

SNARE

System iNtrusion Analysis & Reporting Environment

Guide to SNARE for MSSQL

INTERSECT
ALLIANCE

Documentation History

Version No.	Date	Edits	By whom
1.0	15 May 2008	MSSQL agent documentation	InterSect
1.1	14 January 2011	Documented latest features	David Mohr

© 1999-2011 Intersect Alliance Pty Ltd. All rights reserved worldwide.

Intersect Alliance Pty Ltd shall not be liable for errors contained herein or for direct, or indirect damages in connection with the use of this material. No part of this work may be reproduced or transmitted in any form or by any means except as expressly permitted by Intersect Alliance Pty Ltd. This does not include those documents and software developed under the terms of the open source General Public Licence, which covers the SNARE agents and some other software.

The Intersect Alliance logo and SNARE logo are registered trademarks of Intersect Alliance Pty Ltd. Other trademarks and trade names are marks' and names of their owners as may or may not be indicated. All trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications and content are subject to change without notice.

About this guide

This guide introduces you to the functionality of the SNARE Microsoft SQL Server Agent within the Windows operating environment. The development of 'SNARE for MSSQL' will now allow for events generated by Microsoft SQL Server to be forwarded to a remote audit event collection facility. SNARE for MSSQL will also allow a security administrator to fully remote control the application through a standard web browser.

Other guides that may be useful to read include:

- SNARE Server User's Guide.
- Installation Guide to the SNARE Server.
- SNARE Server Troubleshooting Guide.
- The SNARE Toolset - A White Paper.

Table of contents:

1 Introduction	4
2 Overview of SNARE for MS SQL Server	5
3 Agent Installation	6
3.1 Prerequisites.....	6
3.2 Wizard Install.....	7
3.3 Silent Install.....	13
4 Service Status	15
5 Web Interface	16
5.1 Accessing the web interface.....	16
5.2 Accessing the web interface remotely.....	16
5.3 Navigating the web interface.....	18
5.4 Making Changes.....	18
5.5 Remote Control Configuration.....	19
5.6 Network Configuration.....	20
5.7 Objectives Configuration.....	24
5.8 Objective Configuration.....	26
5.9 Apply the Latest Audit Configuration.....	31
5.10 View Audit Server Status.....	32
5.11 Latest Events.....	33
6 SNARE Server	34
7 About Intersect Alliance	36
Appendix A - Event output format	37
Appendix B - SnareMSSQL registry configuration description	38
Appendix C - Objectives and security event IDs	40

1 Introduction



The team at Intersect Alliance have experience with auditing and intrusion detection on a wide range of platforms - Solaris, Windows NT/2000/2003/XP/2008/Vista/Win7, Netware, Tru64, Linux, AIX, IRIX even MVS (ACF2/RACF); and within a wide range of IT security in businesses such as - National Security and Defence Agencies, Financial Service firms, Government Departments and Service Providers.

This background gives us a unique insight into how to effectively deploy host and network intrusion detection systems that support and enhance an organization's business goals.

The development of 'SNARE for Microsoft SQL Server' allows events generated by MS SQL to be collected and forwarded to a remote audit collection facility. SNARE for MSSQL will also allow a security administrator to fully remote control and monitor the application through a standard web browser. SNARE has been designed in such a way as to allow the remote control functions to be easily effected manually, or by an automated process.

The overall project is called 'SNARE' - **System iNtrusion Analysis & Reporting Environment**. Event audit modules for Windows, Solaris, AIX, IRIX, Linux and other applications have been released under the terms of the GNU Public License. The '**SNARE Server**' is a commercial release of software beneficial to organizations that wish to collect from a wide variety of SNARE agents and appliances such as firewalls or routers.

Intersect Alliance welcomes and values your support, comments, and contributions. Our contact details are available from our contact page at www.intersectalliance.com.

2 Overview of SNARE for MS SQL Server

SNARE for MSSQL operates through the actions of the *SnareMSSQL* service *SnareMSSQL.exe*. The *SnareMSSQL* service interfaces with Microsoft SQL Server to initiate, read, filter and send trace logs from MSSQL to a remote host or a local log file.

The *SnareMSSQL* service can be configured to monitor a variety of MSSQL installation types. The default objective template will monitor the master database within the default local MSSQL instance. This can be modified on a per objective basis to specify a named MS SQL instance and a database within that instance. Snare for MSSQL can also be used to monitor SQL instances running on a failover cluster. See chapters 3, Agent Installation on page 6, and 5.7, Objectives Configuration on page 24, for more information on configuring objectives.

The *SnareMSSQL* service is controlled and monitored using a standard web browser.



Figure 1: The SnareMSSQL Web Interface

This web interface can be used either locally or remotely to control the operation of the *SnareMSSQL* Agent. See chapter 5, Web Interface, on page 16 for more information on gaining access to the *SnareMSSQL* web interface.

3 Agent Installation



SnareMSSQL is available as a self-contained installation package, and includes a setup wizard and silent install options to allow for easy installation and configuration of all critical components. The installation package includes various support files, and the following core components:

- *SnareMSSQL.exe*

The *SnareMSSQL* service is contained in the '*SnareMSSQL.exe*' binary. This binary implements all the functionality required to initiate trace logs, read trace log records, filter events according to the objectives, provide a web based remote control and monitoring interface, and includes all the necessary logic to act as a service under Windows 2000/2003/2008/2008R2 or XP/Vista/Win7.

SnareMSSQL has two distinct deployment scenarios:

- Stand alone scenario

This scenario involves a single system running one or more instances of MS SQL Server. The *SnareMSSQL* installer will deploy a single service with the capability to monitor all available instances.

- Failover cluster scenario

This scenario involves two or more systems, operating as a Windows failover cluster, running one or more instances of MS SQL Server. The *SnareMSSQL* installer will deploy one service per instance, on every available node, and each service will have the capability to continue monitoring its assigned MS SQL instance in the event of a system failure (or any other event which causes the instance to change its operating node). The *SnareMSSQL* installer need only be run on one node with sufficient privileges to distribute the agent to the remaining nodes, that is, administrator privileges on all cluster nodes.

3.1 Prerequisites

The *SnareMSSQL* Agent has the following requirements:

- For stand alone instances,
 - Windows 2000/2003/XP/Vista/2008/Win7/2008R2, 32 or 64 bit architecture
 - Microsoft SQL Server 2000 or above must be installed, 32 or 64 bit architecture
- For clustered instances,
 - Windows Server 2003/2008/2008R2, 32 or 64 bit architecture arranged in a failover cluster
 - Microsoft SQL Server 2005 or above, 32 or 64 bit architecture in either a single or multiple instance deployment
- The drive where *SnareMSSQL* is installed requires a minimum of 10MB of free space. Additional free space is required to operate the agent, see Event Log Retention on page 31, for more information on objective space requirements

3.2 Wizard Install

Download the SnareMSSQLSetup-*{Version}*.exe file from the Intersect Alliance website (where *{Version}* is the most recent version of the file available).

Ensure you have administrator rights, double-click the SnareMSSQLSetup-*{Version}*.exe file. This is a self extracting archive, and will not require WinZip or other programs.

You will be prompted with the following screens in all deployment scenarios:

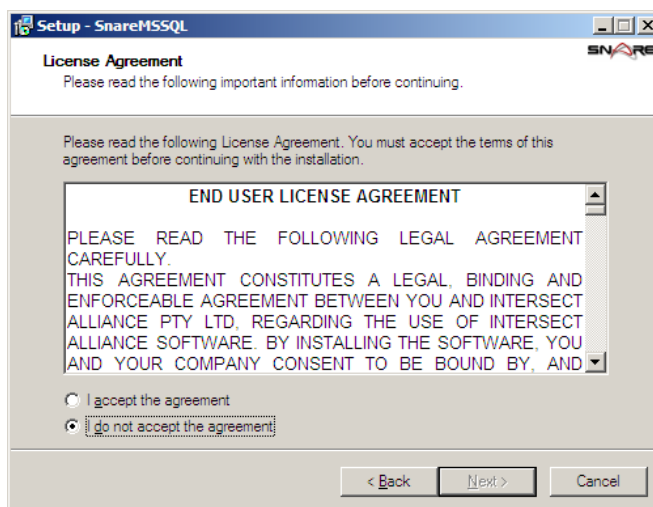
Welcome to the SnareMSSQL Setup Wizard



This screen provides a brief overview of the product you are about to install.

