs: to RAM for best performance or to disk to reduce memory consumption.

Fast search by any criteria

With Event Log Explorer you can easily search for event that meets a certain criteria. Just use **View / Find** command to start search. To find a next event that meets this criteria, please use **View / 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.

Compatibility with well-known event knowledgebases

You can get more information about event in the public event knowledgebases. Event Log Explorer supports EventID.net and Microsoft

knowledgebases.

Sending Event Log to printer

Unlike standard Windows Event Viewer, Event Log Explorer can print event logs. Print options let you select from several styles of print.

Export log to different formats

You can export your event logs to other formats. At the time, Event Log Explorer supports export to HTML, tab-separated and Excel documents.

© 2005-2018 FSPro Labs. All rights reserved.

Using Event Log Explorer (Basics)

In this section:

[Opening Event Log](#)


[Opening Event Log Files](#)


[Viewing Event Logs](#)

[Sending Event Log to Printer](#)

Opening Event Log

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 an 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 select the desired event log. See also [Event Log API](#)

Opening Event Log Files

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

Standard open allows you to open .evt files on Windows NT, 2000, XP and .evtx on Windows Vista. Direct open allows you to open .evt files on all operating systems. See also [Direct Access to Event Log Files](#)

Viewing Event Logs

Event log view displays events as a multicolumn list. By default newest events are on the top.

To sort the list by a certain column, click on the column header. Click a second time to reverse the sort order. To sort event list from the oldest events to the newest or visa versa, select **View->Oldest First** or **View->Newest First** from the main menu.

If you open several event log views, you can switch between them using Ctrl+Tab key combination.


To navigate between events in a log view, use mouse, arrow keys or a navigator bar in the upper left corner of the log view.


A bottom side of event log view contains Description Box. It displays event description or binary data associated with the selected event.

View->Show Description Box allows you to hide or show this box.

See also: [Event Log View](#)

Sending Event Log to Printer

To print current event log view, select **File->Print** from the main menu or click .

Select **File->Print Preview** or click  to preview the output before printing.

© 2005-2018 FSPro Labs. All rights reserved.

Event properties

The Event Properties dialog box shows event attributes, text description of the event and any available binary data. Binary data, which appears in hexadecimal format, is information generated by the program that is the source of the event record.

To display event properties dialog:

Activate Event Log View, highlight the event and select **View->Event Properties** from the main menu or just double click on the desired event in the log view.

Unlike Windows Event Viewer, you can open new Event Properties dialogs for each log views.

To close Event Properties dialog, just press **Close** button. If you close a log view, the corresponding Event Properties dialog will be closed automatically.

Event Log Explorer Concept

In this section:

[Workspaces](#)

[Computers Tree](#)

[Log Views](#)


Workspaces

Event Log Explorer has a document-oriented architecture. Event Log Explorer documents are called *workspaces*. When you start Event Log Explorer first time, it automatically creates an empty workspace **Untitled**.

Workspaces store Computers tree and Opened event log views including windows placement, filters, log loading options, etc). Workspaces don't store Event Log Explorer Preferences. All global options and preferences are stored in the user's registry.

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**.

Computers Tree

Computers 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  sign near the computer name, Event Log Explorer displays all event logs available on this computer - double click on the log opens the event log immediately.

Log Views

Log view is a visual representation of event log or event log file. Log view consist of event list, description box and control toolbar. 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.

© 2005-2018 FSPro Labs. All rights reserved.

Event Log API

Event Log Explorer supports both two APIs to access Windows Event Logs.

- » Legacy Event Log API, designed for Windows NT, 2000, XP and Windows 2003
- » New Event Log API, introduced by Microsoft in Windows Vista/2008

When you open an event log, Event Log Explorer verifies if New API is available and displays select API dialog.

New Event API is available only when your local and remote computers are running at least Windows Vista operating system.

© 2005-2018 FSPro Labs. All rights reserved.

Filtering events in Event Log Explorer

Event Log Explorer offers 5 ways of data filtering.

In this section:

[Pre-filtering events \(log loading options\)](#)

[XML query filter](#)

[General filter](#)

[Quick filter](#)

[Linked event filter](#)

Pre-filtering events (log loading options)

Use pre-filtering to filter events during the log loading process.

You can pre-filter events by event age, event types and other parameters.

To set the global log loading options, open [Preferences](#) dialog and select [Log View Defaults](#).

To change log loading options for active view, select **View->Log Loading Options** from the main menu.

XML Query Filter

XML query filter also prefilters events, but unlike log loading options, it is executed on the target machine. This may significantly reduce network load and improve log loading performance.

To filter events using XML query, select **View->XML query** from the main menu. This will open [XML Query window](#).

General Filter

To filter events in an event log view, select **View->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 filtered 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-applied after log reloading.

To clear filter, select **View->Clear Filter**.

Quick Filter

Quick Filters 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 filtered list easy and clearly.

When you refresh the event list, all quick filters will be cancelled.

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

Linked event filter

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

Select **Advanced->Linked Event Filter** from the main menu to display [Linked Event Filter](#) dialog.

To clear linked event filter, select **View->Clear Filter**.

© 2005-2018 FSPro Labs. All rights reserved.

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.

See also: [Event Log View](#)

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 (both legacy and 2007) 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.

Note: Due to Excel document limitations, Event Log Explorer is unable to export more than 65500 events to Excel format. If you need to export more than 65500 events, you should export to Excel 2007 format.

You can also export event log into EVT file. Read [Backing up Event Logs](#) for more information.

© 2005-2018 FSPro Labs. All rights reserved.


Backing up Event Logs

In this section:

[Save Event Log As File](#)

[Automatic Event Log Backup](#)

Save Event Log As File

To save current event log into event log file, select **File->Save Log As -> Save Event Log (backup)** from the main menu or click . 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.

