

SeNTry ELM Product Guide



Event Log Alert Management for Windows NT

June 1996

Release 1.6



Serverware Group plc
Denton House,
40-44 Wicklow Street,
London WC1X 9HL
United Kingdom

Tel: +44(0)171 419 2020 Fax: +44(0)171 419 2030
email: sales@serverware.com
[http: www.serverworld.com](http://www.serverworld.com)

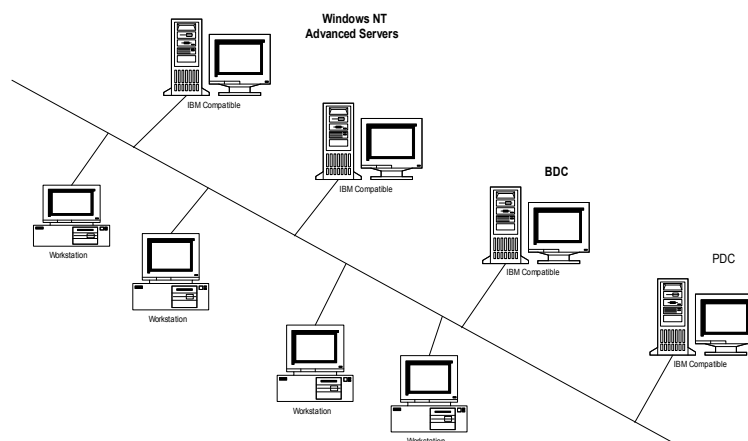
"SeNTry ELM" is a trademark of Serverware Group plc
"Windows" and "Windows NT" are trademarks of Microsoft Corporation

Contents

- 1. INTRODUCTION.....
- 2. HARDWARE AND SOFTWARE REQUIREMENTS.....
- 3. THE PRODUCT.....
 - 3.1. SENTRY ODBC CONFIGURATION.....
 - 3.2. SAGS (SENTRY ALERT GATHERING SERVICE).....
 - 3.2.1. *SeNTry Alert Gathering Service (SAGS) Configuration*.....
 - 3.3. SASS (SENTRY ALERT SENDING SERVICE).....
 - 3.3.1. *SeNTry Alert Sending Service (SASS) Configuration*.....
 - 3.4. ALERTS AND FILTERS.....
 - 3.4.1. *SeNTry Alerts & Filters Configuration - Filters*.....
 - 3.4.2. *SeNTry Alerts & Filters Configuration - Red Alerts*.....
 - 3.4.3. *SeNTry Alerts & Filters Configuration - Amber Alerts*.....
 - 3.5. MAPI.....
 - 3.6. SENMON (SENTRY MONITOR).....
 - 3.7. SENTRY SERVICE MANAGER.....
 - 3.8. LICENSES.....
 - 3.9. SENTRY REGISTRY BUILDER.....
- 4. THE BENEFITS OF SENTRY ELM.....
- 5. AVAILABLE DOCUMENTATION.....
- 6. PRODUCT ROADMAP.....

1 Introduction.

SeNTry ELM is an Event Log Alert Management System for Microsoft Windows NT. It monitors, collects, and filters Events from Windows NT Servers and Workstations and forwards them to one or many master Event Log Gatherers in a domain(s) or trusted domain(s). Event conditions determined as CRITICAL can be automatically forwarded in real-time together with email Escalation via the MAPI interface for MS Mail or MS Exchange users.



The information from Events is stored in an ODBC compliant database format i.e. MS Access, SQL Server, Oracle etc.. Multiple databases can be deployed as Events can be hierarchically filtered to regional network administration centers. Events can be displayed using the SeNTry Monitor. The monitor starts as an icon which, when activated, lists the available SASS servers. Once a Server is selected from the list displayed, the system drills down to the individual Event Log details.

2 Hardware and Software Requirements

The SASS (Sending Service) can run on the Intel version of the Windows NT operating system (Alpha & PPC versions will be available shortly) and can be used on both NT Server and NT Workstation. Installation requires under 1MB of disk space. The service uses little resource when running and is only activated when Event Log records are generated.

The Gathering Service (SAGS) and the SENCONF and SENMON programs require Windows 3.51 or later as they utilise 32bit OCX controls and the new ODBC 2.5 32bit drivers which do not work with earlier releases.

Installation can use up to 8mb of disk space depending on what products are already installed. The size of the ODBC Access Database must also be allowed for.

SeNTry ELM is not reliant upon any particular network transport or protocol and will work with any network configuration.