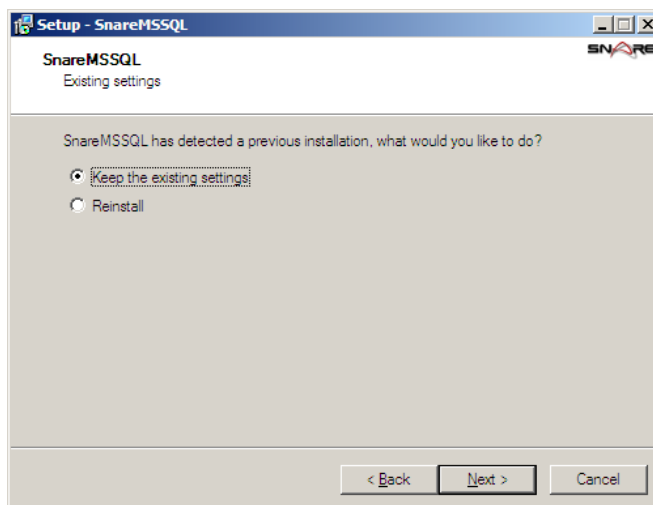
Where available, select “Next” to continue the installation, “Back” to return to the previous screen or “Cancel” to abort the installation.

License Page



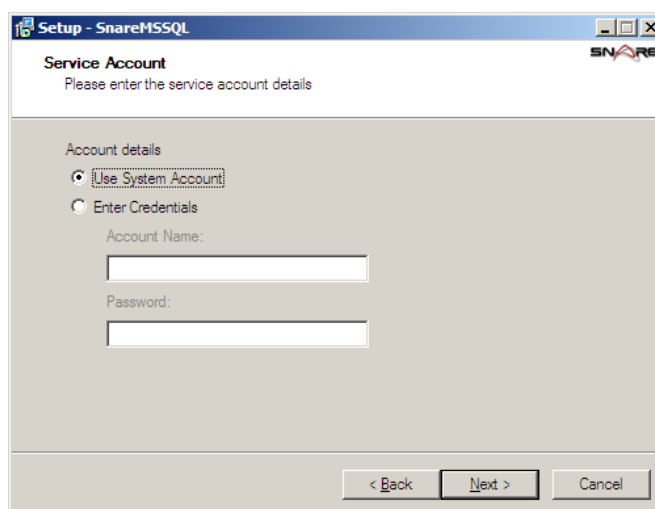
The License Page displays the End User License Agreement (EULA). Please read the document carefully and if you accept the terms of the agreement, select “I accept the agreement” and the “Next” button will be enabled allowing the installation to continue.

Existing Install (Upgrade only)



If the Wizard detects a previous install of the SnareMSSQL agent, you will be asked how to proceed. Selecting “Keep the existing settings” will leave the agent configuration intact and only update the SnareMSSQL files. The Wizard will then skip directly to the Ready to Install screen. Selecting “Reinstall” will allow the configuration wizard to continue and replace your existing configuration with the values you input. Note that replacing the configuration does not happen immediately; it takes place after selecting the “Install” button on the Ready to Install screen.

Service Account

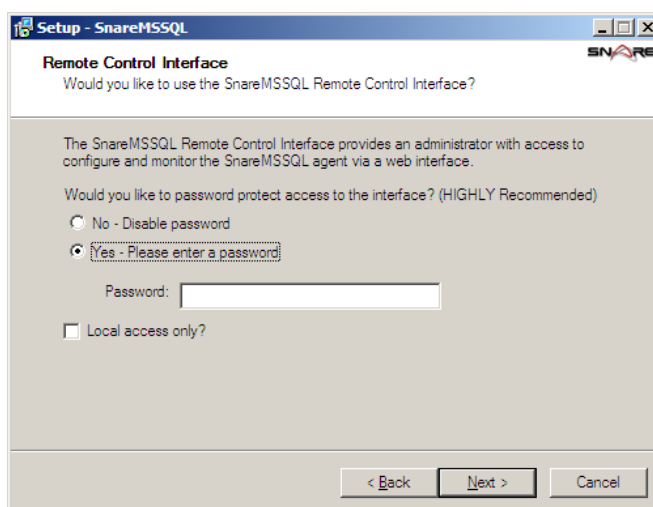


The SnareMSSQL agent requires a service account to operate. It uses this account for two main purposes:

- **Run the service.** The SYSTEM account is the default choice. Any credentials provided will require permission to run as a service.
- **Authenticate to the MS SQL instance(s) being monitored.** By default, MS SQL instances grant the SYSTEM account sufficient access to manage traces (i.e. the ALTER TRACE permission), otherwise, a custom service account will be required. Based on the deployment scenarios described at the start of this chapter, other authentication options may be available.
 - **Stand alone scenario.** Two authentication options are available. As described above, the service account can be used for authentication, however, an alternate username and password can also be assigned on a per-objective basis, bypassing the need to use the service account credentials. For more details, see chapter 5.8, Objective Configuration on page 26.
 - **Failover cluster scenario.** For security reasons, alternate credentials are not stored by the agent. Therefore the service account credentials are the only method of authentication available.

For more information, see chapter 5.8, Objective Configuration on page 26.

Remote Control Interface



This screen provides a means to configure the *SnareMSSQL* Agent's web interface for first time use.

Select one of the following options to configure the *SnareMSSQL* web interface:

- “No - Disable password”

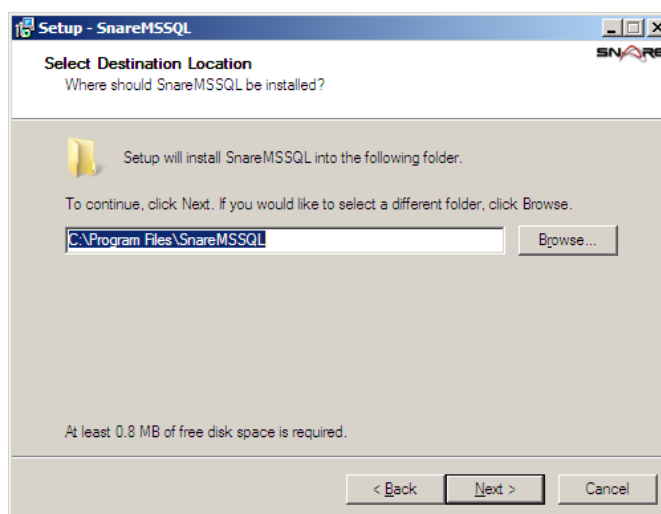
The web interface will operate without a password, allowing unauthenticated access to the configuration options.

- “Yes - Please enter a password”

A user/password combination will be required to access the web interface. The user is always “snare” and the password will be set to text supplied in the “Password” field.

Selecting “Local access only” will configure the web interface to restrict access to local users only. Remote users will be unable to contact the web interface. For clustered instances, this equates to the current owner of the SnareMSSQL resource.

Select Destination Location

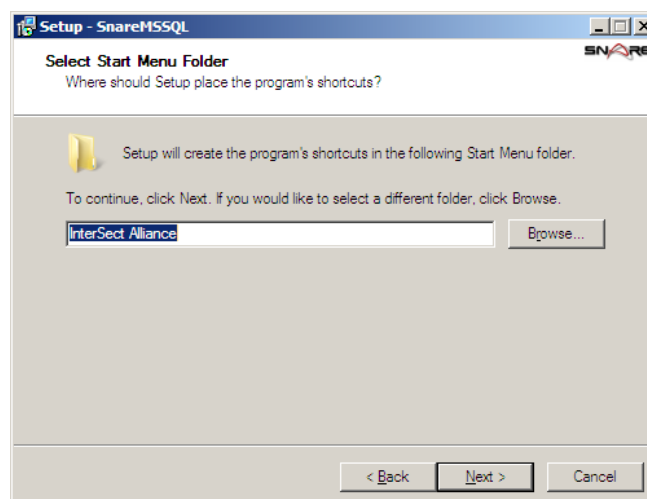


This screen provides a means to select the folder where the *SnareMSSQL* Agent will be installed. If the folder name specified does not exist, it will be created. In a failover cluster scenario, this location will be created on all available nodes.

It is important that this folder has at least enough space available to install the agent. By default, this folder will also be used for storing trace files, however an alternate location can be nominated via the Network Configuration window (see chapter 5.6 on page 20). Also, see the section Event Log Retention, on page 31 for more information on space requirements for trace files.

