SeNTry Installation Guide

Version 1.7

Mod 319

Serverware plc
40-44 Wicklow Street
London WC1X 9HL
United Kingdom

Voice +44 (0)171 419 2020
Fax +44 (0)171 419 2030
sales@serverware.com
support@serverware.com
http://www.serverware.com

CONTENTS

1 Welcome to SeNTry

Welcome to SeNTry, the industry standard tool for Event Log management!

SeNTry is extremely easy to install and configure, and this manual shows you how. The "SETUP" program will install a complete working SeNTry system - it only needs the services to be started for events to be collected in an Access database and displayed using the SeNTry monitor.

Most of this manual is concerned with configuring SeNTry to handle specific more complex matters, such as SQL Server, MAPI Configuration and SNMP.

```
We have highlighted text like this which covers the most
important points of the installation process.
```

If you are just evaluating the product, or have simple requirements, then you can probably skim through this manual just reading these topics. You can always come back later to configure the product properly.

2 What's New in this Release

With SeNTry 1.7 we have redesigned our event browser 'Sentry Monitor'. It has been redeveloped under VC++ which has improved the performance dramatically. Also the browser now contains new functionality such as Starting and Stopping services without having to leave the browser. The new browser is called 'Smart Monitor'. Please check it's on-line help for more details.

Prior to 1.7, modification of Alerts/Filters while Senders were running was a valid feature. Unfortunately we have had to remove this functionality in 1.7 because of memory leakage this caused under NT4.0. Now, any changes to Alerts/Filters will not be seen until the Senders are re-started. This is even more simple to do in 1.7 than in 1.6 because you can re-start all your Senders from the new 'Smart Monitor'.

If you are using NT4.0, it is recommended that you use 'Service Pack 2' as 'Service Pack 1' is still liable to memory leakage. You must upgrade from 1.6 to 1.7 if you are using NT4.0 as the SeNTry 1.6 Alerts/Filters refresh feature will still leak under NT4.0 whichever service pack you have installed.

```
You must still ensure that SASS services are running under
accounts that have admin level privileges and logon service
rights.
```

There are now several SeNTry 'plug-ins' available to enhance SeNTrys capabilities:

- Alerting via Pager / Cellular Phone messaging
- Conversion of SNMP Alerts to NT Event Log
- Performance Monitoring (available shortly)

If you are upgrading from Version 1.5, you will need to recreate the supporting database. We have provided two utilities **filtsave** and **filtrest** which can save filters and alerts from a 1.5 database and restore them to a new 1.7 database.

2.1 Version Control

From Release 1.5 we have been using a system of Version Control whereby we will provide periodic updates to the installation images on CD or from the Internet. The document "README.TXT" will indicate the current release level and the changes, new features and bug releases incorporated in this new release. This document will also be accessible from the Home Page on the web.

You can find out what version you are currently running by running the program "senregbd.exe" - icon is called "Sentry Registry Builder".

3 Distributed Processing

Release 1.6.1 introduced the concept of true Distributed Processing. This allows you to run the SAGS gathering service on one NT server whilst configuring it from another NT workstation or server. The SeNTry monitor can be run from any NT machine, provided that an ODBC connection can be made to the SeNTry database.

```
Configuring SAGS and running the SeNTry monitor remotely is only
designed for SQL Server installations, as these allow ODBC data
sources to connect to remote SQL Servers.  The same effect can be
achieved with Microsoft Access data sources using remotely
mounted drives, but this is not recommended as there are some
problems with concurrency and locking.
```

To setup SeNTry for distributed processing, install SeNTry from the distribution CD onto the machine which is to be running the SAGS service. Then install SeNTry "Configuration and monitor" components onto the machine to be used for remote monitoring. On this machine, use the ODBC administration applet in the Control Panel to create a System Data Source that connects to the SeNTry database on the SAGS server. You can now run **SeNTry ODBC Configuration** to establish the connection to the remote database. If the connection is successful, and is saved in the registry, then you can run the programs **SeNTry Monitor**, **SeNTry Alerts and Filters** and **SeNTry Server Manager** which will run using the database on the SAGS server.

You can also run **SeNTry Licensing** to update the license on the SAGS server by entering the server name directly.

The program **SeNTry Gatherer Service Config** can be used to configure and start/stop the SAGS service on another machine provided that sufficient User Privileges are available.

SeNTry Sender Service Config can be used similarly to control remote SASS senders. This program can also install SASS onto remote machines, obviating the need for SeNTry to be installed from CD on each machine whose events you wish to collect.

```
You can configure a remote DEC ALPHA machine from an INTEL
machine, and vice versa.  You cannot remotely install SASS on a
machine of different architecture from the configuration machine.
```

4 Support for DEC ALPHA Architecture

From Release 1.6.1 we supported DEC ALPHA architecture. On CD this is installed by running SETUP from the ALPHA directory instead of the I386 directory. An ALPHA version can also be found on the WorldWideWeb.

Both versions have identical functionality, although we have not fully implemented SNMP in the ALPHA version.

You can run configuration and monitor programs remotely on machines of different architecture without any problems. You cannot, however, install SASS remotely onto a machine of different architecture.

5 Upgrading from earlier releases of SeNTry

There is no need to "Uninstall SeNTry" before installing the new release if you are upgrading from 1.6 to 1.7. However, you must re-run the SeNTry ODBC configuration program if you are using any database or ODBC drivers other than SeNTrys defaults (ie Access). Note you will have to re-install your full license information as the full install sets up a demo license.

If you are upgrading to SeNTry 1.7 from SeNTry 1.5, then you must bear in mind the following considerations:

1) There are new versions of all executable programs, including services.
2) Remote senders need to be reinstalled, and possibly changed to run under a new account.
3) There is a slight change to database.