SeNTry ELM can be installed from the "setup" CD-ROM (or alternatively from our web site - <http://www.serverworld.com>).

In addition, SASS can be remotely installed & configured by the SASS Installation for the main server, NT Security permitting!

SeNTry ELM is initially licenced for 4 Servers for a 30 day evaluation period. The codes to extend this period can be purchased from Serverware Group plc.

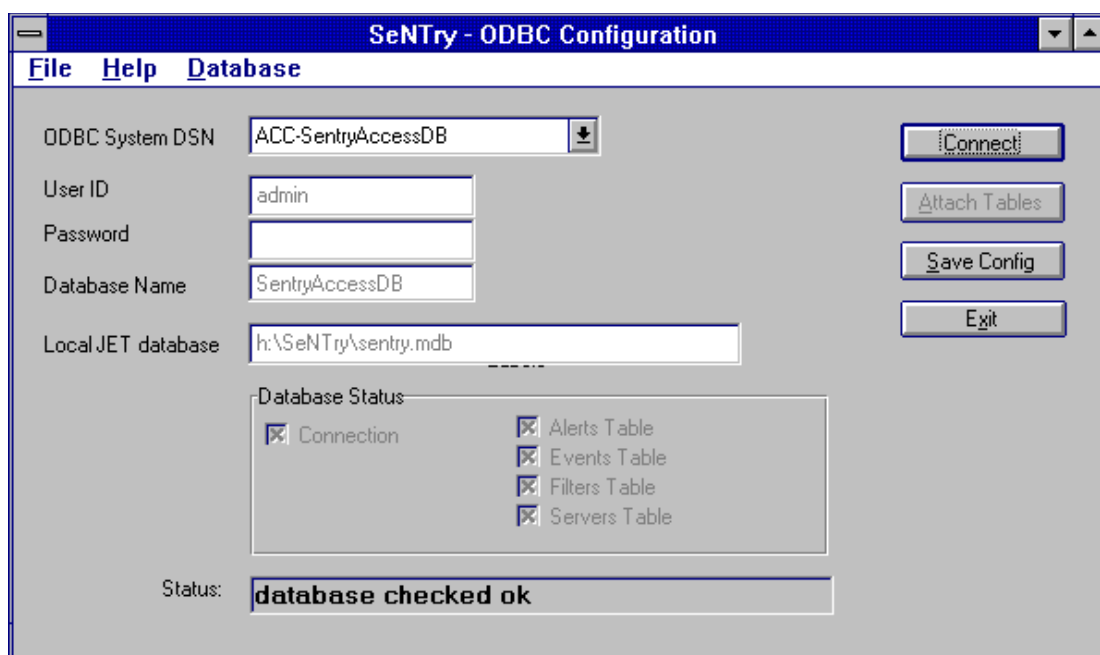
SeNTry ELM is currently ported to INTEL versions of Windows NT and will not work with other processor architectures. ALPHA support will be implemented in version 1.6.2 which is scheduled for release at the end of June 1996.

3 The Product

SeNtry ELM provides the Windows NT network administrator(s) with the ability to centrally view and manage multiple Event Logs from multiple servers. In addition the system provides optional filtering out of unimportant events as well as real time alerting of all conditions categorised as Red or Amber. All event data is stored in an ODBC compliant relational database such as SQL Server for further analysis if required.

3.1 SeNtry ODBC Configuration

SeNtry ELM is attached to an industry-standard ODBC database (a Microsoft Access database is shipped as standard). All messages are sent to this database. An SQL script is supplied with SeNtry ELM to act as a template for creating your own databases.




3.2 SAGS (SeNTry Alert Gathering Service).

This is a service which runs on a designated NT Server. It 'listens' on the network for connections from remote SeNTry ELM services in order to receive filtered and alerted events, which it then writes to the database defined in the SeNTry ODBC Configuration program. It also 'signals' the SENMON monitor if it is running as an icon if the colour of the traffic light needs to be changed and communicates with MAPI or MS Exchange if mail needs to be sent. SAGS also checks to make sure that the licenced number of servers is not exceeded.

3.2.1 SeNTry Alert Gathering Service (SAGS) Configuration.

This program controls the SAGS service on the local machine. It is used for installation and removal, setting parameters, and starting and stopping the service. It is also used for setting trace file options (debug level). A startup delay can also be entered. This is useful if an SQL database is used, as it gives SQL time to start before SAGS does.