You can save/export certain events from event log to .evt file. To do so, select **File->Save Log As -> Save Displayed Events** or **File->Save Log As -> Save Selected Events** from the main menu to create a new .evt files from the current event log view or currently selected events.

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, then clear it**. 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\config\ (for Windows 2000, XP, 2003 Server) or Windows\System32\winevt\Logs (for Windows Vista, 7 and 2008 Server), 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](#)

Export tree to 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.

Add Computers Wizard

Add Computers Wizard helps you to add a bulk number of computers to the tree.

To start the wizard, select **Tree -> Add Computers Wizard** from the main menu.

Add Computers Wizard starts automatically when you create a new workspace and option Run Add Computers Wizard is enabled in [Workspace Preferences](#).

On the first page of the wizard you should specify the types of servers you would like to search for.

The following options are available:

- » All Windows NT workstations and servers
- » Domain controllers (primary and backup)
- » Standalone servers (not domain controllers)
- » Servers or workstations that run SERVER service
- » Servers running with Microsoft SQL Server
- » Servers sharing print queue
- » Terminal Servers
- » Server clusters available in the domain

The next page will display the search result. You should choose which of the found computers will be added to the tree.

The last page displays the computers that will be added to the tree and allows you to select the group to which they will be added. If **Add description** is enabled, computer descriptions (if any) will be added to the tree as well.

Log properties

To display log properties dialog:

Activate Event Log View and select **File->Log Properties** from the main menu or

Right click on the log name in the [Computers Tree](#) and select **Log Properties** from [Tree context menu](#).

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.

Overwrite events older than xx days - when the log is full new events will replace the old ones only if they are older than xx days.

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, then clear it - log will be saved as a file and the emptied. See also: [Automatic Event Log Backup](#).

Restore defaults - resets **Event Log Size** options to default values.

Clear Log - empties event log.

© 2005-2018 FSPro Labs. All rights reserved.

Credential manager

Sometimes you may need to connect the remote computer with different credentials (**Tree -> Connect with different credentials**).

Event Log Explorer lets you automate connecting with different (alternative) credentials by storing required user credentials for each remote computer.

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. User credentials are stored in the [workspace](#) file, the password is encrypted.

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 any 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.

See also: [Credentials conflict](#)

Credentials conflict

Sometimes you need to connect the remote computer with different credentials (**Tree -> Connect with different credentials**). Such situation can occur when your account doesn't have enough permissions to access a remote log. However when you try to connect with different credentials, you may get credential conflict error:

Multiple connection to a sever or a shared resource by the same user, using more then one user name, are not allowed.

This error message appears in the **Connect Error** dialog, if connection is failed due to credentials conflict.

There are 3 ways to resolve this issue:

1. Disconnect previous connections to the server.

You can do it in the **Connect Error** dialog.

Sometimes this method doesn't work properly, e.g. when another local process reestablish connection to the server, and sometimes this method is not allowed because you may need the previous connections established.

2. Connect the remote server using IP address, instead of the computer name.

Just add a new computer to the tree, specifying it's IP address. E.g. if the remote server's IP address is 192.168.1.1, you can add it as

\\192.168.1.1 or even **192.168.1.1**

3. Run Event Log Explorer using different (required) credentials.

In Windows XP you can just click right mouse button on the Event Log Explorer shortcut and select **Run as**. Then specify user name and password in the **Run As** dialog and press **OK**.

See also: [Credential Manager](#)

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

© 2005-2018 FSPro Labs. All rights reserved.

Event Alerter

Event Log Explorer can automatically monitor new events in event log view and alert you when a specific event occurs. This helps you to get informed about a problem right after it happen.

To open Event Alerts window, select **Advanced->Event Alerter** from the main menu.

You can add/change alert rule using **Add/Change** buttons.

Clone button clones current event rule.

Save button saves alerts to a file.

Load button loads previously saved alerts.

Test Events scans all events in the active event log view and alerts if an event matches one of the alert rules.

Alert pattern dialog

Alert pattern dialog lets you edit alert rule.

Event source and **Event ID** define the pattern - the condition on which the rule will be applied.

Action defines the action to start when the condition matches the event.

Run a program indicates the program name and its command line parameters to start as alert action.

Available parameters box lists the event details you can pass as command line parameters to the program. Double click in the list copies the parameter into **Run a program** box.

Example:

You can set Event Log Explorer to send email using blat (or similar) program. Blat is an open-source free software available at <http://sourceforge.net/projects/blat/files/>

Let's say you want to monitor Application event 26214, source: Chkdsk (Checkdisk run).

Event source: Chkdsk.

Event ID: 26214.

Action:

```
C:\Utils\blat\blat.exe -to "John Doe" -subject "Event Alert" -f john@server.com -server server.com -u john -pw password -body "Checkdisk event! Logname: [LogName]; Time: [TimeStamp]; EventId: [EventIDNorm]; User: [UserName]; Computer: [Computer] "
```

Whenever this event appears, you will get email:

```
Checkdisk event! Logname: Application on STORM , Time: 3/1/2012 4:06:09 PM; EventId: 26214; User: N/A; Computer: STORM
```

Notes:

Event Alerter tests new events only when event view is refreshing. So you should either enable autorefresh using **View->Auto-refresh** or schedule refresh using [Scheduler](#).

When you enable Event Alerter, you will automatically activate option **Only new events after refresh**. This guarantees that only new events will be tested and you will not get recurring alerts on the same event.

© 2005-2018 FSPro Labs. All rights reserved.

Custom columns

Custom columns options 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.

Event Log Explorer lets you add up to 5 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 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.

You should use description parameters in this field. Description parameters are enclosed in curly brackets.