To achieve a clean reinstallation of SeNTry it is suggested that the following checklist be applied:

1. Stop all senders with the SASSINST program.
2. Stop SAGS with SAGSCONF.
3. Use SASSINST to remove all SASS services.
4. Save the current database (if MS ACCESS) by copying to another directory.
5. Run the UNINSTALL SENTRY icon from the SeNTry program group
6. Use the Registry Editor **regedt32** to delete the key HKEY_LOCAL_MACHINE/Software/Serverware/SeNTry and all subkeys.
7. Delete the installation directory and contents if not fully performed by step 6
8. Reboot the SAGS machine if possible
9. Reinstall SeNTry 1.7 from the CD or Web Image.

At this point you can configure the SAGS service and reinstall SASS on remote senders as outlined in the following sections.

Please note that SeNTry 1.7 *et seq* are incompatible with earlier versions. Any attempt to 'mix and match' programs will be unsuccessful!

5.1 Preserving Filters and Alerts

Because some users have spent some time creating and refining their filter and alert definitions we have provided a simple means of saving the old definitions and reapplying them to the new SeNTry version 1.7.

The program **filtsave.exe** is provided on the CD image in uncompressed form and can be copied and run under SeNTry version 1.5. This program will save all filter and alert definitions to a sequential file, the name of which is prompted for.

After you have installed Sentry Version 1.7 and configured ODBC to point to the correct database you can run the program **filtrest.exe** from the Sentry Installation Directory.

This prompts for the name of the saved file and rebuilds the filter and alert tables and recreates the appropriate registry.

6 Installation - Setup Procedure

To install SeNTry 1.7 from CD or from the downloaded web files, run **setup.exe** from the appropriate directory. Note that after installation the Sender and Gatherer services will have been installed and will be ready to start.

```
You must be Administrator (or have full administrative rights) to
install the software.  You may need to be Domain Administrator to
run some setup facilities and to perform remote Sender
installation via the Sender Installation/Configuration program,
your user will also need the advance user right 'act as part of
the operating system'.
```

You will see the welcome screen as the setup wizard is prepared, then the dialog proceeds as follows:

- You are first advised that you should close down all applications if possible. This is sound advice, as some components may be in use and thus cannot be checked by the version checking functions or upgraded. Note that the ODBC 3.0 drivers are obligatory if using MS Access™ and hence all ODBC applications should be closed down if this component is to be installed.

- You are then asked to register your user name and company. This information is stored in the registry and can be used to validate licenses.

- This is followed by an “Installation Type” dialog in which you choose which of the components to install -
    1. Sender Service (SASS)
    2. Gatherer Service (SASS)
    3. Configuration and Monitor programs
    4. ODBC Access Drivers v3.0
    5. Access Database for SeNTry to store events in
    6. SeNTry API Programs and Samples
    7. Extensions and Utilities for SNMP Support

ODBC Installation is strongly recommended unless you have version 3 desktop drivers installed already. Also remember that you must install Configuration and Sender components if you will be using the Remote Sender Installation capabilities of SASSINST.

This dialog also allows you to choose the destination directory in which to install SeNTry component files. This is defaulted to “sentry” on the same disk as your Windows NT system files. Some space checking is performed, but you may need to allow space for the ODBC database to grow. You can press the “disk space” button to check available space on each available drive. Remember that SETUP will install OCX controls and ODBC components in the WINDOWS\SYSTEM32 directory and not in the destination directory.

At this stage SETUP will check that your configuration of Windows NT is consistent with your chosen options, and that the architecture is correct for the installation version. You will receive message boxes with warnings and fatal errors if any problems are discovered.

```
You must have Windows NT 3.51 or later to run the "Configuration"
components as the programs use the new 32 bit OCX controls.
"Sending" and "Gathering" components can run on Windows NT 3.5.
```

- If you have elected to install SAGS the setup procedure will now check whether you have Microsoft Exchange™ or Microsoft Mail® installed on your machine. It does this by checking for a file called MAPI32.DLL in the Windows System Directory. If the Major version of this file is 4 or greater it is a support dll for CMC, the messaging protocol used by Exchange and thus it assumes that Microsoft Exchange™ is installed. An earlier version implies MS Mail and the absence of the file means neither. You are then asked to confirm which version of programs to install. You need not concern yourself with this if you do not intend to use the MAPI facilities.

```
If there is incompatibility between the DLL version and the
chosen messaging system then MAPI calls will not work
```

- If you have specifically selected the SNMP Extensions then the setup program will check that you have already installed and setup the SNMP Service. If this is done correctly then the Registry is updated to enable the SNMP service to load the SeNTry Extension Agent. If the SNMP service is not installed then a dialog box is presented informing you that the SNMP extensions are not installed. You can reinstall this option later after correcting the problem.

```
SeNTry will only send SNMP Traps if the SNMP service is already
installed and configured correctly.  You must stop and restart
this service after installing SeNTry to allow the Extension Agent
to be loaded
```

- Then you are called upon to decide on the name of the program group to install into. Note that SeNTry 1.7 will create twelve icons in whichever group is chosen.

SETUP is now ready to begin installing the components, and a confirmation screen is presented showing what action is about to be taken. If you choose to continue, the following actions will occur:-

1) The appropriate files will be copied to the target directories. If any files cannot be copied, a warning about "read only" existing files is displayed and you can choose to force overwrite (risky) or not. At the end of file transfer, if some files have not been copied a warning message is displayed.

2) SETUP will maintain registry entries for shared components (DLL's, OCX's and Access objects) automatically.

3) SETUP will build registry entries appropriate for initial use of the product.

4) If you have installed the ODBC component, the ODBC registry will be maintained and a default data source "sentry default" created to point to the Access database just installed.

5) SETUP will create an installation log file allowing later removal of the product.

6) Program groups and icons will be created.

If you have elected to install ODBC drivers, SeNTry will have configured a default System Data Source Name **SentryAccessDB** which will refer to the database **sentry.mdb** installed with the product. This will be used unless Sentry ODBC Configuration program is run.

At this stage SENTRY is fully installed and the local Sender and Gather services are ready to start. However, if you wish to use SQL, you will need to configure the ODBC settings correctly before starting the SeNTry services.

To remove SeNTry completely you must first stop and remove all services using the Sender Installation/Configuration program and the Gatherer Configuration program. Then run the UNINSTALL Icon from the program group. The SeNTry directory may still exist if you have some log files or files you have created. Simply remove the SeNTry directory manually.