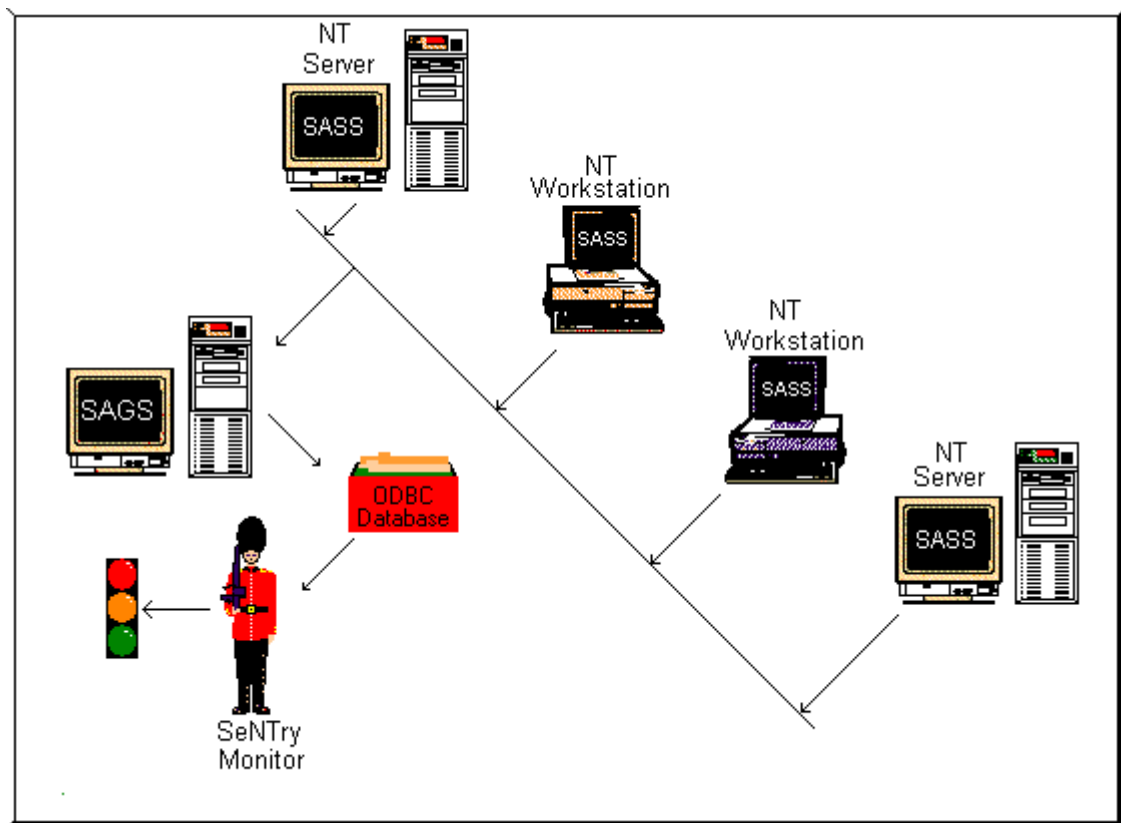
Gatherer Configuration for Server BACKUP

Log File Name	<input type="text" value="h:\SeNTry\sags.log"/>	<input type="button" value="OK"/>
Debug Level	<input type="text" value="0"/>	<input type="button" value="Cancel"/>
Inactivity Time (mins)	<input type="text" value="600"/>	
Send Events Onwards	<input type="text" value="N"/>	
Spawn Command	<input type="text"/>	
Spawn Parameters	<input type="text"/>	
Spawn Time (hh:mm)	<input type="text"/>	
Startup Delay (mins)	<input type="text"/>	
Version	<input type="text" value="1.6"/>	
Service Component Directory	<input type="text" value="h:\SeNTry"/>	

3.3 SASS (SeNtry Alert Sending Service).

This is a service which runs on all Windows NT systems for which Event Log management is required. It communicates via Named Pipes with the SAGS (SeNtry Alert Gathering Service) on a Windows NT server. SASS receives updated information from the SAGS regarding alerts and filters as they become available. Otherwise, it sits waiting for Alert Logs to change, whereupon it applies filters. If unfiltered, it then applies alerts to raise the level if appropriate. Batched Events are then sent to the SAGS via NAMED PIPES to be inserted into the database.


It can be seen that the normal requirement is one server running SAGS, SENMON and the SeNtry Configuration programs (this machine can also run SASS to monitor its own Events!) and several remote machines running just the SASS service.