Let's say you want to display user logon name from the following event description

An account was successfully logged on.

Subject:

Security ID:	S-1-5-18
Account Name:	MIKE-HP\$
Account Domain:	FSPRO
Logon ID:	0x3e7

Logon Type: 5

New Logon:

Security ID:	S-1-5-21-1388294503-2733603710-27532
Account Name:	Michael
Account Domain:	FSPRO
Logon ID:	0x13a0091e

```

        Logon GUID:                {00000000-0000-0000-0000-000000000000}
Process Information:
        Process ID:                0x2f8
        Process Name:              C:\Windows\System32\services.exe
Network Information:
        Workstation Name:          MIKE-HP
        Source Network Address:    -
        Source Port:               -
Detailed Authentication Information:
        Logon Process:             Advapi
        Authentication Package:    Negotiate
        Transited Services:        -
        Package Name (NTLM only):  -
        Key Length:                0

```

This event is generated when a logon session is created. It is gener
The subject fields indicate the account on the local system which re
The logon type field indicates the kind of logon that occurred. The
The New Logon fields indicate the account for whom the new logon was
The network fields indicate where a remote logon request originated.
The authentication information fields provide detailed information a

- Logon GUID is a unique identifier that can be used to corr
- Transited services indicate which intermediate services ha
- Package name indicates which sub-protocol was used among t
- Key length indicates the length of the generated session k

You need to get information from New Logon->Account Name.
So just input **{New Logon\Account Name}**

You can also specify a description parameter by index. This is helpful if
you have localized version of event descriptions. To specify the
parameter by index, just use input **PARAM[index]**. E.g. to get Account
name, input
{PARAM[6]}

You can input as many parameters as you wish. E.g. if you want to
display user name as DOMAIN\ACCOUNT NAME, you should set value
to
{PARAM[7]}\{PARAM[6]}
or
{New Logon\Account Domain}\{New Logon\Account Name}

Clear column clears this column.

Load column loads this column or all columns from a file.

Save column saves this column or all columns into a file.

See also: [Filter by description params](#)

© 2005-2018 FSPro Labs. All rights reserved.

Computer properties

To display computer properties dialog, highlight the computer in the [Computers tree](#), click right mouse button on it and select Properties from the [context menu](#).

Description - description of the computer. The description will appear in the tree near the computer name in parentheses.

Group - a group to which the computer belongs.

Time correction - a value that will be added to the time of each event on this computer.

Time correction is useful when you want to view event logs as you would be in other timezone. All event logs store event time in UTC. When you view event logs with Event Log Explorer, it automatically converts UTC to your local time. Sometimes you may want to view event logs in their server time zone. To do so, you should set time correction as hour difference between your local time zone and the remote server time zone.

You can press **Calculate** button to automatically calculate such difference.

API to access event logs - Windows API that Event Log Explorer will use to open and read event logs from this computer.

Read [more information about log API](#).

© 2005-2018 FSPro Labs. All rights reserved.

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.

Scheduler

Scheduler lets you automate some tasks.

You can schedule such tasks as Refresh, Export, or Print.

To start Scheduler, select **Advanced-> Scheduler** from the main menu.

To add a new task, click **New Task**. This will display Task Wizard.

In Task Wizard input task name (as you like) and task description.

Click **Next**.

Input when the task will start and specify the recurrence interval.

Click **Next**.

Select what task do you want to automate (Refresh, Export, Print)

Click **Next**.

Depending on your task you may need to fill task options.

Click **Next**, review your input and click **Finish**.

You can assign an unlimited number of tasks for one log view - just click **New Tasks** again to add a new task.

To apply the tasks and activate scheduler, click **OK** button.

Do disable scheduler, remove all tasks (e.g. using **Clear tasks** button).

If you want to apply a task to another log view, you can use **Copy** and **Paste** buttons in Scheduler dialog.

Copy copies highlighted tasks to Windows clipboard and **Pastes a task from clipboard into Scheduler**.

Direct Access to Event Log Files

Standard Windows Event Viewer as well as the overwhelming majority of Windows Event Log software reads Windows event file using Windows Event Log API. Event Log API works perfectly if log files are OK or your log file format is compatible with the API. If your log files are damaged or Event Log functions are inaccessible (e.g. you run Bart PE or you are trying to open EVTX files on Windows XP or 2003) , Windows API will fail.

Direct File Open allows you to read event files without Event Log API functions.

Use Direct File Open (**File->Open Log File->Direct**) every time you open event log file and

1. This file seems to be damaged.
2. You start your computer from Bart PE or similar environment.
3. You computer is running Windows Vista or higher and you need to open legacy .Evt file.
4. Your computer is running Windows XP/2003 and you need to open .Evtx files.

Working with database

You can read events stored in a database and you can upload events into a database table.

Event Log Explorer 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.

Create database

Although it's recommended to create new databases from special tools like SQL Server Management studio, Event Log Explorer lets you create a new database.

To create database, 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 select the required upload options.

- » Append if table exists – if checked, Event Log Explorer will append events to the existing table. If not checked and table exists, Event Log Explorer will delete all events from the table before upload.
- » Export XML data – if checked, Event Log Explorer will extract XML for each event and upload it into the table. This may take long time on large event views, so we recommend using [Event Log Database Export utility](#) to upload events.

Load events from table

To load events from the database, select Database -> Load from table.

Select the required table name and click OK.

Event Log Explore will display events from the database table as a native windows event log.

See also:

[Event Log Database Export utility \(eldbx.exe\)](#)

© 2005-2018 FSPro Labs. All rights reserved.