7 Configuring Sentry - ODBC and Databases

SeNTry is above all a product for getting information from Event Logs into Relational Databases. The standard (default) database is a Microsoft Access database called SENTRY.MDB which is installed into the target directory by the SETUP process. SETUP also installs the JET engine and the Remote Data Object (RDO) (if not already present) which allows all SeNTry configuration and monitor programs to access this database directly. If ODBC Drivers V3.0 are installed with SeNTry, a default ODBC source is created to allow the SeNTry services to access this database.

IF YOU ARE USING THE MICROSOFT ACCESS DATABASE SUPPLIED AND THE DEFAULT ODBC SOURCE CREATED YOU DO NOT NEED TO CONFIGURE ODBC FURTHER AND CAN IGNORE INFORMATION IN THIS TOPIC.

However, users may wish to configure their systems differently, perhaps using SQL Server as the relational database or configuring the Access database on a different drive. To that end the program **Sentry ODBC Configuration (senodbc.exe)** is used.

In order for this program to work, there must exist System Data Source Name (System DSN) entries for the databases you wish to access. These can be created by using the Control Panel ODBC32 Administrator applet and creating entries for the SQL Server and/or Microsoft Access driver. (Of course, if using SQL Server the sentry database must be created and user ids enabled - see the topic **Configuring SeNTry - SQL Server Considerations** for how to do this).

If you have chosen to install the ODBC and Database options then SETUP will have created two databases in the installation database.

> **SENTRY.MDB** is the default Access database which will be used to store all SeNTry information. A System DSN will be created by the SETUP program to refer to this database and this will be pre-configured in the SeNTry registry.
>
> **SENSAVE.MDB** is a copy of this installed in case of total disaster later. Note that the ODBC applet in the control panel contains entries to repair and compact the database so this should not really be needed.

SENODBC.EXE will load all SQL and Access System DSN into a combo box allowing the user to select which source to use. A **Server Name** text box contains the name of the server where the database is located - this defaults to blank (local server). The program then fills three text boxes: **User ID**, **Password,** and **Database Name**.

- For Access, these boxes are ‘greyed out’ as this information is stored in the System DSN. The “Local Jet Database” will be defaulted to the SENTRY.MDB database mentioned above.
- For SQL Server you must enter a valid userid/password combination of a user with sufficient rights to create and delete records in the SeNTry database; the name of which is placed in the “Database Name” box.

Having filled in the information above, press the **CONNECT** button. The program will first check that SENTRY is correctly installed on the server named in **Server Name**. SENODBC.EXE will then attempt to connect to the database using this information and if it succeeds will check the “connection” indicator in the Database Status Panel. It will

then check for the presence of the four required tables and check their indicators as it goes. If all is OK the bulb will light and the **SAVE CONFIG** button will be enabled allowing you to press this and save this database as your data source.

All programs running on the local machine will use the registry information stored with the **SAVE CONFIG** button to connect to the database directly

8 Configuring Sentry - SQLServer Considerations

If you intend to use SQLServer™ as your database then it is your responsibility to ensure that an appropriate database is made available and correctly configured. You can use SQLServer™ 4.0 or later with this release but future releases of SeNTry will require SQL 6.0 or later as they will need ODBC Level 2 compliance.

An outline script **SENTRY.SQL** is shipped with SeNTry and installed in the destination directory when the "Gathering Service" component is installed. This script contains the SQL statements necessary to create the tables and indexes and some sample statements to create user and logon ID's.

This script must be modified as necessary, ***paying particular attention*** to your own local security policy. Please remember that the userid/logon information will be stored in the Local registry and so it is highly recommended that a user be created who can only access the SeNTry database and no other as a determined 'hacker' could uncover this information.

It is in any case sensible that the userid/password allocated should **default** to the sentry database created, and have access to no other databases.

```
For SQL Server™ you must create a system DSN to refer to the
appropriate database and use the SENODBC program to provide a
link to the SeNTry programs as described earlier.
```

8.1 SQLServer and Automatic Startup

If you will be configuring the SAGS service to start automatically whenever the system is rebooted, you will need to have set SQLServer services to start automatically and you must set the **Startup Delay** value in SAGSConf to about 4 mins or greater. This will give the SQL Services time to start before the SAGS service tries to connect to the database. If SAGS has no startup delay, it will probably attempt to connect to the database before it is made available and in such circumstances SAGS will write an event log message and stop immediately. It must then of course be automatically restarted.

9 Configuring SeNTry - Filters and Alerts

The program **Sentry Filter/Alert Configuration (SENFIL.EXE)** is used to define **filters** (to prevent unimportant events reaching the central database) and **alerts** (to cause the 'traffic light' for the server to change to yellow or red). This information is held in the central database but is also transferred to the registry on the Sentry Alert Gatherer machine to allow updating of remote senders as information changes.

FILTERS can be made specific to a given sender or global to apply to all senders. By design, filters are exclusive - only events specifically matched are excluded and all others are sent by default. This ensures that unexpected Events are not filtered out. As a consequence of this approach is usual for filters to be refined as more knowledge is gained.

Filters can be made on combinations of the following tokens taken from the source event:

Event Log file	System Log, Security Log or Application Log
Event Severity	Stop (red stop sign), Warning(yellow exclamation mark), Information(blue Question Mark), Success Audit (a key), Failure Audit (a padlock).
Event Number	
Event Source User ID	Limited "pattern matching" and "wildcards
Event Text	Search for strings with limited "wildcard" support

The tokens are in an "AND" relationship; blank fields are ignored. So a filter set up for Severity "WARN" and source "NETLOG*" will filter out all warning events from any source that starts with the letters "NETLOG*".

Any Event raised at the remote sender that matches a FILTER (either specific to that server or global) will be effectively ignored - not sent to the gatherer.