3.3.1 SeNtry Alert Sending Service (SASS) Configuration.

This program controls the SASS service on local and remote machines. It is used for installation and removal, setting parameters, starting and stopping the service, configuring which server is to handle the Events and Alerts and for setting trace file options (debug level). It is also used to handle Service monitoring and Process monitoring. A startup delay can also be specified to minimise overhead during bootup.

Sender Configuration for Server BACKUP

 SAGS Host

Log File Name

Debug Level

Buffer File

Buffer Cycle Time (secs)

Last Event Recv'd

Send Alerts Directly Service Check Time (mins)

Process Check Time (mins)


Spawn Batch Command (full path & name)

Spawn Parameters


Spawn Time (hh:mm) Filter Flag

Max recs in buffer Recs before send

Startup Delay (mins) Process Delay (Y/N)

Service Component Directory 

Sender Installation Setup

Mapped / Local Drive for installation 

Actual Drive & Path if above drive is remote connection


SASS Server Name

Sentry Sub-Directoy

User ID for Service Start e.g. DOMAIN\AdminUser

Password

Start Service Automatically at Startup

Location of SASSInst INI File 

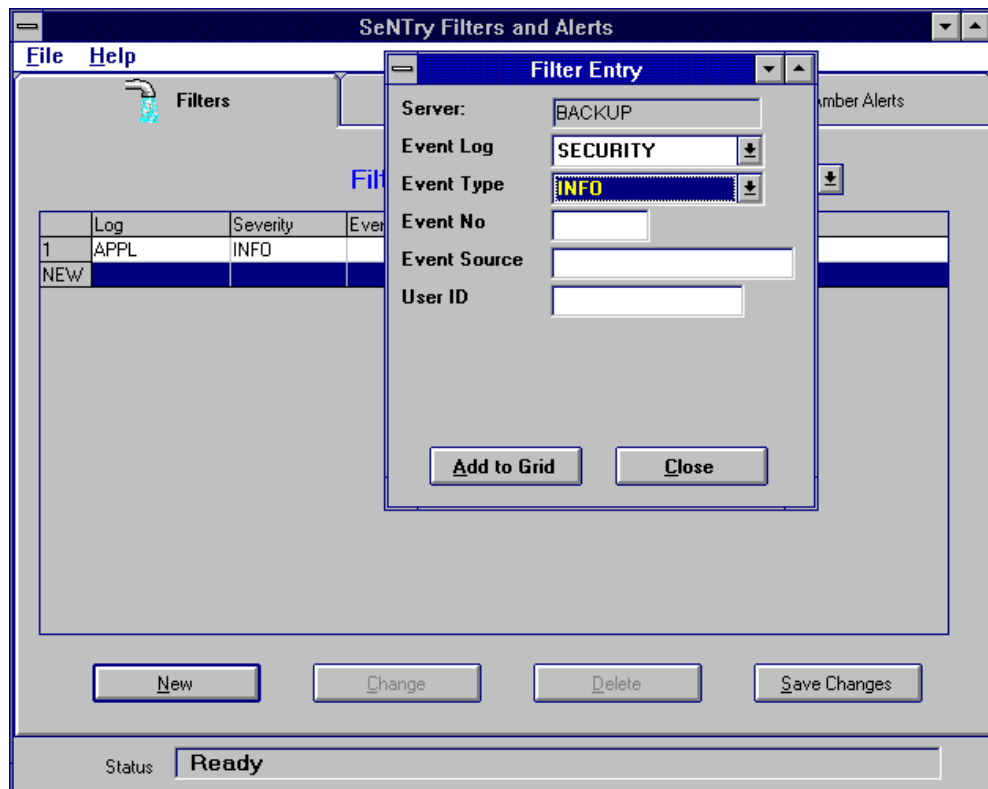
3.4 Alerts and Filters

3.4.1 SeNTRY Alerts & Filters Configuration - Filters

This section describes the 'filters' that determine which Event Log records are not to be passed to the Gathering Service. Selection of filters can be made on any combination of the following fields:

- Event Log File (System, Application or Security).
- Severity (Stop,Warn,Info,Security Violation)
- Event Number
- Event Source (using * for pattern matching)
- Event Category " " " " "
- User ID " " " " "
- The descriptive text associated with an Event