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*]

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*

Examples:

```
elex.exe C:\Data\MyLogs.elx
```

```
elex.exe /clean /openlog system \\server\security
```

```
elex.exe /openlog system application security
```

```
elex.exe /openfile C:\backup\system.evt "C:\app backup.evt"  
\\server\c$\eventlogs\sysback.evt
```

```
elex.exe /openlog server\security server\system /openfile  
C:\backup\system.evt /clean
```

© 2005-2018 FSPro Labs. All rights reserved.

Preferences

Preferences dialog window allows you to change default Event Log Explorer parameters.

To 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.

Click items as follows defines the controls behavior on single or double click.

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 and **Size** define the default font and its size for main Event Log Explorer window and event log views.

Visual Style defines Event Log Explorer visual style.

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.

Log View Defaults

This 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 Options

Temporary Data Storage sets the location of temporary data. When Event Log Explorer reads events from logs, it uses a temporary storage for these events. You can choose between Memory and Disk storage. Memory is the best choice for relatively short event logs (up to 300 000 events). Disk is good for a large number of events.

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

Window width and **Window height** define event log view window size. These options are effective only for MDI interface.

Open maximized - the new log view window will be maximized in the parent window. This option is effective only for MDI interface.

Display grid lines - if checked, event list will be displayed with grid lines.

Display description box - if checked, when you open a new event log window, the description box will appear in the bottom part of the window.

Description box location - defines the default location of description box in log view windows.

Description box height - defines the height of the description box (in percentage of the log view height).

Description box width - defines the width of the description box (in percentage of the log view width).

Description in line - if checked, event list will be displayed with description column. Multi-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.

Run Add Computers Wizard - if checked, Event Log Explorer will start [Add Computers Wizard](#) to fill in the 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 (auto save workspace) - if checked, the program will always save changed workspace when you close it.

Log Files

Default mode to open .EVT file defines access mode to .evt files when you try to open .evt file.

Standard - Standard Win API access to .evt file. This option is default on Windows NT, 2000, XP, 2003 operating systems.

Direct - Direct access to .evt file. This option is default on Windows Vista.

See also [Direct Access to Event 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.

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.

Updates





Automatically poll for updates - Hide Folders XP 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.

© 2005-2018 FSPro Labs. All rights reserved.

Main menu and toolbar

Main menu command	Toolbar button	Command description
File -> New Workspace		closes the current workspace and creates a new one.
File -> Open Workspace		closes the current workspace and opens saved workspace from a file.
File -> Save Workspace		saves opened workspace to a file.
File -> Save Workspace As		saves opened workspace to a new file.
File -> Open Log		shows the Open Log dialog and lets you open an event log.
File -> Open Log File		shows the Open Log File dialog and lets you pick an event log file to open.
File -> Merge Log		opens event log and merges it with the current event log view
File -> Merge Log File		opens event log file and merges it with the current event log view
File -> Save Log As -> Save Event Log (Backup)		performs full event log backup.
File -> Save Log As -> Save Displayed Events		saves the displayed events into .evt file.
File -> Save Log As -> Save Selected Events		saves the selected events into .evt file.
File -> Clear Log		removes all events from event log.
File -> Log Properties		displays Log Properties dialog for active log view. See also: Log Properties , Computer Properties .
File -> Close		closes current event log window.

File -> Close All		closes all opened event log windows.
File -> Export Log		exports active event log view into different formats.
File -> Print Options		selects the style in which event logs will be printed.
File -> Print Preview		displays active event log view in the print preview window as it would appear when printed.
File -> Print		prints active event log view.
File -> Preferences		displays Preferences dialog to set up Event Log Explorer.
File -> Language		selects user interface language.
File -> Quit		quits Event Log Explorer.
Tree -> Add Group		shows the Add Group dialog and lets you create a new group in the computers tree.
Tree -> Add Computer		shows the Select Computer dialog and lets you add a new computer to the computers tree.
Tree -> Add Computers Wizard		shows the Add Computers Wizard and lets you add several computers to the tree.
Tree -> Remove		removes a selected computer(s) or group(s) from the computer tree.
Tree -> Export		exports computer tree to XML file.
Tree -> Import		imports computer tree from XML file.
Tree -> Connect with different credentials		displays Connect To dialog and connects a remote computer. See also: Credentials conflict .
View -> Show Grid Lines		shows/hides grid lines in the current event log view.
View -> Show Event Descriptions		shows/hides event descriptions box in the current event log view.
View -> Description		shows/hides event descriptions in the

in line		event list.
View -> Configure columns		displays Configure columns dialog and lets you hide/show event log fields.
View -> Rename		changes caption of the current log view.
View -> Newest First		sorts the active event log view from the newest events to the oldest.
View -> Oldest First		sorts the active event log view from the oldest events to the newest.
View -> Filter		shows the Filter dialog to filter events on a specific criteria.
View -> Clear Quick Filters		cancels all quick filters of the active event log view.
View -> Clear Filter		cancels all filters of the active event log view.
View -> Filter enabled		enables and disables active event filter. This lets you easily rollback to unfiltered state, and subsequently reactivate your filter.
View -> Find		shows the Find dialog to search for an event that meets a specific criteria.
View -> Find Next		searches for the next event that meets the criteria, that you entered the last time in Find dialog for a current event log.
View -> XML Query		displays XML query dialog.
View -> Log Loading Options		displays Log Loading Options dialog.
View -> Loading Options Enabled		enables and disables loading options prefiltering. This lets you easily rollback to unfiltered state, and subsequently reactivate your filter.
View -> Only Recent Events After Refresh		After every log view refresh, Event Log Explorer will display only new events that appear since the last refresh/load.
View -> Description Server		displays Description Server dialog.
View -> Time		sets time correction for current log view.

correction

You can also choose UTC time.

View -> Color coding

shows/hides [Color coding](#) dialog to color code events.

View -> Event Properties

shows/hides [Event Properties](#) dialog for the current event log view.