SENFIL.EXE maintains its table of filters by displaying the filters appropriate to the selected server in a data grid. You can click on a line of the grid to change it, or click on a "NEW" line to add more filters.

```
You are strongly recommended to define SOME filters!  Unless you
reject the 'dross' the SeNTry database will be as useless as the
Event Viewer for analysing problems and security aspects.
```

ALERTS are defined and used exactly in the same way as FILTERS, but there are separate grids for RED and AMBER alerts. Events pass through filters first and are then compared against the ALERTS to see if this event should change the traffic light color on the monitor.

ALERTS can be made on the same fields as FILTERS, but there are two extra fields:

Text String - Matching against strings in the TEXT of a message.
Enable MAPI- Whether to send a message using MAPI when an event is received

The “text string” alert can be used to raise alerts based upon specific strings in the “Event Description” field. This cannot be used for filters as the mechanism used for expanding text strings would require too much system resource. Enable MAPI can be used in conjunction with **SeNTry MAPI Configuration** to control the sending of MS Mail™ and MS Exchange™ messages.

```
Remember that although filters and alert data is stored in the
sentry database, they must also be updated to the registry before
they can be read by the Senders.  The registry is only updated
when the “save changes” button is pressed.
```

10 Configuring SeNTry - Sentry Alert Gathering Service

The Sentry Alert Gathering Service (SAGS) is a service which runs on the Gathering server. Its main functions are:

- Collect events sent from remote Sentry Alert Sending Services (SASS) via Named Pipes
- Store these events in a database using ODBC
- Send messages via MS Mail™ or MS Exchange™ using MAPI if required
- Periodically "ping" SASS services that have sent no events to see if they are still alive
- Signal the Sentry Monitor if the traffic light color needs to be changed.
- Raise SNMP traps (if configured) on service start and stop, and for each red alert

If you have chosen to install "Gatherer Components" then SAGS will have been already installed on your server, but you may need to configure the service.

If you are using Access as your database, unless you already have **ODBC Desktop Driver Pack V3.0** you **must** install the "ODBC Component" in the SETUP program. Earlier versions are either not compatible with 32bit applications or have memory leakage problems.

The correct tool for initially installing or re-installing the service and configuring it for correctly is NOT the **SAGS Service Configuration** program. You should only install the Gatherer from the CD/Web image as this is the only procedure which correctly installs the Gatherer software, configures the necessary registry entries and creates the service. The SAGS Configuration program - Install option, ONLY creates the service entry.

This program is installed by the Sentry Setup program and has two large buttons on its main screen:

Install/remove Gatherer Service which allows you to install and remove the service components. You can use this to change the service so that it starts automatically when the machine is rebooted or to run under a different account/password which could be necessary to allow MAPI messages to be sent. Both these change functions can also be performed from the Services dialog in the Control Panel under "Startup" options.

Note that the service is automatically installed when SETUP is run. It is not, however, removed if SeNTry is UNINSTALLED. Thus to remove SeNTry you must first remove the SeNTry services before running the UNINSTALL Icon.

Gatherer Configuration which has the following functions:

1. Start SAGS Service
2. Stop SAGS Service
3. Show status of SAGS service (started/stopped)
4. Configuration

You can Start, Stop, Query status and Configure the Gatherer on any machine, provided you have sufficient rights under NT to do so. Enter the name of the server into the **Server Name** text box, or use the **?** button to browse the network. The default is the local server.

Configuration allows you to alter certain parameters affecting operation of SAGS. These do not normally need modification but can be changed if you wish:

- **Log File Name** and **Debug Level** are used to provide a "trace" of SAGS activity into the Log File. There are currently only two log levels - 0 (no logging) and 1 (output to Log File). This option can be useful when debugging network problems.

- **Inactivity Time** is the time interval in minutes after which SAGS will "ping" remote servers to see if they are still alive. If they are not a warning event is written to the Event Log.

- **Send Events Onwards** If this parameter is set to Y then SAGS will pass events to the SASS service running on this server. This must of course point to another server where SAGS is running. The effect of this is that events collected by SAGS on this server are subjected to another set of filters and alerts then passed to another database; thus allowing a hierarchy of databases with a different set of critical alerts

- **Spawn Command** SeNTry v1.7 has the ability to automatically spawn a job at the same time each day. If you wish to run a ".BAT" file this command should be "<windows system directory>\CMD.EXE" which is 32bit and not "command.com" which is the DOS version

- **Spawn Parameters** are the string of parameters passed to the spawn command above

- **Spawn Time** is the time (in 24hr format) at which the command will be launched.

The spawn capabilities are typically used to launch a job to produce daily reports or charts from the Sentry database. Note that the job will run as the same user who is running the service.

- **Startup Delay** is used to control the time after a system boot before SAGS will attempt to connect to the ODBC database. This can be very useful if attempting an automatic start as the SAGS service will start before SQL has finished initializing, resulting in a connection failure.

- **SNMP Trap on Service** can be used to make SAGS send a trap as the service starts, and as it stops. This can be used by a program such as HP OpenView™ to raise alarms on a console.

Other parameters displayed cannot be altered at this time.

These parameters are saved when the **OK** button is pressed, but SAGS only reads parameters when it starts up, so you must stop and restart the SAGS service to read the new parameters.

No Events will be lost if SAGS is not running. The remote SASS services will buffer their events into a disk file to transmit when SAGS is restarted

SAGS additionally reads parameters set by **SeNTry ODBC Configuration** to determine which database to populate and by **SeNTry MAPI Configuration** to determine how to handle alerts which raise MAPI Messages.

The SAGS service is installed by the SETUP program to run under the SYSTEM account and to be started and stopped manually. If this is all you require, you need only use **SAGS Service Configuration** to start and stop the service. If you are familiar with the control panel, you can start and stop the service with this and only use this program to change configuration parameters when needed.

11 Configuring SeNTry - Sentry Alert Sending Service

SASS (SeNTry Alert Sending Service) is the service that runs on Windows NT computers to send filtered Events to a designated SAGS (Gatherer) Service, whereupon these events are stored in the database. The SASS service is fed details of filters and alerts during its initial communication with the central SAGS service.