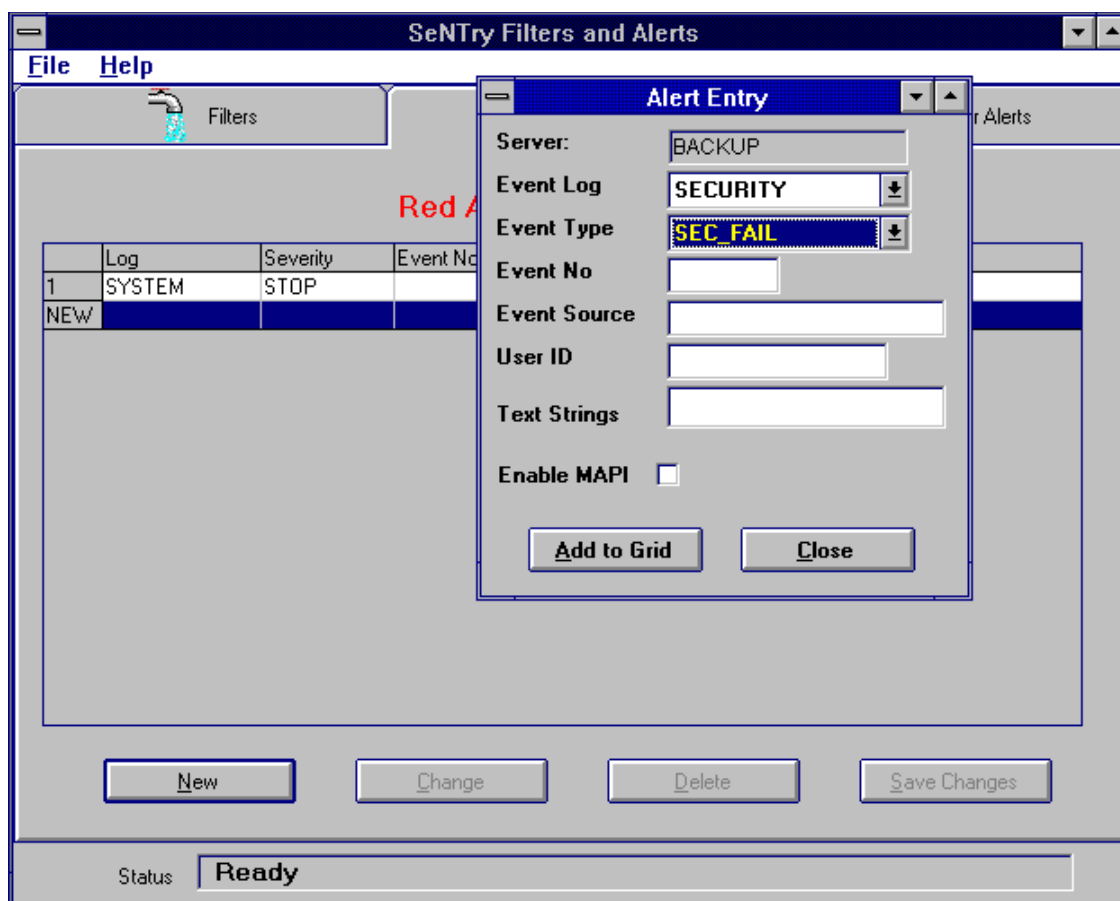
Filters can be defined as "Global" to apply to all servers or set for specific servers. Selection can be made using simple "pattern matching" on text strings.



3.4.2 SeNTRY Alerts & Filters Configuration - Red Alerts.

This program defines 'red alerts' that determine which events are considered 'critical' and will set the red traffic light on the monitor. This definition is performed in an identical manner to the definition of filter records.

When the box "Enable MAPI" is checked, any alerts which match the criteria selected will cause a Mail message to be sent (see **MAPI Configuration**).



3.4.3 SeNTRY Alerts & Filters Configuration - Amber Alerts.

This program defines 'amber alerts'. These are dealt with in the same way as red alerts except that they set the amber light.

3.5 MAPI

SeNTry ELM can be configured to send Electronic Mail to specific users when critical events occur, using MS Mail or MS Exchange. This is selectable on installation. The Definition of MAPI critical alerts is independent of the "red, amber, green" metaphor employed by SeNTry ELM.

Mail can be sent to different support staff (or anybody else) at different times, depending on the entries in a grid which takes account of shift patterns and associated personnel availability. Messages can be sent immediately they are received or 'batched' to be sent at given intervals.

A separate message can be sent at the 'End of Day' to show the overall number of alerts received for each monitored server.