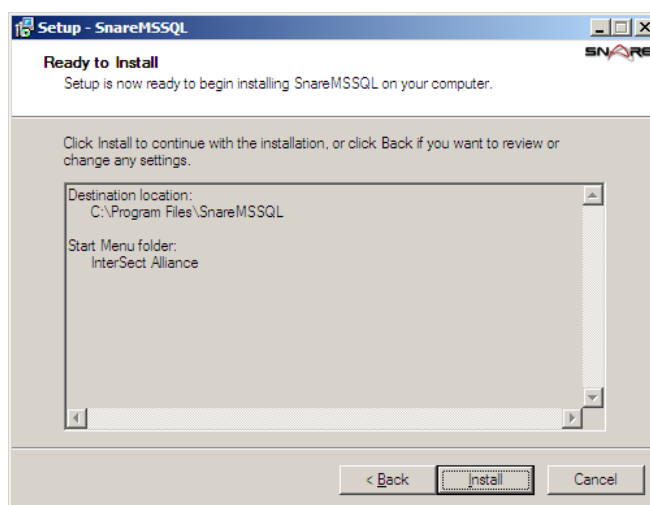
By default, the installation wizard will install *SnareMSSQL* under the *Program Files* folder. If a different destination is desired, one may be selected via the “Browse” button, or by typing the full path name directly into the box.

Select Start Menu Folder



Select the program group within the *Start Menu* under which a shortcut to the Snare MSSQL Agents remote control interface will be created.

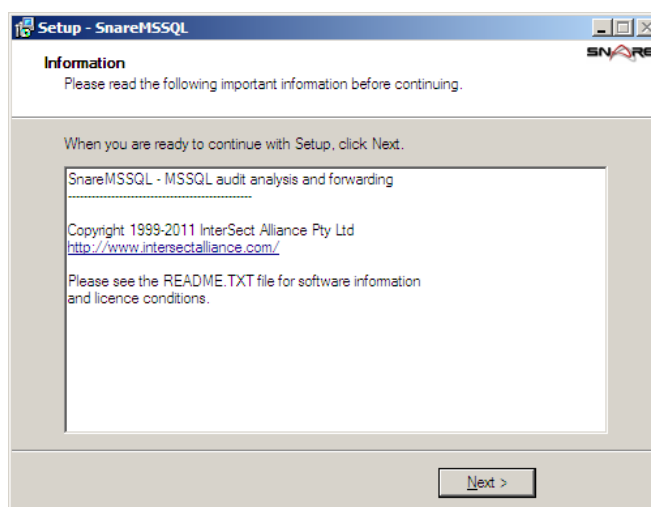
Ready to Install



This screen provides a final summary of the chosen installation options. If the options listed are incorrect, select the “Back” button to return to previous screens and change their configuration.

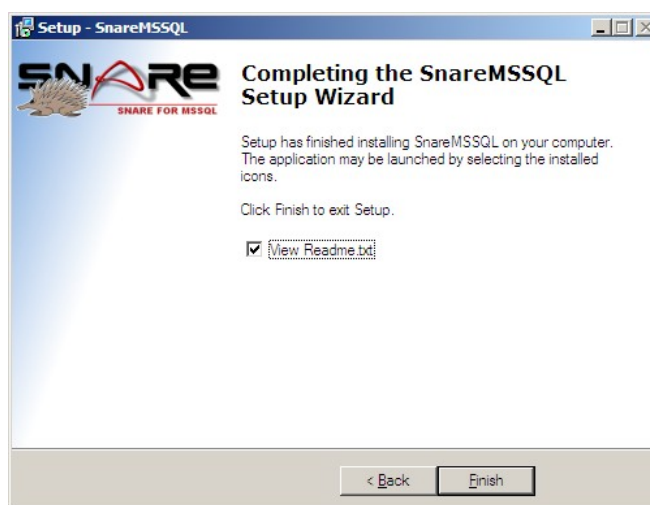
Select the “Install” button to proceed with the listed choices, or “Cancel” to abort the installation without making any changes. The “Back” button may be used to return to the previous screen.

Information



This screen provides basic copyright information and last minute documentation which may not be included within this manual.

Completing the SnareMSSQL Setup Wizard



This is the final screen of the installation wizard. By default, a Readme.txt file will be opened after selecting “Finish”. Please review this readme for details of the changes made to the agent.

3.3 Silent Install

The silent install option is provided for system administrators wishing to automate the process of installing SnareMSSQL.

Command line options

The SnareMSSQL installer has a number of command line options to support silent, automated installations in either deployment scenario:

- **/VerySilent** - The Wizard will be hidden for the duration of the installation process. Any message boxes will still be displayed.
- **/SuppressMsgBoxes** - Any messages boxes will be dismissed with the default answer.
- **/Log="filename"** - Two log files will be create: *filename* and *filename.Snare.log*. The Wizard installation log will be written to *filename* and a detailed SnareMSSQL installation log will be written to *filename.Snare.log*.
- **/LoadInf="INFfile"** - The *INFfile* is a template file produced by another SnareMSSQL installation. It contains all the necessary information to complete the installation and configure the agent for normal operations. See below for more details on how to produce this file.
- **/SnarePass="ZPass"** - For security reasons, some parts of the *INFfile* are encrypted and require a decryption password. *ZPass* is an encrypted version of the decryption password and is produced as part of the *INFfile* procedure.
- **/Reinstall** - Tell the installer to overwrite any existing installation.
- **/Upgrade** - Tell the installer to upgrade the existing installation. If no existing installation is detected, the installer will abort. This option will only upgrade the SnareMSSQL files, all configuration settings will remain untouched and the “LoadInf” file will be ignored.

Silent Install Setup Information File (INF)

To silently deploy a completely configured agent, the installer requires the help of a Setup Information File, also known as an INF file. To produce a working INF file, follow these steps:

1. Install the SnareMSSQL agent using the Wizard.
2. Using the web interface (chapter 5 on page 16), configure the agent's Network, Remote Control and Heartbeat settings.
3. Configure one or more objectives (chapters 5.7 and 5.8 starting on page 24) targeting just one MSSQL instance.
4. Ensure you have administrator rights, open a command prompt and browse to the directory where SnareMSSQL is installed.
5. Run the following commands:
 - **SnareMSSQL.exe -x**
Export the information and error messages, along with the INF file contents to the screen.
 - **SnareMSSQL.exe -x "INFfile"**
Export the information and error messages to the screen and write the INF file contents to *INFfile* for use with the /LoadInf command line option.
6. Follow the prompts carefully and where required, enter the necessary password information for either the Service Account and/or the Sensitive Information encryption.
7. Note down the Installation Password. The /SnarePass command line option will accept this encrypted password and use it to decrypt the sensitive information in *INFfile*.

Silent Deployment

To install using the silent installer, ensure you have administrator rights, open a command prompt and browse to the directory where the setup program is stored. Using the "/verysilent" option, run the file:

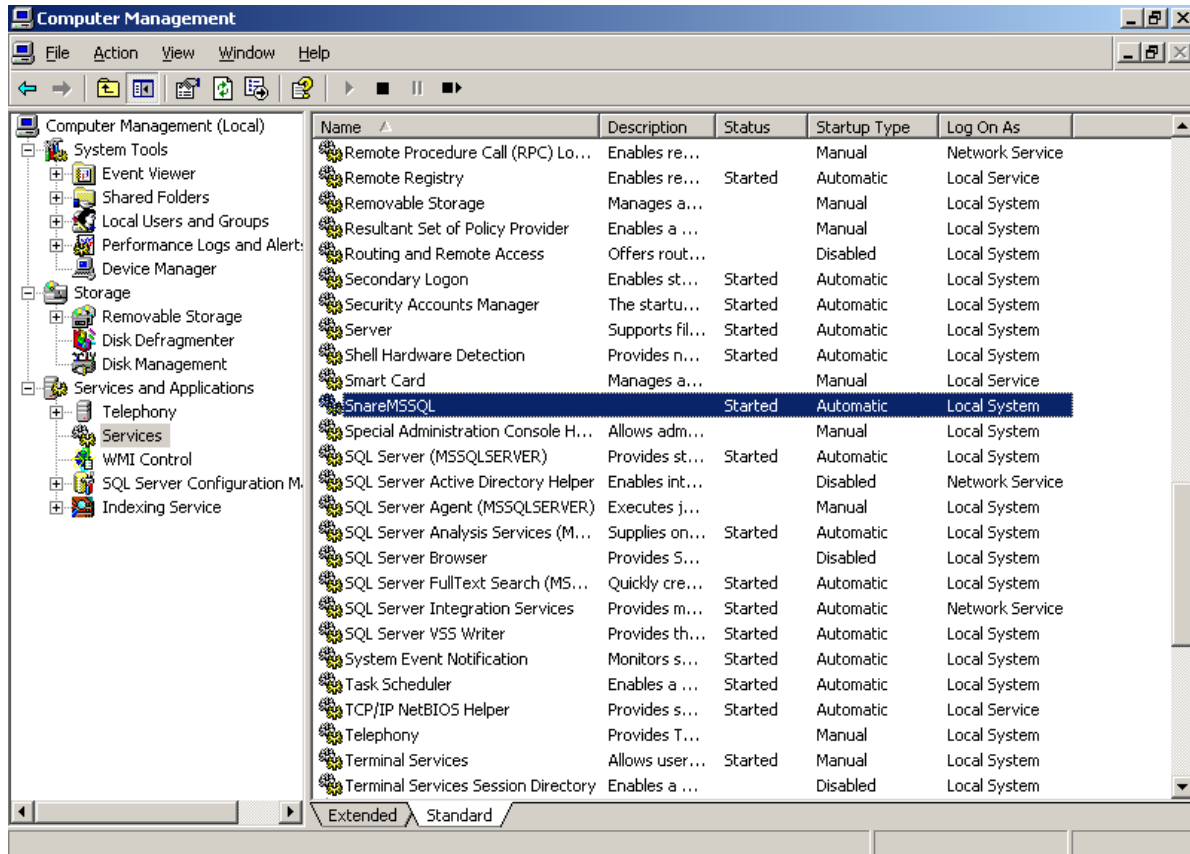
```
SnareMSSQLSetup-{Version}.exe /verysilent /suppressmsgboxes /LoadInf="Settings.inf"
```

This will install the *SnareMSSQL* application with the options specified in the Settings.INF file and will not display any pop-up windows. This option is suitable for packaging and non-interactive installations. For deployment in a failover cluster scenario, this command only needs to be run on one node by an account with administrator privileges on all nodes.

4 Service Status



For events to be collected, the *SnareMSSQL* service or services must be running. The status of the *SnareMSSQL* services may be confirmed via the Services listing in Windows. The Services listing may be found either under Administrative Tools or by selecting Services from Control Panel->Administrative Tools->Computer Management->Services.



For stand alone installations (see chapter 3, Agent Installation on page 6, for details on the deployment scenarios), if the service is not running, select **start** and **automatic** so that the service is started automatically when the host is rebooted.

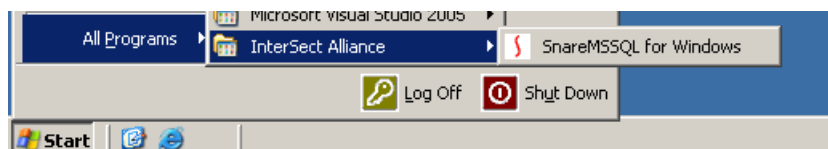
For failover cluster installations, there might be one or more services. Each service will be identified by the SnareMSSQL name followed by a dollar sign and the name of the instance being monitored, e.g. SnareMSSQL\$NamedInst.

Once the *SnareMSSQL* Service is running, its status can be viewed via the web interface. See chapter 5.10, View Audit Server Status, on page 32 for more information on viewing the *SnareMSSQL* status via the web interface.

5 Web Interface

5.1 Accessing the web interface

Upon installation of the *SnareMSSQL* agent, an “Intersect Alliance”¹ menu item is created on the Windows Start menu. The *SnareMSSQL* remote control interface is then available² from “Programs->Intersect Alliance->SnareMSSQL for Windows”.



If the menu launcher is not available, the *SnareMSSQL* web interface may be accessed via a web browser from the local machine by visiting the URL <http://localhost:6163/>³. If you previously configured a password, you will need this to log in, along with the username “snare”.

5.2 Accessing the web interface remotely

The *SnareMSSQL* web interface may be accessed via a web browser by visiting the URL [http://\[computer-name\]:\[port-number\]/](http://[computer-name]:[port-number]/). Computer name should be replaced with either the direct IP address of the machine or cluster to be controlled, or a name which resolves to that IP address.

Example: Contact the machine “SQLSERVER” on port “6163”.

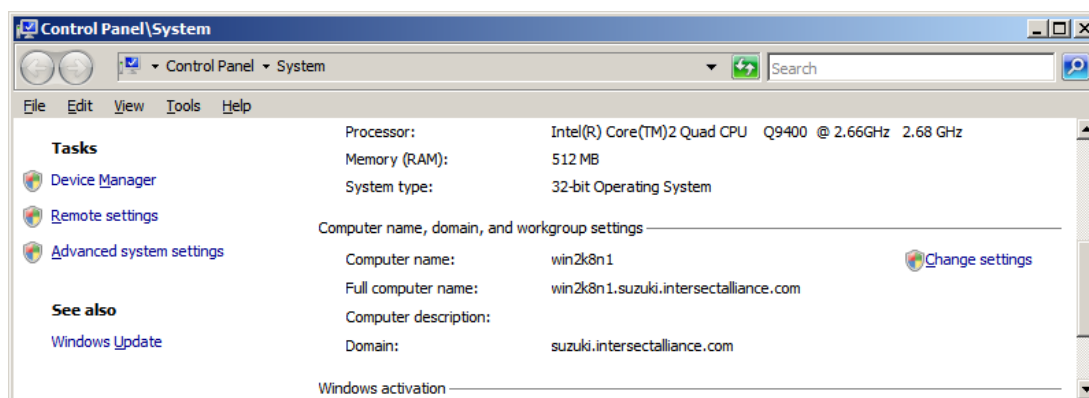
<http://SQLSERVER:6163/>

Example: Contact the machine “10.5.33.183” on port “6163”.

<http://10.5.33.183:6163/>

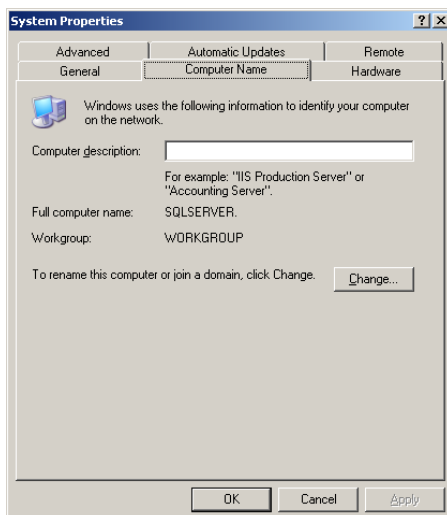
Determine computer name

To determine the name of a computer in a stand alone deployment scenario, browse to “Control Panel->System” and find the text after the label “Computer name”:

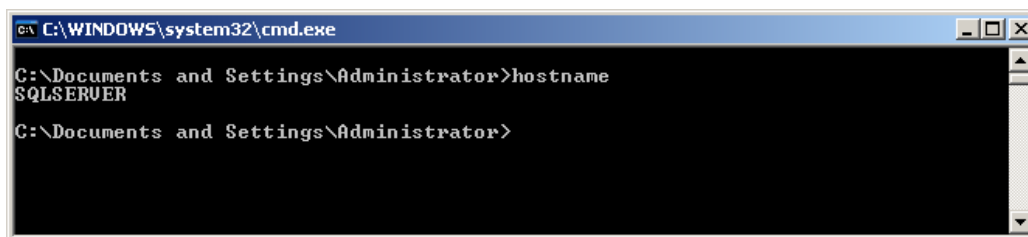


- 1 This is the default program group created by the installation system. If another program group was selected during installation please refer to that selection.
- 2 The *SnareMSSQL* Web Interface will not be available if it has been disabled in the registry. If the web interface is disabled then *SnareMSSQL* must be configured via the registry.
- 3 6163 is the default port for the *SnareMSSQL* web interface. If a different port has been chosen, please replace this with the chosen number.