View -> Auto-refresh

enables/disables event log view auto-refresh. When enabled, current event log will be automatically reread every ***Auto-refresh interval***.

View -> Auto-refresh interval

changes auto-refresh interval for current event log.

View -> Refresh



rereads an active event log. Please note, Refresh command resets all Quick filters.

Event ->Copy to Clipboard

copies selected events in the active event log view to clipboard.

Event ->Bookmarks ->Toggle Bookmark

bookmarks/"unbookmarks" current event in the active event log view

Event ->Bookmarks ->Next Bookmark

moves selection to the next bookmark.

Event ->Bookmarks ->Previous Bookmark

moves selection to the previous bookmark.

Event ->Bookmarks ->Bookmark by criteria

displays [Find/Filter](#) dialog and lets to to bookmark events by criteria.

Event ->Bookmarks ->Clear Bookmarks

clears all bookmarks in the active event log view.

Event ->Lookup in EventID.Net Database

tries to find information about current event in EventID.Net knowledgebase.

Event ->Lookup in Microsoft Knowledgebase

tries to find information about current event in Microsoft's knowledgebase.

Advanced ->

displays Credentials manager to set the

Credentials	default credentials for accessing remote computers.
Advanced -> Scheduler	displays Task Scheduler dialog to manage scheduled tasks.
Advanced -> Linked Event Filter	displays Linked Event Filter dialog for active log view.
Advanced -> Analytical Reports	creates Analytical Reports such as pivot tables and pivot charts.
Advanced -> Event Alerter	enables you to automate event log monitoring and alert when a specific event comes. See also Event Alerter .
Window -> Cascade	arranges multiple event log windows in a cascade (overlapped) fashion.
Window -> Tile Vertically	arranges event log windows as non-overlapping vertical tiles.
Window -> Tile Horizontally	arranges event log windows as non-overlapping horizontal tiles.
Window -> Next	switches between multiple event log windows.
Window -> <Event Log Name>	switches to <Event Log Name> event log window.
<i>Note: Window commands are available only for multi-document user interface.</i>	
Help -> Help	shows Event Log Explorer help.
Help -> Check for Updates	connects Event Log Explorer site and check if a new version of the program is available for download.
Help -> Feedback	opens your email client to send a feedback about Event Log Explorer.
Help -> About	shows the About box.

In addition to aforesaid toolbar commands, there is Event Filter menu on the toolbar. It lists previously saved event filters and lets you apply a filter immediately.

See also: [Filter/Search window](#), [General Preferences](#)

© 2005-2018 FSPro Labs. All rights reserved.

Event Log View

Event log view is a visual representation of event log.

Log view consists of

Event list

Control toolbar

Description box

Event list

Event list is the main element of Event Log Explorer. It displays log view as a scrollable table.

The following event log columns are available:

- » Event Type (Information, Warning, Error, Audit Success, Audit Failure)
- » Event Date
- » Event Time
- » Event ID
- » Source Name
- » Category Name
- » User name (including domain name)
- » Computer name
- » Description (if **View -> Description** in Line is enabled).

Some Event Log Explorer commands (e.g. Copy to clipboard) may work with multiple selection.

To select several events in the event list

If they are contiguous:

1. Click the first message
2. Go down the list to the last message
3. Press and hold SHIFT, and then click the last message. The whole set of messages will be selected.

If they are are not contiguous press and hold CTRL, and then click each message that you want to select.







To sort the list by a certain column, click on the column header. Click a second time to reverse the sort order. To sort event list from the oldest events to the newest or visa versa, select **View -> Oldest First** or **View -> Newest First** from the main menu.

To popup [Event list context menu](#) click right mouse button anywhere on the Event list.

See also: [Bookmarking events](#), [Filtering events](#), [Event list context menu](#), [Viewing Event Logs](#)

Control toolbar

Log view control toolbar displays log view status message (e.g. Loading, Filtering, Showing events), event list navigator buttons (First, Previous, Next, Last) and different status indicators:

Indicator	Description
	Log loaded partially. You can double click on this icon to display log loading options.
	Log loading error.
	Time correction is enabled for the computer.
	Autorefresh enabled. You can double click on this icon to change autorefresh interval.
	Non-default description server is set.
	Event log is loaded into memory/temporary file

Description box

Description box displays event description (Description tab) and binary data (Data tab) associated with the selected event.

To hide or show the description box, select **View -> Show Description Box** from the main menu.

© 2005-2018 FSPro Labs. All rights reserved.

Event list context menu

Menu command	Command description
Quick filter by ... Filter	Sets Quick Filter shows the Filter dialog to filter events on a specific criteria.
Clear Quick Filters	Cancels all quick filters
Clear Filter	Cancels all filters
Copy to Clipboard	Copies selected events to clipboard.
Bookmarks ->Toggle Bookmark	Toggles bookmarks/"unbookmarks" selected event
Bookmarks ->Next Bookmark	Moves selection to the next bookmark.
Bookmarks- >Previous Bookmark	Moves selection to the previous bookmark.
Bookmarks ->Clear Bookmarks	Clears all bookmarks.
Lookup in Knowledge Bases- >Lookup in EventID.Net Database	Tries to find information about current event in EventID.Net knowledgebase.
Lookup in Knowledge Bases- >Lookup in Microsoft Knowledgebase	Tries to find information about current event in Microsoft's knowledgebase.
Find	Shows the Find dialog to search for an event that meets a specific criteria.
Find Next	Searches for the next event that meets the criteria, that you entered the last time in Find dialog.
Log Loading Options	Displays Log Loading Options Dialog.

Auto-refresh enables/disables event log view auto-refresh. When enabled, the event log will be automatically reread every ***Auto-refresh interval***.

Auto-refresh Interval changes auto-refresh interval.