SASS can of course be run on the same machine as the SAGS service. If you elect to install the "Sender Components" in the Sentry Setup program this service is already installed and, when started, will send its events to SAGS on the LOCAL computer when started. Note that when starting the SASS Sender for the first time after installation or when the Sender has been down for some time, it will have to process it's back-log before data is passed to the Gatherer and so it may take 5 or 10 minutes before the first series of data appears in the SeNTry Monitor. Please allow the system to run for this period of time before loading the Monitor otherwise the Monitor will display an error because there is no data in the database yet and will then abort.

If SASS is running on a remote machine then the service must be installed to run under an account that has administration privileges (domain admin if applicable) and logon as service rights.

```
In Release 1.7, SASS services running on remote senders cannot be
left to run on the SYSTEM account.  Because of a bug in NT, the
user right to manage the security logs does not work correctly
and so we are currently limited to using a service startup ID
which has administration level privileges as well as service
startup rights.  You can specify a startup ID with SASSINST or
via the control panel.
```

If you try to stop the SASS service after recently starting it, you may receive a message that the service has not stopped. This is because the Service is processing the back-log. Check the NT Event Log for a message from SASS. Once the back-log has been processed, the service will become stoppable. However, if you need to stop the service immediately, simply continue to try to stop the service. After about 6 attempts, the service will stop.

With this release, there are two ways to install SASS on REMOTE computers.

- You can install the SeNTry software on each server from the CD/Web image (you only need the "Sender Component"). This method allows you to run **SeNTry SASS Configuration** on that machine to configure the service. Note that if you install the Sender using this method, you must configure the Senders Service Startup ID manually using Control Panel as the default ID is 'Local System' which will NOT communicate across the network. Remember that the startup ID must have administration privileges and logon as service rights. You must also configure the Senders SAGS Host field to point at the computer containing the Gatherer, by default the field contains the local system name.

- You can install the SASS service onto the remote machine by running **SeNTry SASS Installation / Configuration** - Install option, on this machine. This is only possible if you have sufficient rights on the remote machine to create/remove and

start/stop services. You will also need access to a networked directory on that machine to install the SASS software into. You can also configure the remote SASS service and start or stop it **provided that NT security will allow you to do this**. Remember that you can only install to a machine of the same processor family. During installation, the service startup ID/password is validated and if your user (not SeNTrys user) does not have the advanced user right 'act as part of the operating system' the validation will fail. Assign your user this right and re-install after re-logging in to NT to utilize the new rights.

The Sender Installation/Configuration program is similar in function and content to the SAGS configuration program with the following major differences:

- The Installation dialog allows you to copy the software components from the directory created by the SETUP program to another directory, which can be on the local or a remote server. You can browse and connect network drives to find the desired location. The ability to start the service automatically and change the account under which the service runs is also present. You can install, remove, start and stop this service provided you have sufficient rights to do so.

- You can start, stop and query multiple services at once by making multiple selections under "server name". This selection list can be saved and reloaded to allow you to control all SASS servers simply.

- You can configure SNMP traps to run not only on service starting and stopping, but also whenever a **RED ALERT** is received at the server. This trap will contain details of the event in it's Variable Bindings allowing a program such as HP OpenView™ to browse red alerts.

- You can start/stop and install services in batch mode.

For more information on facilities to manage remote servers, see the online help text for the **SeNTry SASS Configuration** program.

The SASS Configuration parameters may need to be modified for your environment:

SAGS Host names the server that SASS must send its events to. This must be a valid host name and must "trust" the SASS machine for events to be accepted.

Log File Name and **Debug Level** function as in the SAGS configuration program, but there are more debug levels available (0-5) each of which will produce more tracing information.

Buffer File names the file that SASS will store events in if it cannot communicate with the SAGS service. This file can grow quite large if, for example, the SAGS server is down for a weekend and should be placed on a drive with plenty of free space.

Buffer Cycle Time (secs) denotes the time interval that SASS will store events before transmitting them. Red and Yellow alerts can be handled separately, see below. Normal (green) events and all events if not specifically excluded are better handled by "batching" them before transmission. This is because libraries need to be loaded and unloaded to expand message numbers and this can be

done more efficiently for groups of events. SASS will buffer events for this number of seconds before expanding them and then transmitting them to the SAGS service.

Last Event Received This is the time of the last event as sent to SAGS. On first installation it is set to a time of two hours ago to ensure that the initial load does not bring in megabytes of old information. SASS then maintains this figure as it sends events. After SASS is stopped, you can edit this value before restarting the service if, for example, you are restarting after a weeks break.

Send Critical Alerts Directly determines what SASS will do when a RED or AMBER alert is detected and there is data in the buffer file. If this field is N (the default) then it will transmit the critical alert and empty the buffer at the same time. If Y then the critical alert will be set separately and the buffer file will be left alone.

Service Check Time A value other than zero will cause the SASS service to query the status of all installed services at this time interval. Any changes (e.g. RUNNING to STOPPED, STOPPED to STARTED) will be reported in an EventLog record which can obviously be used to raise a red alert if needed.

Process Check Time This works in the same way as **Service Check Time** above except that changes in the actual processes running is reported. This information is obviously useless for machines which have a local user logged on, as the process table information is constantly changing. It can, however, be very useful for true servers which have no local users as it can detect processes which are not services (such as some Virus Checkers) going down.

Spawn Batch Command
Spawn Parameters
Spawn Time

These fields work exactly as on the SAGS configuration program described above. Job submission from SASS services is typically used to archive and/or clear event logs. Note that SASS services detect the clearing of an event log and do not fall over or lose data.

New to 1.7 the “Optimization” button displays another dialog which offers the following:

Best Performance (green alerts asap) Selecting this option and pressing OK will modify the Sender Configuration parameters on the configuration screen to optimize throughput so that Red and Amber Alerts appear directly and Green Alerts are transferred as soon as possible. You must press OK at the configuration screen to save the changes or press Cancel to abort.

Best Performance (green delayed) Selecting this option and pressing OK will modify the Sender Configuration parameters on the configuration screen to optimize throughput so that Red and Amber Alerts appear directly. Green Alerts are considered not important and are transferred after a length delay once the system is more idle. You must press OK at the configuration screen to save the changes or press Cancel to abort.

