

More Information about Event Log Audit Professional

Since the introduction of Windows NT platform by Microsoft, network administrators have struggled a lot with the task of maintaining their event logs on their networks. Every Windows NT machine either it's a Workstation or Server, has three types of event logs:

1. Application Logs
2. Security Logs
3. System Logs

All three of these event logs serve an essential purpose, such as reporting on the status of applications, auditing access attempts on computers throughout the network, and indicating potential hardware problems before they become terrible.

Although event logs plays very significant role in network management but they do create problems for network administrators because they grow in size rapidly. In some cases, administrators may choose to make NT machines overwrite old event log entries when the logs become full and continue in a circular fashion. In most security conscious organizations, however, this is avoided since vital information is lost and unrecoverable in this way. On the other hand, administrators can set up their NT/2000 machines so that no information is overwritten or lost. Unfortunately, for this administrator have to clear each log by hand using the Event Viewer application that is shipped with Windows NT/2000. Obviously, in a LAN containing hundreds or more computers, it's next to impossible to maintain each computer's event logs by hand and is appalling.

Even if administrators write scripts to insure the timely backup and clearing of his/her server's event logs, finding away to centralize the data collected from the computers on LAN is another problem. Most organizations require that the log data be stored in different formats, such as Microsoft SQL Server database format. Gathering the data manually in multiple formats for long term storage simply requires a lot of time to implement. Too often, logs get misplaced or neglected, and critical security data is not readily available in the event of a network attack.

Finally, there is no native way in Microsoft Windows NT itself to push out a unified event logging strategy to all of the servers and workstations which comprise a Windows NT/2000 domain.

This is where EMCO Event Log Audit Professional fits to fulfill your needs. It's a very powerful tool brought to you by EMCO Software while keeping all the need of the network administrators in maintaining event logs on networks. ELA Pro is a tool for scanning, storing, and manipulating event log data on a LAN. It stores the event log data from all machines on a LAN to a powerful Microsoft SQL Server database where you can search for any details such as Event ID, Type, Category, Source, User SID, string from the event Message, and Time period, by applying your SQL Queries. You can build

your custom queries through powerful and flexible Query builder of EventLog Audit Professional. You can define an alert from any of these details which will be sent to you by email, with or without an attachment (available in several formats).

EMCO EventLog Audit Professional uses a DCOM service that is automatically sent to the remote computers in order to collect the events. The collection of event logs can be scheduled to run at certain intervals and for certain computers. The collected event logs can be backed up and cleared at the remote end, to avoid collecting the same data, if required. You can also export selected events from an advanced search function to text, PDF, HTML, RTF, and JPEG, and mail attachments can be selected for the same formats.

EMCO EventLog Audit Professional has the following functionality:

- ✧ Scan a LAN for any or all event log data
- ✧ Update the scan data automatically or manually
- ✧ Easily integrated with Ms. SQL Server Database
- ✧ More Powerful, flexible and reliable database.
- ✧ Define custom Event Log criteria
- ✧ Build and Execute your own SQL Queries
- ✧ Powerful and flexible built-in Query Builder
- ✧ Visual Query builder, you can even build SQL Queries without knowing SQL
- ✧ Built-in SQL Editor
- ✧ Define alerts which can be emailed to you as they occur
- ✧ Save LAN data in a SQL server database
- ✧ Chart event log data
- ✧ Print event log data
- ✧ Export event log data to a variety of different formats
- ✧ Find specific events with an advanced search feature
- ✧ Find specific events by defining custom auto filter
- ✧ Backup event log data

The main features of Event Log Audit are described below:

- ❖ **Enumerate LAN** - The main function of EMCO Event Log Audit is to scan a LAN and collect a wide variety of machine-specific data. This process creates a new set of data - all of the old data will be replaced for this. The following scanning options are available:
 - ❖ **Enumerate LAN via IP Name** - Opens a filter window that allows you to choose the required network provider and domain, an range of IP addresses for new machines, and a list of specific IP addresses to ignore.
 - ❖ **Enumerate LAN via Domain Name** - Opens a filter window that allows you to choose the required network provider and domain to scan.
- ❖ **Save Alert Data to SQL Server Database** –Now EMCO EventLog Audit Professional supports Powerful SQL Server Database. Which gives you more flexibility and power; you can utilize the power of SQL Server.
- ❖ **Define Custom Queries**– New EMCO EventLog Audit Professional enables you to to define custom SQL Queries on the Event Log database.
- ❖ **Flexible visual Query Builder**– New EMCO EventLog Audit Professional comes up with a powerful visual Query builder that enables you to define SQL queries more easily in record time. So, if you are not a SQL expert you can use utilize the powers of EventLog Audit Professional’s powerful Query builder.
- ❖ **Built in SQL Editor**–EMCO EventLog Audit Professional has a built-in SQL query editor that enables you to write and customize your SQL queries enables you to to define custom SQL Queries on the Event Log database.
- ❖ **Setting alerts** -You can define specific types of events, called alerts, that you want to be able to view as a separate group or have an email notification sent to you when they occur. You can specify as many alerts as required, and they can be very general (all Security events) or very specific (all Application events with an event ID of 2300).
- ❖ **Emailing new alerts** - You can set EMCO EventLog Audit Professional to automatically email you the details of any new alerts as they occur. You need to be able to access an SMTP server to use this feature.
- ❖ **Editing an alert** - You can edit the properties of an event alert at any time. The edited alert will be used in the next LAN scan.
- ❖ **Deleting an alert** - You can delete an event alert at any time. The deleted alert will not be used in the next LAN scan.
- ❖ **Displaying current alerts** - You can display all the alerts that have been logged by the most recent scan in one window. This allows you to see all the most recent alerts quickly in one window. You can then sort or print these items, as required.

- ❖ **Backing up event log data** - You can set EMCO EventLog Audit Professional to backup each machine's event log each time it is scanned. This allows you to keep an accurate record of events as they occur over time. You can also delete the event log after each scan, if required.
- ❖ **Finding a specific event** - EMCO EventLog Audit Professional has a powerful sorting search function that allows you to display only certain types of events. The search can be very general (all Security and Custom events) or very specific (all Application events with an ID of 2300 that were logged between the 10/01/2003 and 12/01/2003). You can print the found data or save to disk in a variety of output formats.
- ❖ **Reporting**- There are several different ways you can generate reports in EMCO Event Log Audit. The following functions are available:
 - ❖ **Reporting to the screen** - Generates a report that is available for immediate printing to hardcopy.
 - ❖ **Reporting to a file** - Generates a report file in a variety of different formats.
 - ❖ **Export to Excel** - Generates an Excel report.
- ❖ **Generating an on-screen report** - You can generate a report that is available for immediate printing to hardcopy. You can choose what information you want to include in the report. This does not save the report in an electronic format.
- ❖ **Generating a report file** - You can generate a report file in a variety of different formats. The following formats are available:
 - ❖ **Plain text** - One .txt file.
 - ❖ **PDF** - One .pdf file.
 - ❖ **HTML** - Each computer and tab is a separate .html page.
 - ❖ **XML** - XML file
 - ❖ **Excel** - One Excel file.
 - ❖ **RTF** - One .rtf file.
 - ❖ **Bitmap** - Each computer and tab is a separate .bmp file.
 - ❖ **JPG** - Each computer and tab is a separate .jpg file.

You can choose what information you want to include in the report. This does not allow you to print the report immediately.
- ❖ **Exporting to Excel** - You can generate an Excel file of any or all of the scanned LAN data.
- ❖ **Charting Scan results** -EMCO Event Log Audit has a powerful built charting tool that enables you to Chart the scan tool results in a wide variety of charts. The following type of charting support is available in Event Log Audit
 - ❖ Pie Chart,
 - ❖ Bar Chart
 - ❖ Line Chart

You can also print the results, if required

- ◊ **Exporting charts** - You can export chart data in the following formats:
 - ◊ Text
 - ◊ HTML
 - ◊ XML
 - ◊ Excel
 - ◊ Bitmap

- ◊ **Exporting event data** - You can export event data into a variety of different file formats. The following formats are supported:
 - ◊ Text
 - ◊ HTML
 - ◊ XML
 - ◊ Excel
 - ◊ PDF
 - ◊ RTF
 - ◊ JPG

- ◊ **Creating a database** - You can create a database in EMCO Event Log Audit Pro in two ways:
 - ◊ Scan a LAN and then save the results to a new file.
 - ◊ Create a new database, and then scan the LAN.

- ◊ **Questions that Event Log Audit Pro can help you answer:-**
 - ◊ Is it possible to define alerts which can be emailed to you as they occur?
 - ◊ Can I save the Events log data to a SQL database, through which I can utilize the powers of SQL server?
 - ◊ Is there any tool that allows me to define my custom queries on my Event log data
 - ◊ Can I Chart event log data?
 - ◊ I want to export event log data in different formats like Text, HTML, XML, Excel, PDF, RTF or JPG; is it possible?
 - ◊ Can I find specific events?