SeNTry - MAPI Configuration

File Help Disable

Buffer File: h:\SeNTry\sags.mpi Profile Name: LOGOFF

Alert Interval: 10

User for selected cells: Alan Stretton P.O. Insert CLR Grid

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
00:00-03:00							
03:00-06:00							
06:00-09:00							
09:00-12:00		Selim Kohen	Selim Kohen	Selim Kohen	Alan Stretton	John Lawson	
12:00-15:00		Selim Kohen	Selim Kohen	Selim Kohen	Alan Stretton	John Lawson	
15:00-18:00		Selim Kohen	Selim Kohen	Selim Kohen	Alan Stretton	John Lawson	
18:00-21:00						John Lawson	
21:00-24:00							

EOD Message to: Dave Toms P.O. at 18:00 Update

Escalation Message to: Neil Lofts P.O. after 30 mins Exit

Status: Ready

Escalation

It is possible to specify a recipient of Escalation messages, i.e. if the user who would normally deal with E-Mail sent by SeNTry ELM does not read their message within a specified period after receipt, SeNTry ELM will send a message to another user.

Escalation will be to a mailbox, radio pagers or cellular telephones.

Escalation is only available under Microsoft Exchange.

3.6 SENMON (SeNtry Monitor).

This is the users 'front end' to the SeNtry ELM product which can run on NT Server or NT Workstation. It comprises a Windows program which is normally left to run as a floating Icon using a 'traffic light' metaphor. It is also incorporated into the NT v.4.0 Taskbar



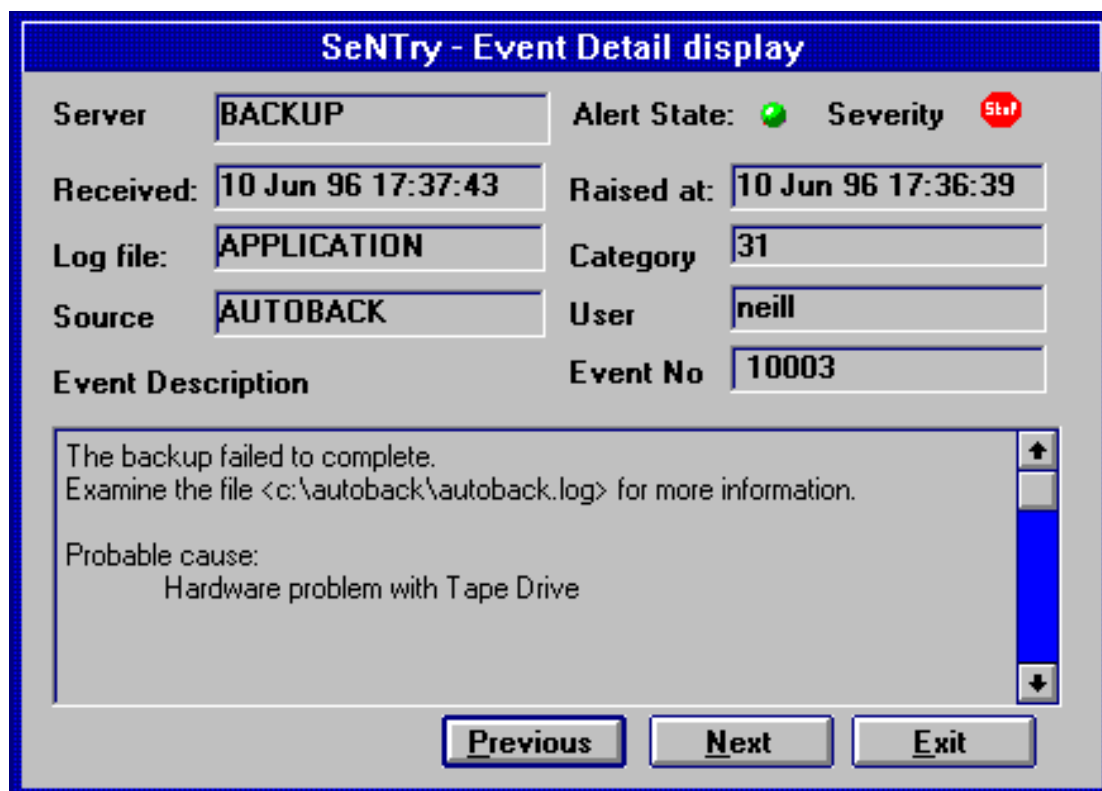
The light is normally green but changes to amber or red as 'critical' events are received into the ODBC relational database. The user can click on the icon to reveal a window showing the summary alert state of all monitored servers. He can click on any server to 'drill down' to a summary of that event and click further to reveal the full detail of the original Event Log record.