For versions of Windows prior to Vista, browse to “Control Panel->System->Computer Name” and find the text after the label “Full computer name”:

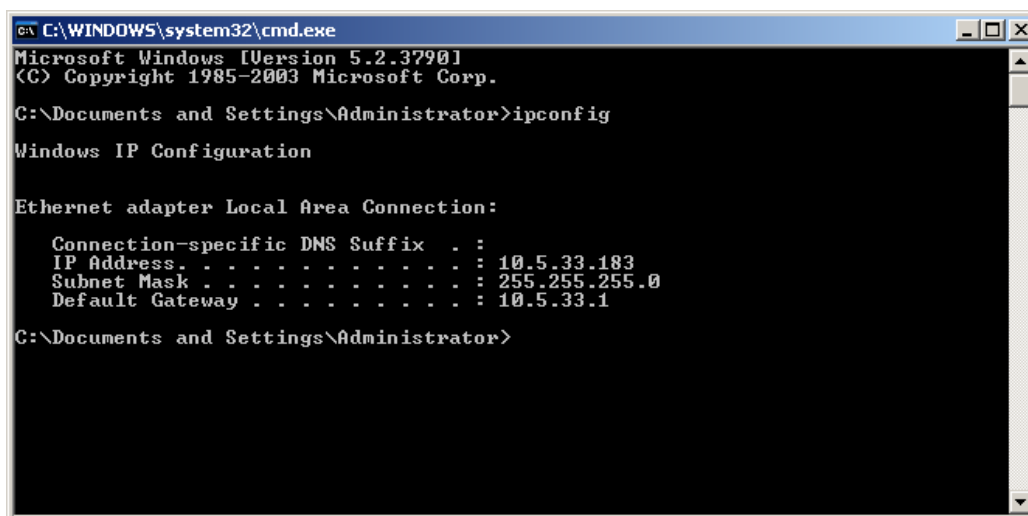


Alternatively, open a command prompt and type the command “hostname”:



Determine IP address

Open a command prompt and type “ipconfig”:



Find the text after the label “IP Address....”:

5.3 Navigating the web interface



Figure 2: Navigating the web interface

The *SnareMSSQL* web interface contains a title bar, a navigation pane and a content area.

Title bar

The title bar contains the Intersect Alliance logo and the title of the *SnareMSSQL* agent.

Navigation pane

The navigation pane is used to navigate the functional areas of the *SnareMSSQL* agent. Each section is listed in detail below.

Content area

The content area is filled with contextual information according to the functional area selected from the navigation pane.

5.4 Making Changes

To save the changes made within one of the forms below, select the “Change Configuration” button. Saved changes will not take effect until the *SnareMSSQL* Agent is restarted. See chapter 5.9, Apply the Latest Audit Configuration on page 31, for more information on applying saved changes.

5.5 Remote Control Configuration

A critical function of the *SnareMSSQL* service is its ability to be remote controlled. The *SnareMSSQL* service employs a custom designed web server to allow configuration through a browser. The parameters which may be set for remote control operation are shown in Figure 3 and discussed in detail below:



Figure 3: Remote Control Configuration

Restrict remote control of SNARE agent to certain hosts

Use this setting to restrict access to the *SnareMSSQL* web interface based on IP address. If this option is selected, then only hosts that use the designated IP address are allowed access to the web interface.

Restrictions based on IP address are prone to spoofing¹. It is advisable that this security measure be used in conjunction with other countermeasures.

IP Address allowed to remote control SNARE

If the “Restrict remote control of SNARE agent to certain hosts” checkbox is selected, then this field may be used to specify the IP address of a computer which may access the *SnareMSSQL* web interface. If only local access is required, then setting this to “127.0.0.1” will restrict access to the local machine.

¹ IP Spoofing is a technique whereby an attacker sends messages to a computer with an IP address indicating that the message is coming from a trusted host.

Require a password for remote control

When selected, users contacting the web interface are required to provide a username and password. The username is always “snare” and the password must match the one provided below in the “Password to allow remote control of SNARE” field.

Password to allow remote control of SNARE

If the “Require a password for remote control” checkbox is selected, then this field is used to specify the password a user must enter to gain access to the web interface.

Change Web Server default (6163) port

Normally, a web server operates on port 80. If this is the case, then a user need only type the address into the browser to access the site. If however, a web server is operating on port (say) 6163, then the user needs to type <http://mysite.com:6163> to reach the web server. The default *SnareMSSQL* web server port (6163) may be changed by selecting this checkbox and specifying a new port number in the field below. Care should be taken to note the new server port, as it will need to be placed in the URL to access the *SnareMSSQL* web interface.

See chapter 5, Web Interface, on page 16 for more information on connecting to the *SnareMSSQL* web interface.

Web server port

If the “Change Web Server default (6163) port” checkbox is selected, then this field is used to specify the new port which the *SnareMSSQL* web interface will operate on.

5.6 Network Configuration

The Network Configuration is used to specify how and where *SnareMSSQL* will output its event logs.

The initial audit configuration parameters to consider are:

- The location, size and number of Trace files used, per objective, while monitoring is in progress.
- The hostname, IP address and UDP or TCP port of the remote collection server. SNARE Server users should only send events to UDP or TCP port 6161.
- The location and size of a local log file, if required.
- The requirement to incorporate a SYSLOG header.
- If 'SYSLOG' is used, and if 'Dynamic' is selected as the SYSLOG priority value, the priority sent to the remote SYSLOG server will mirror the SNARE 'criticality' value of the matched objective.

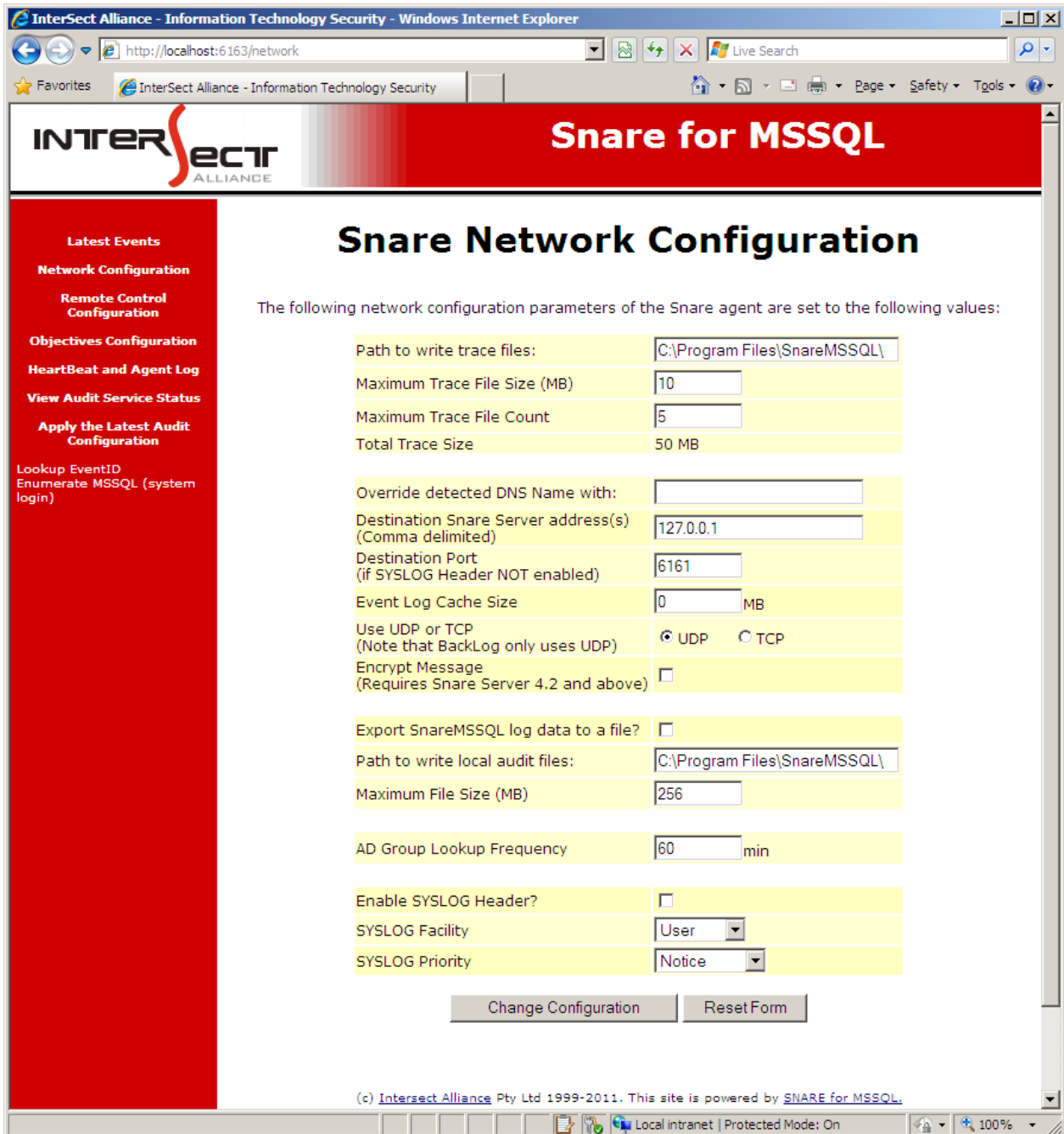


Figure 4: Network Configuration

Path to write trace files

This is the path where MS SQL Server will write the trace files on behalf of SnareMSSQL. The MS SQL Server service account or accounts must have write access to this folder for the trace files, and subsequently SnareMSSQL, to operate correctly.