Refresh rereads event log. Please note, Refresh command resets all Quick filters.

Event Properties shows/hides [Event Properties](#) dialog.

Log Properties displays [Log Properties](#) dialog.

See also: [Event Log View](#)

© 2005-2018 FSPro Labs. All rights reserved.

Computers Tree

Computers Tree is designed to provide you with quick access to event logs and event log files.

In this section:

[Add Computer to Tree](#)

[Add Group to Tree](#)



[Add Log File to Tree](#)

[Remove Computer or Group](#)

[Sorting Items in Tree](#)

Add Computer to Tree


To add a new computer to the tree:

1. Select **Tree->Add Computer** from the main menu or click  or right click on the computer tree and select **Add Computer**.
2. In the **Select Computer** dialog box, check **Another computer**.
3. Click , then select the computer in the **Browse for Network Computer** dialog box and press OK.
4. Type the computer description in the **Description** field.
5. Select the computer group from **Group** field.
6. Press OK button.

Add Group to Tree

To make the tree more compact and usable, Event Log Explorer allows you to group computers in the tree.

To add a group to the tree:

1. Select **Tree->Add Group** from the main menu or click  or right click on the computer tree and select **Add Group**.
2. In the **Add Group** dialog box, type group name and comment (group description).
3. Press OK.

Add Log File to Tree

Log files are added to the tree automatically when you use **File->Open** command and **Automatically add log files to tree** option is enabled in [Log Files Preferences](#).

Remove Computer Group or Log File

To remove a computer, group or a log file from the tree:

Select the object you wish to delete.

Click  or right click on the computer tree and select **Remove <object>**.

Sorting Items in Tree

To sort items within the same nesting level, right click on the item in the tree and select **Move Up** or **Move Down** from the context menu. You can also use keyboard shortcuts (Alt+Up or Alt+Down).

To move the computer to another group, right click on the computer in the tree and select **Properties** from the context menu. In the **Computers Properties** dialog, change **Group** field and press OK.

© 2005-2018 FSPro Labs. All rights reserved.

Computers tree context menu

Menu command	Command description
Open or Expand	opens event log or expands Group or Computer node.
Open All Logs in Meregger View	unites all event logs from the computer in one new view.
Open in New View	open event log in a new view.
Merge with Current View	unites event log with current event log view.
Close Log(s)	closes corresponding log views.
Connect with Different Credentials	displays connect to computer dialog and lets you to supply username and password to access the remote computer. See also: Credentials conflict .
Add Group	creates a new group in the tree.
Add Computer	lets you add a computer to the tree.
Remove Computer or Remove Group	removes selected computer or group from the tree.
Move Up	moves the selected item in the tree up.
Move Down	moves the selected item in the tree down.
Save Log(s) As	allows you to save the selected event log(s) to file(s)
Clear Log(s)	empties the selected event log(s)
Properties	Displays properties dialog. See also: Log Properties , Computer Properties .

Filter/Search Window

This window allows you to specify the criteria for Filter or Find command.

Apply filter to defines on which views the filter will affect.

Active event log view - if checked, the filter will be applied to current event log view only.

Event log view(s) on your choice lets you select event views to filter.

Event Types:

- » Information - if checked, Event Log Explorer will display/search for events logged by successful operations of major services.
- » Warning - if checked, Event Log Explorer will display/search for events that are not necessarily significant but may cause future problems.
- » Error - if checked, Event Log Explorer will display/search for events logged by significant problems.
- » Audit Success - if checked, Event Log Explorer will display/search for security access attempts that were successful.
- » Audit Failure - if checked, Event Log Explorer will display/search for security access attempts that were failed.

Source - Event Log Explorer will display/search for events logged by a specified software.

Category - Event Log Explorer will display/search for events of a certain category.

User - Event Log Explorer will compare User column with the specified text. The compare is not case-sensitive. If Substring check box is checked, Event Log Explorer will display/search for events that contains this criteria text in the User column.

Computer - Event Log Explorer will compare Computer column with the specified text. The compare is not case-sensitive. If Substring check box is checked, Event Log Explorer will display/search for events that contains this criteria text in the Computer column.

Event IDs - Event Log Explorer will display/search for events that match the specified Event 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**

Text in description - Event Log Explorer will display/search for events that contains the specified text in the event description. Tick **RegExp** checkbox if **Text in description** is a regular expression.

Filter by description params - You can filter security log by description parameters.

E.g. - you have an event (eventid: 4688) with description:

A new process has been created.
 Subject:

```

    Security ID:           S-1-5-21-1388292303-2233603710-27532
    Account Name:         Bob
    Account Domain:      FSPRO
    Logon ID:             0x1af38
Process Information:
    New Process ID:       0x23b0
    New Process Name:     C:\Program Files (x86)\Microsoft Off
    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

Description params match is not case sensitive.

Date - if checked, Event Log Explorer will display/search for events logged between **From** and **To** dates.

Time - if checked, Event Log Explorer will display/search for events logged between **From** and **To** times.

Separately - if not checked, Event Log Explorer will behave as standard Windows Event Viewer: it will display/search for events that fall into date time interval (from **From Date, Time** to **To Date, Time**).

If checked, Event Log Explorer will display/search for events that fall into date interval (from **From Date** to **To Date**) and fall into time interval (from **From Time** to **To Time**). This can be helpful for example, when you want to check the events that were generated last week during the working time.

Display events for the last dd days yy hours - Event Log Explorer will display/search for the recent events logged during the last DD days and yy hours. Set these values to 0 to display all events.

Exclude - you can enable Exclude option for each clause. E.g. if you want to display all events except spooler events, check in the Source drop-down list "Spooler" and enable Exclude option next to the Source drop-down list.

Load button - allows you to load a saved filter/search criteria.

Save button - saves current filter/search criteria in a file.

OK button - closes this window and starts filtering/search process according to the specified criteria.

Cancel button - close this window.

See also:

[Filtering events in Event Log Explorer](#)

© 2005-2018 FSPro Labs. All rights reserved.

XML query

You can use XML query to filter events.

XML queries are executed on target computers, so this way of event filtering may work much faster than others.

To display XML query dialog box, select **View-> XML query** from the main menu of the program.

Type your query (you can use Structured XML Query or XPath 1.0 format).

These two examples show security events with Event ID=5152 or Event ID=5157