SeNtry server monitor				
File Configure Help				
server	last information	red	amber	green
(all servers)	10 Jun 96 17:51:43	31	230	3252
BACKUP	10 Jun 96 17:51:43	8	1	14
CASTOR	10 Jun 96 15:17:12	18	6	2421
URANUS	10 Jun 96 16:10:23	5	221	353
JUPITER	10 Jun 96 16:18:47	0	2	464
SATURN	10 Jun 96 16:18:02	0	0	0

SeNtry - Event Browser							
Help							
Server		BACKUP	Last Information		10 Jun 96 17:48:42	Reds	31
Event Types		RED:AMBER+GREEN	Last Cleared		10 Jun 96 16:51:28	Ambers	230
						Greens	3251
A	S	L	Time Rcvd	Source	Event	Server	Description
		A	10 Jun 17:48	SAGS	801	BACKUP	Failed to logon user MS Exchange Settings to
		A	10 Jun 17:48	SAGS	801	BACKUP	Failed to logon user MS Exchange Settings to
		S	10 Jun 17:47	NETLOGON	5719	BACKUP	No Windows NT Domain Controller is available
		S	10 Jun 17:47	NETLOGON	5719	BACKUP	No Windows NT Domain Controller is available
		A	10 Jun 17:40	SAGS	806	BACKUP	MAPI Information message.
		A	10 Jun 17:39	AUTOBACK	10003	BACKUP	The backup failed to complete. See the autoback
		A	10 Jun 17:37	AUTOBACK	10003	BACKUP	The backup failed to complete.
		A	10 Jun 17:33	SAGS	801	BACKUP	Failed to logon user MS Exchange Settings to
		A	10 Jun 17:33	SAGS	801	BACKUP	Failed to logon user MS Exchange Settings to
		S	10 Jun 17:32	NETLOGON	5719	BACKUP	No Windows NT Domain Controller is available

Include all events

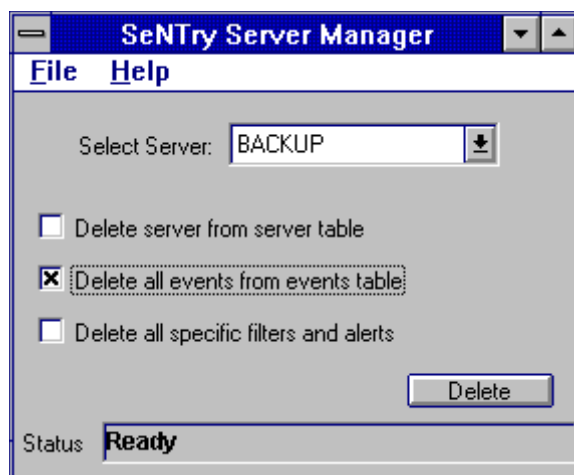
Detail Clear Exit



Full clearing and resetting facilities are provided to reset the lights to green and delete records from the database.

3.7 SeNTry Service Manager

This program, as the name suggests, manages the Servers. It is used to remove information from the database about servers which are no longer to be monitored.



3.8 Licenses.

The product is licensed 'by server'. In this context, 'server' means any Windows NT machine from which you wish to collect events, whether Domain Controller, WNT Server or WNT Workstation. The licensing is accomplished by having the Gathering Service (SAGS) only accept connections from the maximum number of licensed servers. There is no licence checking on SASS sending services.