Maximum Trace File Size

As the trace files are written to disk, this value, in megabytes, will define the maximum size of any single trace file. Once a trace file reaches the maximum size specified, that trace file will be closed and a new file opened.

Maximum Trace File Count

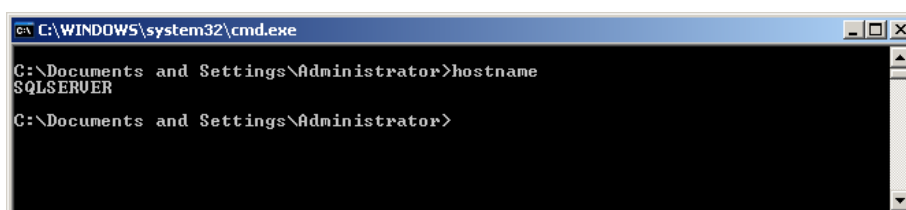
The Trace File Count defines how many files can exist at any given time. As new trace files are required, the oldest trace files are deleted to ensure the total number of files does not exceed the Trace File Count.

Total Trace Size

Based on the Trace File Size and Count fields, this value will automatically update to show the storage space required per objective.

Override detected DNS Name with

The “Override detected DNS Name” field can be used to override the name that is given to the host when Windows is first installed. Unless a different name needs to be sent in the processed event log record, leave this field blank, and the *SnareMSSQL* service will use the default host name set during installation. Note that executing the command `hostname` from a command prompt window will display the current host name allocated to the host.



```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>hostname
SQLSERVER
C:\Documents and Settings\Administrator>
  
```

Destination Snare Server address

Specify the IP address or hostname of the Snare Server or other network device which will collect events from this agent.

Destination Port

Specify the destination port of the Snare Server or other network device which will collect events from this agent. By default Snare Servers receive logs from agents on port 6161. Only change this if your Snare Server has been configured differently.

Event Log Cache

This value represents the size, in megabytes, of the cache that will be kept by SnareMSSQL if communications are lost with the Snare Server or other network device. Due to the nature of the network communication protocols available, this option is only valid for TCP connections.

Use UDP or TCP

The agent supports two network communication protocols: TCP and UDP. TCP is a guaranteed delivery protocol and will detect the availability of the Snare Server or other network device. If the destination is unavailable, the agent will cache any unsent messages, up to the size specified by the Event Log Cache and forward them once the destination server is available once more.

Encrypt Message

For use only with a Snare Server, this option will encrypt all outgoing messages being sent across the network.

Export SnareMSSQL log data to a file

Select this option to have the SnareMSSQL agent log audit events to a file.

Path to write local audit files

Specify the directory to write the audit log files. These files will be rotated on a daily basis, or when the Maximum File Size is reached, whichever comes first.

Maximum File Size

Audit log files written by the SnareMSSQL will not exceed this size.

AD Group Lookup Frequency

Objectives allow the use of Active Directory group identifiers in the User Search Term (see section User Search Term on page 30). This setting defines the frequency, in minutes, that the agent will recheck the members of any groups identified.

Enable SYSLOG Header

The SYSLOG function is a UNIX based service that allows for event records to be processed remotely, but has the requirement that the event records need to be in a specific format. This feature will allow the event log record to be formatted so as to be accepted by a SYSLOG server.

For more information on SYSLOG, consult your SYSLOG server documentation.

SYSLOG Facility

Discussion of the “SYSLOG Facility” option is beyond the scope of this document. Consult your SYSLOG server documentation for further information on this field.

SYSLOG Priority

Discussion of the “SYSLOG Priority” option is beyond the scope of this document. Consult your SYSLOG server documentation for further information on this field.

5.7 Objectives Configuration

The primary function of the *SnareMSSQL* system is to monitor and filter events from MS SQL trace logs. This is accomplished via “Objectives”. Objectives monitor a list of specified MS SQL events from selected databases and propagate the information according to the Network Configuration as discussed in previous chapters.



Figure 5: Objectives Configuration

Objectives List

Once an objective is configured, the “Objectives Configuration” window will show a list of configured objectives. Each objective is listed with a summary of information as well as buttons to modify or delete the objective, or check the current members of any groups specified in the User Search Term. See chapter 5.8, Objective Configuration, on page 26 for information on the exact meaning of each summary column.

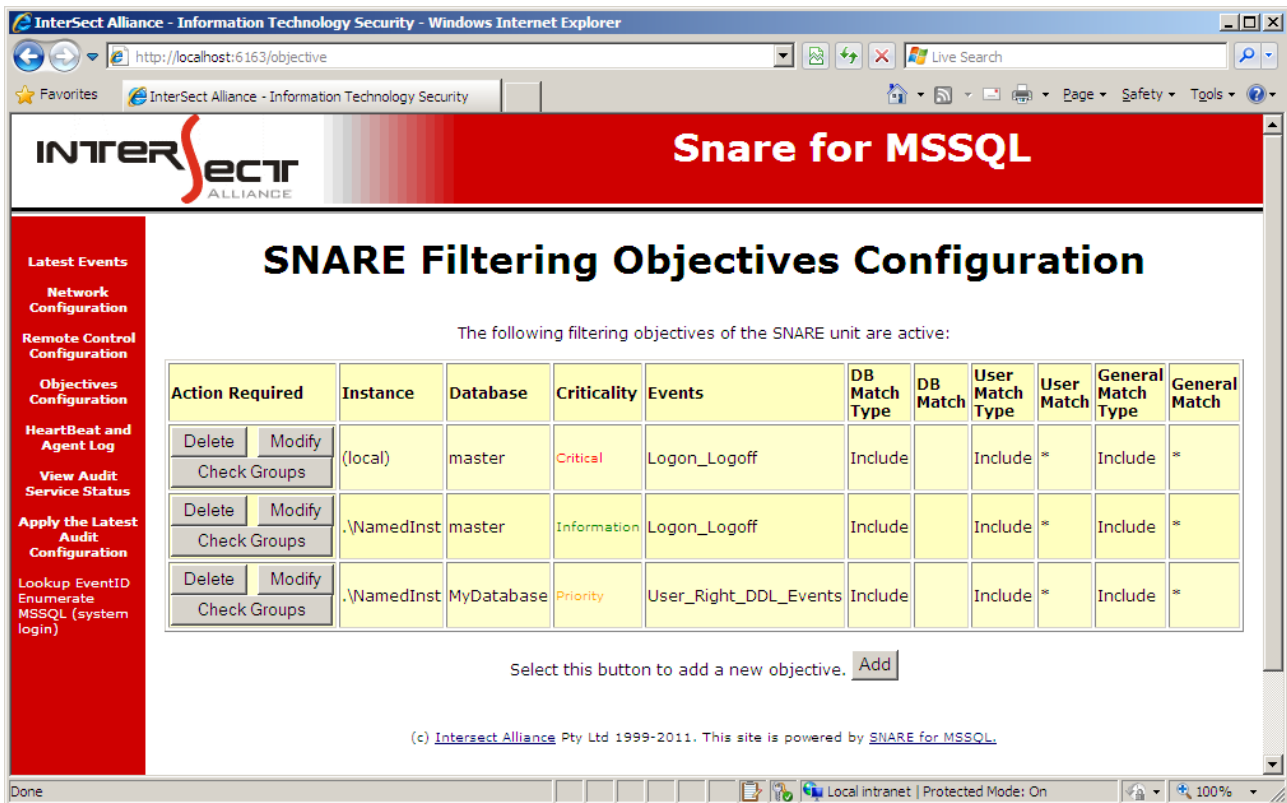


Figure 6: Objectives Configuration List

Adding an Objective

By default, when *SnareMSSQL* is first installed, no objectives are configured. To add an objective, select the “Add” button.