Least Network Traffic Selecting this option and pressing OK will modify the Sender Configuration parameters on the configuration screen to optimize throughput so that all events are buffered and transferred using maximum buffer sizes with least impact on the network. You must press OK at the configuration screen to save the changes or press Cancel to abort.

The "Advanced" button displays more parameter options as follows:

Filter Flag This is normally left at "O" (filter Out). All filter records act as exclusive filters and exclude any events which match the criteria. It is also possible to define "I" (filter In) which means that only records which match the given filters are included and all others are excluded regardless. This can be used for specialist applications in which just a few specific records are required but is otherwise not recommended.

Max recs. in buffer determines how many records the buffer file can contain before transmission is attempted. This value defaults to 50 which may not be sufficient. NOTE THAT IF CONNECTION TO SAGS IS LOST THIS FILE WILL GROW BEYOND THIS FIGURE - THERE IS NO UPPER LIMIT. This value is used in conjunction with the **Buffer Cycle Time** parameter to determine the frequency and size of batches.

Recs. Before Send should normally be left at the default of 1.

Startup Delay works as defined in SAGS configuration previously. This can be used to decrease the workload on the machine at boot time and ensures that event collection only commences when the machine is stable. Note that no event loss will occur as on startup SASS looks for the time of the last event received and begins collection from there.

Process Delay A value of N means that collection starts immediately. A value of Y will cause SASS to wait until the next event is written to the event log before commencing extraction.

SNMP Service Trap A value of Y means that SASS will send an SNMP trap whenever the service is started or stopped.

Red Alert Trap This can be set to Y only if Service Trap is switched on, and will cause SASS to send a trap for each red alert as it is raised. This trap will contain information on the event in the variable bindings sent with the trap.

As with SAGS configuration, the SASS service must be stopped and restarted to read new parameters. SASS will not lose any events when restarted as it stores the "time of last event received" in its registry.

If you are only testing the software, and only want to collect events from the **local** server, you need only use this program to start and stop the SASS service. But if you wish to collect events from **remote** servers you must either use this program to install the SASS service remotely or run SETUP on the remote machine to install the SeNTry software.

12 Configuring Sentry - Enabling MAPI

SeNTry can be configured to send messages using MS Mail™ or MS Exchange ™ when particular events are received. Determining which events send messages is handled by checking the "Enable MAPI" box for individual Alerts in the **Sentry Alerts/Filters** program.

```
Please ensure you have an MS Mail 3.2. post office and not a
Workgroups post office as the MAPI Configuration program will
work with the Workgroups post office but there is no API
available for our SAGS service to use.
```

The **SeNTry MAPI Configuration** program configures who gets the messages, etc. The SeNTry setup procedure will have installed either the MS Mail™ or the MS Exchange™ version of this program depending on the components detected - you can tell which version by looking at the 'splash' screen displayed when the program is invoked.

Before MAPI will work correctly, you must attend to the following points:

MS Mail™

1. You must have the correct combination of SeNTry and Messaging setup. Ensure that your MS Mail MAPI32.DLL in system32 is about 16K. If you are using MS Mail but the DLL is much larger (50K+) then you have at some point installed Exchange Client and then perhaps removed it. This DLL is not compatible and you must replace it with MS Mails DLL.
2. You should create a new mailbox which the SAGS service can use to send messages. This user MUST have a password as there is a problem in the API with null passwords. You must occasionally clean out the "sent mail" for this user or profile as the API cannot do it. Ensure that the inbox is stored on the Server and not locally on the computer so that this mail box will be accessible from any NT logon.
3. You can either create a new NT user for the SAGS service startup or use an existing one such as administrator. You will need to configure the SAGS service using the STARTUP options in the Control Panel applet so that the service will run under this account. This account requires 'log on as a service' user rights in order to start the SAGS service.
4. You should also test that the MAPI Configuration program is able to logon with the given mail name and password details whilst being logged on to NT interactively as the user under which the SAGS service will run. Check that you can logon to MSMail and send a test message using the mail name and password you have assigned for SeNTry to use. Also check you can logon using the **SeNTry MAPI Configuration** program using the same mail name and password. If you cannot logon interactively, the service will have no chance!
5. If you do not already have an MS Mail MAIL.DAT file, you must create one using the MS Mail Security program and place this in your system32 directory so that the SAGS service can locate the P.O. when no user is logged into the system. By default MS Mail locates it's P.O. using the users personal registry which is not available if no one is logged into the terminal.

MS Exchange™

1. You must have the correct combination of SeNTry and Messaging setup. Ensure your MAPI32.DLL is 50K+.
2. You should create a new NT user for the SAGS service to use and assign this user the rights 'logon locally' and 'logon as a service' and configure the SAGS service to start as this user using Control Panel.
3. Create an Exchange mailbox for the new SAGS user. You may want to configure the primary NT account as 'EveryOne' so that you can administer the mail box without having to log into NT as this user.
4. Logon to NT as the new SAGS service user and create an Exchange profile which you can use to configure MAPI and which SAGS can use to logon to Exchange with. Note that Exchange profiles are personal to each user and this is why you are logged in as the SAGS service user setting up a profile as this profile will not exist for your user or any other user. Any MAPI configuration must be done once logged into NT as the SAGS service user.
5. Test the Exchange profile you have created by running Exchange and sending a test message.
6. Configure SeNTrys MAPI interface now using our MAPI Configuration program specifying the Exchange profile you have just created. See the remainder of this section for details of fields etc. Note that any further or re-configuration of MAPI must be done whilst logged into NT as the SAGS service user.
7. Logon back onto NT as your own user.
8. You must occasionally clean out the "sent mail" for this profile as the API cannot do it and the Exchange profile setting to not keep sent mail does not currently work.

If all this is configured correctly, using the **SeNTry MAPI Configuration** program is extremely simple. The first time you run the program you receive an informational message reminding you that you must set up the service account, then you proceed as follows:

> Enter the sentry mail account and password or profile name into the appropriate box(s) then press the **LOGON** button. If successful, the icon changes to reflect the fact that you are connected and the button caption changes to **LOGOFF**.