SeNTRY Licensing

File Help

WARNING

Do not alter these numbers unless
you have a new code from
Serverware Group plc

voice +44 (0) 171 419 2020
sales@serverware.com

Server Name: BACKUP

No. of licensed servers: 4

Software Expiration Date: 1996/07/10

Magic Number One: FFFF57A

Magic Number Two: 3A77

Update Licence

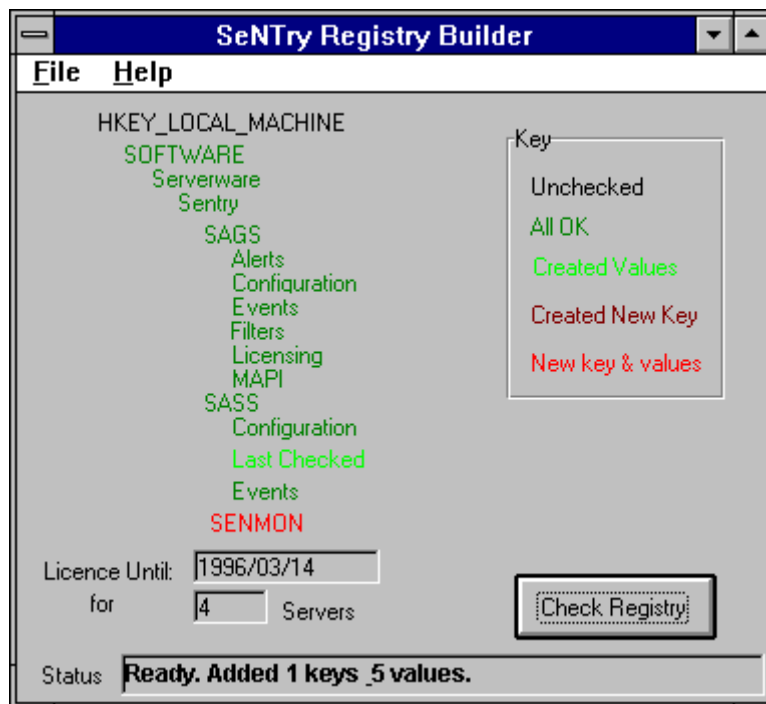
Exit

When SeNTRY ELM is first installed, it is licensed for 30 day's evaluation with a maximum of FOUR connected SASS servers. You may have been given updated licensing information with the product, in which case you must enter this information EXACTLY AS PRINTED into the "License" program within the evaluation period, then stop and restart the SAGS service.

If you do not have such a key, or you decide to buy after your evaluation period, please E-Mail sales@serverware.com to arrange a new licence key.

3.9 Sentry Registry Builder.

This program checks the consistency of the registry for SeNTRY ELM Entries. It also displays the current Licence state.



4 The Benefits of SeNTry ELM

With the increasing use of Windows NT as an enterprise Network Operating System where multiple Windows NT servers exist in multiple domains, network administrators spend considerable amounts of time collecting mission critical Event Log information from remote servers in order to manage the enterprise.

The benefits of SeNTry ELM are:

- Architecture designed to minimize network traffic
- Audible alerting for critical events
- Automatic collection of Event Logs
- Centralised administration
- Does not affect use of existing WNT tools
- Exception reporting
- Filtering of Unimportant Events before onward transmission
- Full SQL Server schema support
- Fully scalable architecture
- "Heartbeat" to detect loss of any SASS server
- Hierarchical (regional) filtering of Events
- Install Shield setup
- Low cost
- MAPI Interface & Microsoft Exchange
- Monitoring of NT Services and Task Lists
- Multiple domain collection
- Native Windows NT architecture
- ODBC output for industry standard compliant databases
- Remote installation of Senders
- Simple to configure and administrate - minimum training required
- Support for Escalation procedure under Microsoft Exchange
- Unattended operation

Available Documentation

There are a number of documents available for SeNTry ELM. These are available in Microsoft Word format from Serverware.

- SeNTry ELM Product Guide (this document)
- Installation Guide (installed when the SeNTry ELM Setup program is run)
- List of F.A.Q.s
- Troubleshooting Guide.

A "Case Studies" document will be available shortly.

There is also a PowerPoint Presentation.

The latest SeNTry ELM information, including details of upgrades and new releases, as well as other Serverware products, can be found on our Internet site -

<http://www.serverware.com>

Support is available by E-Mailing us at :

support@serverware.com

All programs have extensive on-line help.

5 Product Roadmap.

The following enhancements, amongst others, will be available in 1996.

July 1996 :

- Ability to launch a job (program or batch file) on receipt of a particular alert, - passing parameters from the Event Log.
- Key factor performance monitoring.
- Conversion and forwarding of Events to SNMP format from SAGS.
- Support of multiple SAGS for a SASS Sender.
- Timed and multiple filters.
- Inclusive and exclusive filters.

September 1996 :

- Utility programs for archiving, writing event logs, rebuilding registries.
- Communicating with external devices via TAPI, i.e. pagers / cellular phones.
- Integrating syslog information from UNIX boxes into the SeNTry Event Log Management files (ODBC file).
- Incorporating SQL log files.
- Monitor available on Windows 95.

NB - A Software Maintenance agreement for SeNTry ELM facilitates the provision of all upgrades at no extra cost.