Changing an Objective

To modify an objective, select the “Modify” button located next to the objective to be modified.

Removing an Objective

To remove an objective, select the “Delete” button located next to the objective to be removed.

Check Groups

To check the current members of any groups specified in the User Search Term, select the “Check Groups” button located next to the objective to be checked. A list of all group and sub-group members will be displayed.

5.8 Objective Configuration

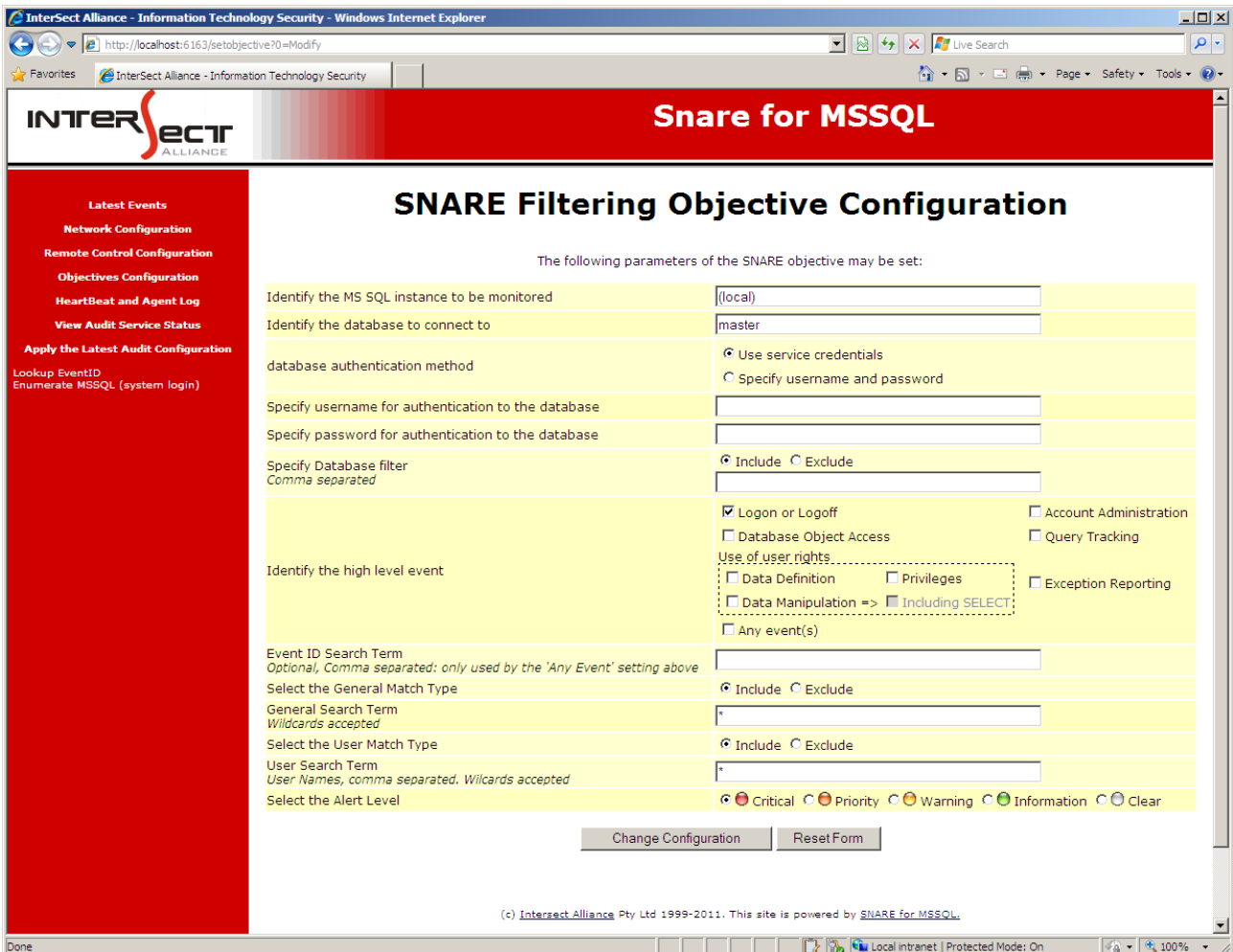


Figure 7: Objective Configuration

Database connection

In SnareMSSQL, each objective in a stand alone deployment scenario provides settings to customize its connection to the database. In a failover cluster scenario, the database authentication method, username and password options are not available.

Identify the MS SQL instance to be monitored

Specifies the MS SQL instance to be monitored. For local default installations of MSSQL, leave this field as “(local)”. For named instances use the notation “.\\InstanceName”, where “InstanceName” is the name of the instance to be monitored.

Identify the database to connect to

Specifies the database to initially connect to within the chosen instance.

Database authentication method

By default the SnareMSSQL agent will connect to MS SQL using the current service account credentials. If this is not desired, then selecting “Specify username and password” will allow the administrator to choose which user *SnareMSSQL* connects to MS SQL with.

Username and Password for authentication to the database

If “Specify username and password” is selected then these fields allow the administrator to input the details which *SnareMSSQL* will use when connecting to MS SQL. The chosen user must be granted the necessary rights to perform “SP_TRACE_CREATE” upon the chosen database. At a minimum, these rights include the “Alter Trace” permission.

For more information on the required rights to perform “SP_TRACE_CREATE”, consult your MS SQL Server documentation.

Database Filter Match Type

The “Database Filter Match Type” determines how the “Database Filter Search Term” filter will be applied. If “Include” is selected (the default), then only events relating to databases listed in the “Database Filter Search Term” will be monitored. If “Exclude” is selected, then only events relating to databases NOT listed in the “Database Filter Search Term” will be monitored.

Database Filter Search Term

The “Database Filter Search Term” allows the user to specifically identify which databases should be monitored.

Search terms may not contain any wildcards, instead exact database names should be listed.

Example: Monitor events from the “Finance” and “Inventory” databases

Database Filter Search Term: Finance,Inventory

Event Selection

Each of the objectives provides a high level of control over which events are selected and reported. Events are selected from a group of high level requirements, and further refined using selected filters.

High level event selection

The high level event specification field allows the administrator to choose one or more predefined sets of events, based upon the chosen group. These groups allow easy selection of some of the most common security objectives. Details on which trace event IDs are used to generate the following objectives can be found in *Appendix C - Objectives and security event IDs on page 40*.

- Logon or Logoff
- Account administration
- Database Object Access
- Query Tracking

- Use of user rights
 - Privileges
 - Data Definition, e.g. CREATE, ALTER permissions
 - Data Manipulation e.g. INSERT, UPDATE permissions
 - . SELECT permission
- Exception Reporting

If an administrator requires finer control, then selecting **Any event(s)** will allow a detailed list of event IDs to be specified via the **Event ID search term** field.

Event ID search term

If the Any event(s) objective is selected then the **Event ID search term** is used to select the specific events to monitor. Each event contains a unique number known as the **Event ID**. It is this number which is used to defined which events will be monitored.

To select an individual event to monitor, specify its Event ID:

Example: Select only the login event (Event ID 14)

Event ID search term: 14

To select a range of events to monitor, specify the first and last Event ID within square braces:

Example: Select all events from 14 to 20 (inclusive)

Event ID search term: [14-20]

To select all available events, use a star (*):

Example: Select all available events

Event ID search term: *

Multiple events may also be selected by separating the selections with a comma (,):

Example: Select only the login event (Event ID 14), the log off event (Event ID 15) and the failed login event (Event ID 20)

Event ID search term: 14,15,20

Example: Select the events 14, 15 and 20, all the events from 80 to 90 (inclusive) and all the events from 100 to 200 (inclusive)

Event ID search term: 14,15,20,[80-90],[100-200]

Events may also be removed from the list by prefixing a term with a minus (-):

Example: Select all events, except for 14 and 15

Event ID search term: *,-14,-15

Search terms are read left to right. This causes the right-most terms to take precedence.