```
<querylist>
<query id="0" path="Security">
<select path="Security">*[System[(EventID=5152 or EventID=5157)]]</s
</query>
</querylist>
```

```
*[System[(EventID=5152 or EventID=5157)]]
```

Load button loads XML query from a file.

Save button saves the XML query to a file.

Linked Event Filter

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-1-5-21-2153856534-97633110-1224965
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-1-5-21-2153856534-97633110-1224965
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;0x13
                       ReadAttributes: Granted by   D:(A

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.

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.

Linking Param defines a linking key from event description.

You can define it as Level1\Level2

E.g. if event description contains:

Key1:
 Key11: Value1
 Key12: Value2
Key2:
 Key22: Value3

Here you can refer to Value 1 as Key1\Ket11, to Value 2 - Key1\Key12...

In our example Linking Param would be **Object\Handle ID**.

Depth (events) and **Depth (milliseconds)** define scan depth for linked event from the base event. Typically it should not exceed 10 events.

Exclude base eventbase 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 **linked param** value and starts an inner scan for **linked event id** with the same value of **linked param**. 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.

Note: Linked event filter is not saved in the program workspace file.

See also:

[Filtering events in Event Log Explorer](#)

Select computer dialog

This dialog window allows you to add a computer to the computers tree.

Local computer - click this option if you want Event Log Explorer to add your local computer. By default, your local computer is already added to the computers tree.

Another computer - type the name of the target computer in the input line or click Browse button to select the remote computer from the dialog window.

OK button - closes this dialog and adds the computer to the computers tree.

Cancel - closes this dialog window.

Note: If you have Windows XP workstations over the peer-to-peer network please read [Peer-to-peer network issues](#).

© 2005-2018 FSPro Labs. All rights reserved.

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 **View->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.

Peer-to-peer network issues

This topic is only for workgroup network users.

When connecting to another Windows computer some non-default security options need to be set on the target computers, or Event Log Explorer may return the message "Access is denied".

If the target Windows computer is a workgroup computer rather than a domain, then the default setting for remote log in is 'guest', which is not enough security level to manage event logs.

How to fix the problem.

Under **Control Panels > Administrative Tools > Local Security Policy > Security Options > Network access: Sharing and security model for local accounts**, change **Guest Only - Local users authenticate as guest** to **Classic - Local users authenticate as themselves**.

Here is the step-by-step instruction:

1. Log on to the target Windows computer with Administrator rights.
2. Click Start and select Control Panel.
3. Make sure that the Control Panel displays its icon in Classic View (To switch Control Panel from Category view to classic view you should click **Switch to Classic View** on the left pane of Control Panel window)
4. Double click the **Administrative Tools** icon.
5. In the Administrative Tools window, double click **Local Security Policy**.
6. In the Local Security Settings window, in the left-hand pane, double click **Local Policies** then click **Security Options**.
7. In the right-hand pane, double click **Network Access: Sharing and security model for local accounts**.
8. In the dialog box, select option to **Classic – local users authenticate as themselves**.
9. Click **OK** button

Note. With classic security model your users should not have blank passwords because it will be possible to crack into the workstation by unauthorized persons. If your users will have blank passwords anyway double click **Accounts: Limit local account use of blank passwords to console logon only**. In the dialog box, select option to **Disabled**.

Repeat this procedure on each Windows computer in the workgroup.

UAC remote restrictions

Starting from Windows Vista, Windows operating system is protected by User Account Control (UAC).

When a user who is a member of the local administrators group on the target remote computer establishes a remote administrative connection, they will not connect as a full administrator. The user has no elevation potential on the remote computer, and the user cannot perform administrative tasks.

Remote Registry

Remote Registry Service must be running on the target machine.

© 2005-2018 FSPro Labs. All rights reserved.

Event Log Backup utility (elback.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.

ELBACK BatchFile

runs **BatchFile** to backup logs.

ELBACK 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:

```
ELBACK batchfile.elb
```

backup Security log from Serv01 to C:\Backup:

```
ELBACK C:\Backup Security Serv01\Security
```

backup all logs from Serv01, Serv02 and Serv03 to C:\My Backup, then clear them:

```
ELBACK "C:\My Backup" \\Serv01\* \\Serv02\* \\Serv03\* /Clear
```

backup Directory Service from Serv01 to C:\My Backup:

```
ELBACK "C:\My Backup" "\\Serv01\Directory Service"
```

See also:

[Event Log Database Export utility \(eldbx.exe\)](#)

© 2005-2018 FSPro Labs. All rights reserved.

Event Log Database Export utility (eldbx.exe)

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}]
```

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}	<p>Specifies what to do if table already exists.</p> <p>Values:</p> <ul style="list-style-type: none"> fail - quit application with error. append - append events to the table. overwrite - delete existing and write new. <p>Optional. Default value: fail.</p>
/HOST	<host_name>	<p>Specifies host name to read events from.</p> <p>Optional. Localhost is implied.</p>
/USER	<user_name>	<p>Specifies user name to access logs on host.</p> <p>Optional.</p>
/PASSWORD	<password>	<p>Specifies user password to access logs.</p> <p>Optional.</p>
/LOGNAME	<log_name>	<p>Specifies log name to export.</p> <p>Mandatory if /QUERY not specified.</p>
/QUERY	<query_file_name>	<p>Specifies file containing XML query to get events for export.</p> <p>Mandatory if /LOGNAME not specified.</p>
/EDR	{all ri render no}	<p>Specifies event description rendering options.</p> <p>Values:</p> <ul style="list-style-type: none"> no - do not render event