Alert Interval is the time during which **SeNTry MAPI Configuration** will buffer MAPI messages (in the file named in **Buffer File**). A value of 0 means that each separate MAPI aware alert will generate a separate message. Any other value means that messages will be buffered for that length of time then sent together as one message.

There is presented a grid of three hour slots. If there is a name in a slot when a MAPI delivery is due, it is sent to that user. A *blank slot* means no mail is sent at that time. Names are inserted into the grid using the **User for Selected Cells** box. First use the mouse to select a cell or cells in the grid (you hold down the left mouse button whilst moving the mouse to select more than one cell) then press the **Insert** button to place that name in the selected cells.

The **P.O.** button allows you to select a name from a postoffice list. Press the "To" button to store the name the "OK" to transfer the name to the appropriate box. Only one recipient is allowed so the first name only is taken.

You can also send an End of Day message to a given user at a certain time each day - this message contains the total number of red, yellow and green events generated at each monitored server. This user can also be selected by the **P.O.** button.

The **Escalation** facility requires MS Exchange as it needs functionality not present in MS Mail. If this box is filled in then a message sent to any user and not opened within the escalation time will be resent (escalated) to this user.

When you press the “Update” button the program will attempt to resolve all names and if successful will update the registry and log the user out. MAPI is now enabled for this SAGS service and will remain so until you choose the “Disable MAPI” option from the menu.

A Disabled system is re-enabled for MAPI merely by logging on again and pressing the UPDATE button.

```
If you are not using MS Mail or MS Exchange then you do not  need
to run this program at all.
```

12.1 Troubleshooting MAPI

Because there are so many considerations, it is possible that your MAPI may not work the first time that you try it. We recommend that your first check out our Sentry Trouble Shooting document our Web Site (www.serverware.com).

If you feel confident with playing with the system then restart the Gatherer service with debug level set to 1. Examination of the debug file produced (SAGS.LOG) can be tricky, but you can identify the sections involved with MAPI to try to pinpoint the problems. You can then email this log to us for further examination (support@serverware.com).

The usual reason is that the SAGS service is running under an account which is unable to logon to the MAPI DLL using the given profile details. This can be identified by “failed to logon” lines in the debug file.

13 SNMP and SeNTry

13.1 Introduction

Release 1.6.1 incorporated the first, limited inclusion of SNMP capabilities into the SeNTry product. We have envisaged the use of SNMP with a Network Management console program such as HP OpenView™ and hence have provided sufficient functionality to allow SeNTry to send traps whenever a service is started or stopped, and whenever a Red Alert is received.

As SNMP is potentially a complex subject and may already be used by other Windows NT components on your servers, this document does not attempt to explain or detail SNMP functionality and methodology in any detail.

```
You are advised not to attempt to install SNMP unless you have at
least an outline understanding of how it works with Microsoft
Windows NT
```

Following the Microsoft SDK implementation of SNMP, we have provided the following files to allow SeNTry to have SNMP functionality:

1. An Extension Agent DLL **SSNMPEXA.DLL** which is installed into the Windows System32 directory. Registry Keys are created by the SETUP process such that when the SNMP service starts this DLL is loaded alongside.
2. A source MIB file **SENTRY.MIB** for the SeNTry database entries. We have allocated ourselves the Object Identifier 1.3.6.1.4.1.121.2 (iso.org.dod.internet.private.enterprises.serverware.sentry) under which we have defined the SeNTry variables. This file can be compiled with the Windows NT MIB compiler MIB.CC or copied to HP OpenView, PolyCentre or whatever and compiled in that environment.
3. A compiled MIB **MIB.BIN** containing the standard MIB entries from the Resource Kit plus the file SENTRY.MIB above already compiled. You can copy this file to the Windows System Directory overwriting the one already there if you are confident that there have been no other changes to this file. If there have been you must use the MIB compiler including all relevant source files.
4. A checkout program **SNMPTEST.EXE** which will check that SeNTry is working correctly with SNMP. This program will interrogate the SeNTry MIB database, launch a thread to listen for traps, simulate a Red Alert trap and then interrogate the database again. If this program works correctly then so will the SeNTry services

13.2 Installation of the SNMP Service

Before SeNTry can work correctly, the SNMP service needs to be installed correctly. This is initially done by selecting **Control Panel/Network** and pressing the **Add Software** button. Choose **TCP/IP and Related Components** and then check the **SNMP Service** box.

To ensure correct operation of this early release of SNMP for SeNTry you should configure SNMP (using the Configure button for the SNMP Service in Network Settings) so that all machines send traps to a community called **public** and the **Trap Destination**. should be tested initially as the Local Machine.

If the Trap Destination is not the local machine then the SeNTry MIB must be installed on that machine.

```
Please Note that the SNMP Service must be installed and running
on all SAGS and SASS machines, or SNMP traps will not be sent.
```

13.3 SETUP of SeNTry for SNMP

You must check the “Extensions and Utilities for SNMP” component when installing the software. This will install the files listed in 13.1 into subdirectory “snmp” under the installation directory and prepare the registry so that the Extension Agent is loaded when the SNMP service is started.

```
“Extensions and Utilities for SNMP” must be correctly installed
for each sender and gatherer if SNMP traps are to be sent
correctly.
```