		<p>description.</p> <p>render - render event description.</p> <p>ri - use event RenderingInfo.</p> <p>all - try RenderingInfo, if not available,</p> <p>render description.</p> <p>Optional. Default value: all.</p>
/CLEARLOG	{no yes tolerate}	<p>Option to clear event log after export.</p> <p>Values:</p> <p>no - do not clear event log.</p> <p>yes - clear event log.</p> <p>tolerate - clear event log, do not report error if clearing fails.</p> <p>Optional. Default value: no.</p> <p>NOTE. "Export&clear" is not an atomic operation! There is a chance that some events appear after export and before clearing!</p>
/VERBOSE	{0 1 2}	<p>Specifies verbosity level.</p> <p>Values:</p> <p>0 - display all information.</p> <p>1 - display warning and errors.</p> <p>2 - display errors only.</p> <p>Optional. Default value: 2.</p>

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}]

```

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}	Specifies verbosity level. Values: 0 - display all information. 1 - display warning and errors. 2 - 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  
/TXA:append /HOST:Host /LOGNAME:System /USER:Administrator  
/PASSWORD:password
```

See also:

[Working with database
Event Log Backup utility \(elback.exe\)](#)

© 2005-2018 FSPro Labs. All rights reserved.

FSPRO LABS
Event Log Explorer.
END USER LICENSE AGREEMENT
LICENSE AGREEMENT

This End User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and FSPro Labs ("FSPRO") for the SOFTWARE(s) identified above, which includes the User's Guide, any associated SOFTWARE components, any media, any printed materials other than the User's Guide, and any "online" or electronic documentation. By installing, copying, or otherwise using the SOFTWARE, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE.

FSPRO and/or its licensors reserve All rights not expressly granted herein.

The SOFTWARE is licensed, not sold.

The SOFTWARE is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties.

1. DEFINITIONS

"Server" means a computer running Microsoft Windows server operating system, including, but not limited to Windows NT server, Windows 2000 server, Windows 2003 server, Windows 2008 server or a computer running

Microsoft Windows workstation and operating for the purpose of serving other computers logically or physically connected to it.

"Workstation" means a computer running Microsoft Windows workstation operating system, including, but not limited to Windows NT workstation, Windows 2000 professional, Windows XP, Windows Vista and which does not fall under definition of "Server"

"Personal use", "Personal user" mean the non-commercial use of the SOFTWARE

in your ("Personal user") home.

"In-house use", "In-house user" means the commercial or non-commercial use of the SOFTWARE within company (organization), by employees (in-house users) of the company (organization) and for the sole purpose of processing and managing data from the company's (organization's) computers.

"Licensed version" means a version of the SOFTWARE that has been licensed for any use (commercial or noncommercial).

"Unlicensed version" means the free version of the SOFTWARE during the evaluation period.

2. GRANT OF LICENSE

1) Unlicensed version

Anyone may use this software during a test period. Following this test period, if you wish to continue to use this software, you must get the license(s). To get the license you should pay the license fee or get the free license for Personal use.

2) Licensed version.

a) Per-user licensing model.

The SOFTWARE is licensed on per-user basis for any use.

You are granted to install this SOFTWARE for a number of users that does not exceed the number of users indicated in your license key.

b) Per-server licensing model.

If you fall under the definition of "In-house user", you MAY license the SOFTWARE on per-server basis.

With this SOFTWARE you are granted to access a number of servers that

does not exceed the number of servers indicated in your license key.

c) Licensed version for personal use

If you fall under the definition of "Personal user", you may get Personal license of the software for noncommercial use.

With Free Personal license you may not access more the 3 computers

(servers or workstations). With Paid Personal license you may not access more than 10 computers.

3. RESTRICTIONS

You may not use, copy, emulate, clone, rent, lease, sell, modify, decompile, disassemble, otherwise reverse engineer, or transfer the licensed program, or any subset of the licensed program, except as provided for in this agreement.

Any such unauthorized use shall result in immediate and automatic termination of this license and may result in criminal and/or civil prosecution.

4. TERMINATION

Without prejudice to any other rights, FSPRO may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the SOFTWARE.

5. NO WARRANTIES

FSPRO EXPRESSLY DISCLAIMS ANY WARRANTY FOR THE SOFTWARE.

THE SOFTWARE AND ANY RELATED DOCUMENTATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON INFRINGEMENT. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE REMAINS WITH YOU.

6. LIMITATION OF LIABILITY. NO LIABILITY FOR CONSEQUENTIAL DAMAGES

IN NO EVENT SHALL FSPRO BE LIABLE TO YOU FOR ANY DAMAGES OF ANY KIND ARISING OUT OF THE DELIVERY, PERFORMANCE, OR USE OF THE

SOFTWARE, EVEN
IF FSPRO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH
DAMAGES.
IN ANY EVENT, OUR LIABILITY FOR ANY CLAIM, WHETHER IN
CONTRACT, TORT,
OR ANY OTHER THEORY OF LIABILITY SHALL NOT EXCEED THE
LICENSE FEE PAID BY YOU.

7. SEVERABILITY

If any provision or part of this EULA is held to be invalid, illegal or unenforceable, the validity, legality or enforceability of the remainder of this Agreement will not in any way be affected or impaired, unless the invalidity, illegality or unenforceability completely nullifies this EULA.