Run the program icon **SNMP Checkout Program** and check for output as follows:

```
Config   |SAGS not configured to send traps
Config   |SASS not configured to send traps
Config   |SASS not configured to send Event Alert traps
Setup    |Community name is public
Setup    |Agent  name is SERVERWR05
TrapWatch|listening for traps...
Init     |Connected to the agent OK
main     |requesting MIB at current state
Walk     |beginning walk through database
Walk     |.sentryVersion.0=OCTET STRING - 1.61
Walk     |.sentryGatherer.0=OCTET STRING -
Walk     |.sentrySAGS.0=INTEGER - 0
Walk     |.sentrySASS.0=INTEGER - 0
Walk     |.sentryEventLog.0=INTEGER - 0
Walk     |.sentryAlertLevel.0=INTEGER - 0
Walk     |.sentryEventNo.0=INTEGER - 0
Walk     |.sentrySource.0=OCTET STRING -
Walk     |.sentryText.0=OCTET STRING -
Walk     |.sentryTrap.0=INTEGER - 0
Walk     |End of MIB subtree reached.

>>>>>>>>>|enter g to continue
Set SNMP |set values and requested RED ALERT trap......
TrapWatch|trap generic=6 specific=1 from (194.6.8.76)  <<< SENTRY TRAP
main     |reexamining MIB after SET
Walk     |beginning walk through database
Walk     |.sentryVersion.0=OCTET STRING - 1.61
Walk     |.sentryGatherer.0=OCTET STRING -
Walk     |.sentrySAGS.0=INTEGER - 0
Walk     |.sentrySASS.0=INTEGER - 0
Walk     |.sentryEventLog.0=INTEGER - 0
Walk     |.sentryAlertLevel.0=INTEGER - 0
Walk     |.sentryEventNo.0=INTEGER - 1111
Walk     |.sentrySource.0=OCTET STRING - TEST SOURCE
Walk     |.sentryText.0=OCTET STRING - This is a simulation of a red alert trap
Walk     |.sentryTrap.0=INTEGER - 0
Walk     |End of MIB subtree reached.


TrapWatch|Quit event received - stopping trap thread
>>>>>>>>>|enter g to continue
```

The program functions as follows:

Config	Checks registry to see if SeNTry will send traps
Setup	Finds Community and Agent Names
TrapWatch	Spawns thread to listen for traps
Init	Connects to the SNMP Manager on given agent

Main	Requests contents of Sentry MIB
Walk	Lists the values of the Sentry variables
>>>>>>	Request program continuation
SetSNMP	Simulate a Red Alert Trap condition
TrapWatch	Should catch the trap (generic 6 specific1) and identify as a SeNTry trap
Main	Requests a new Walk
Walk	Show new values after simulated Red Trap
TrapWatch	Kill trap thread
>>>>>>	Request g to kill program

```
If you do not see all events as displayed above, or get errors or
inability to connect messages, then SNMP is not configured
correctly and the SeNTry trap mechanism will not work.
```

Note that if you are on the machine given as the Trap Destination you will see the valid trap received by the TrapWatch thread. If the destination is another machine you should run the command line program "**snmputil trap**" on that machine (snputil comes with the NT 3.51 Resource Kit).

However, the second walk through the database should show the trap values regardless of where the trap destination is.

If the names of the values are printed as numbers this means that your copy of MIB.BIN does not include the database definitions for the SeNTry variables. Either recompile it or copy the MIB.BIN from the sentry SNMP directory to the Windows System Directory.

14 Licensing SeNTry

SeNTry is licensed “by server” - i.e. SAGS will only accept connections from up to the licensed number of SASS services. SAGS itself is not counted in this list. When SeNTry is first installed it is licensed for evaluation purposes for 30 days for 4 servers.

```
Only SAGS servers need licensing.  Configuration and Sending
machines do not examine license codes.
```

If you purchase SeNTry, or if you wish to extend the evaluation for a longer time or with more servers then you will need to obtain new License Codes from Serverware. These codes are then inserted into the **SeNTry Licensing** Program which then updates the registry so that SAGS can read the new licensing information next time it starts.

You can enter licensing information from any machine by entering the server name in the appropriate text box.

```
You must be careful to enter these codes exactly as printed
```

SAGS will write warning Events into the Event Log as the expiry date approaches or the maximum number of servers is neared. If the maximum number of servers is reached then no more connections will be accepted. If the Expiry date is reached then the SAGS service will close.

SAGS will not start without valid license codes.

You should keep your license codes safely as the **SeNTry Registry Builder** will not restore corrupt or missing license codes.

```
You have thirty days to evaluate the product before the license
codes installed by the Setup program expire.
```

15 Sentry Registry Builder

SeNTry installs a **SeNTry Registry Builder** program that can be used to check and repair the Registry entries needed by Sentry Services for correct operation. The program also displays current release and version information. This program also checks the Licensing information and displays its state but never rebuilds corrupt or expired license codes.

The Registry Builder only checks the Local Registry.

The program is extremely simple to use and can do no harm to run as it only recreates corrupt entries.

```
This program is provided to help recover from problems.  It is
not needed in normal use. You should always run this program
before contacting ServerWare for support and include the Version
and Licensing information in your request.
```

16 Uninstalling SeNTry

If you decide not to purchase SeNTry after evaluation, you can use the **Uninstall SeNTry** program icon to remove its components from your computer after you have stopped and removed the SeNTry Services. Depending on what configuration changes you have made, this program may fail to remove all components and you may need to complete the task by performing the steps outlined in **Upgrading from Earlier Releases** to remove the rest. You may also wish to remove the service information from the registry and delete the Serverware registry entries if you are confident about handling the Registry Editor.

17 Creating Event Log Records from within your Applications

With the use of SeNTry monitor to provide an alerting mechanism, it is obviously useful for programmers and application developers to be able to create Event Log records themselves. This mechanism has been provided in Release 1.7 by means of a Dynamic Link Library containing two exported functions:

1. **MakeNewEventSource** to create a new Event Source for your application to use. The Event Source is the name by which you can identify services and applications in the Event Log
2. **WriteEventLogRecord** to write a record to the Application Event Log. You have five separate Event Message numbers to choose from. The description of the Event is entirely under users control. You can create events of type INFORMATION,WARNING or ERROR.

A Sample **Visual C++** 2.0 project is installed which exposes this functionality and can be used as a template to modify your own applications. A simple **Visual Basic 4.0** project is also provided which contains the correct Declares and Constants to access this DLL from Visual Basic

A simple Command Line interface is also available allowing batch jobs to write event log records. This can be very useful for checking such things as overnight audit or backup procedures.

Full information on these features can be found in the programs.hlp file in this subdirectory. An icon will have been created in the SeNTry program group.

If you want to include this functionality you must select the "Application Programming" option from the SETUP program. All components are installed in the **APIPROGS** subdirectory under the installation directory.

18 Index