Example: Select all events from 1 to 19 (inclusive) and from 31 to 100 (inclusive)

Event ID search term: [1-100],[-20-30]

Example: Select all events from 1 to 100 (inclusive). Note that the first term, “-[20-30]”, is overridden by the second term, “[1-100]”.

Event ID search term: `-[20-30], [1-100]`

The terms for the high level event groups listed in Appendix C, Objectives and security event IDs on page 40, can also be used directly in the Event ID Search Term.

Example: Select all events from the Account Admin and Transaction high level groups

Event ID search term: `[account-admin],[transaction]`

For a complete breakdown of all available event IDs, see the Microsoft Developer Network documentation at <http://msdn2.microsoft.com/en-us/library/ms186265.aspx>

Filtering

Once an event has been collected, it may be included or excluded based upon the objective's filter. All objectives operate independently of each other, so what is included or excluded in one objective will have no effect on any other objective.

Text

Text filtering may be performed on the textual payload of each event.

If text filtering is not desired (the default), specify “Include” for the “General Match Type” and specify “*” for the “General Search Term”.

Select the General Match Type

The “General Match Type” determines how the “General Search Term” filter will be applied. If “Include” is selected (the default), then any event failing to matching the “General Search Term” is discarded by the agent. If “Exclude” is selected, then any event matching the “General Search Term” is discarded by the agent.

General Search Term

The “General Search Term” allows the user to further refine a search based on the event record payload.

Search terms may contain wild cards such as “*”, which matches any number of characters, or “?”, which matches any single character.

Example: Select all events which contain the text “SELECT”

General Search Term: `*SELECT*`

Multiple search terms can be specified by separating them with commas.

Example: Select all events which contain the text “SELECT” or the text “IsShutDown”

General Search Term: `*SELECT*,*IsShutDown*`

Search terms are not case sensitive.

User

User filtering allows the administrator to determine which users will be audited.

If user filtering is not desired (the default), specify “Include” for the “User Match Type” and specify “*” for the “User Search Term”.

Select the User Match Type

The “User Match Type” determines how the “User Search Term” filter will be applied. If “Include” is selected (the default), then any event failing to matching the “User Search Term” is discarded by the agent. If “Exclude” is selected, then any event matching the “User Search Term” is discarded by the agent.

User Search Term

The “User Search Term” is a comma separated list of user names or Active Directory groups used to filter events from this objective.

User-related search terms may contain wild cards such as “*”, which matches any number of characters, or “?”, which matches any single character.

Example: Match all users

User Search Term: *

Example: Match all user names containing either “smith” or “john”

User Search Term: *smith*,*john*

Example: Match only the users “Paul”, “John” and “Alice”

User Search Term: Paul,John,Alice

Group-related search terms need to be enclosed in square brackets and can optionally contain a flat or DNS domain name. If no domain is specified, the local machine's domain membership will be used. To enumerate the members of any AD groups, the service account credentials are used.

Example: Match the “sqlaccess” AD group

User Search Term: [sqlaccess]

Example: Match the AD group “sqlaccess” in the domain INTERSECT (flat name)

User Search Term: [INTERSECT\sqlaccess]

Example: Match the AD group “sqlaccess” in the child domain ACCOUNTING (DNS name)

User Search Term: [sqlaccess@accounting.intersect.local]

Both user and group related search terms are not case sensitive.

Alert Level

The alert level is used to grade each event before it is sent to the SNARE Server. Alert levels do not change the behavior of either the *SnareMSSQL* Agent or the Snare Server it communicates with. The information is used only as a means for the user to categorize events.

Event Log Retention

SnareMSSQL configures each objective to use a specific amount of disk space as specified by the Total Trace Size (chapter 5.6, Network Configuration on page 20). These files are cycled, discarding the oldest once a new file needs to be created. It is up to the administrator to ensure that the necessary disk space is available for each configured objective.

5.9 Apply the Latest Audit Configuration

Changes to the *SnareMSSQL* configuration do not take effect until the *SnareMSSQL* service is restarted. Restarting the *SnareMSSQL* service is accomplished by browsing to the “Apply the Latest Audit Configuration” menu item within the web interface, and then selecting “Reload Settings”. Alternatively, the service may also be restarted by rebooting the system or by selecting restart service from within Windows¹.

Whilst the *SnareMSSQL* Service is restarting, no events will be collected.

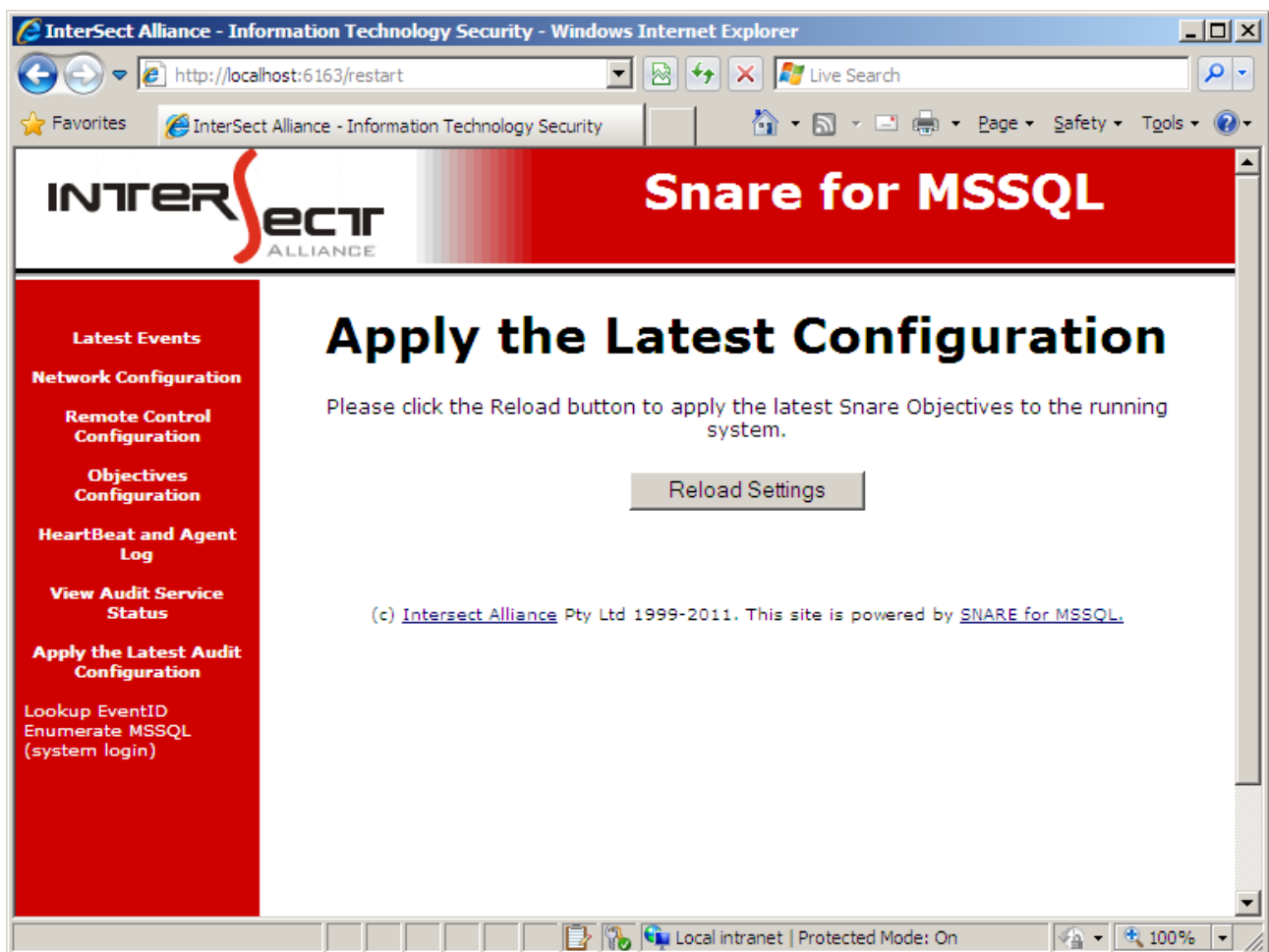


Figure 8: Apply the Latest Audit Configuration

¹ See your Windows documentation for information on how to restart a service

5.10 View Audit Server Status

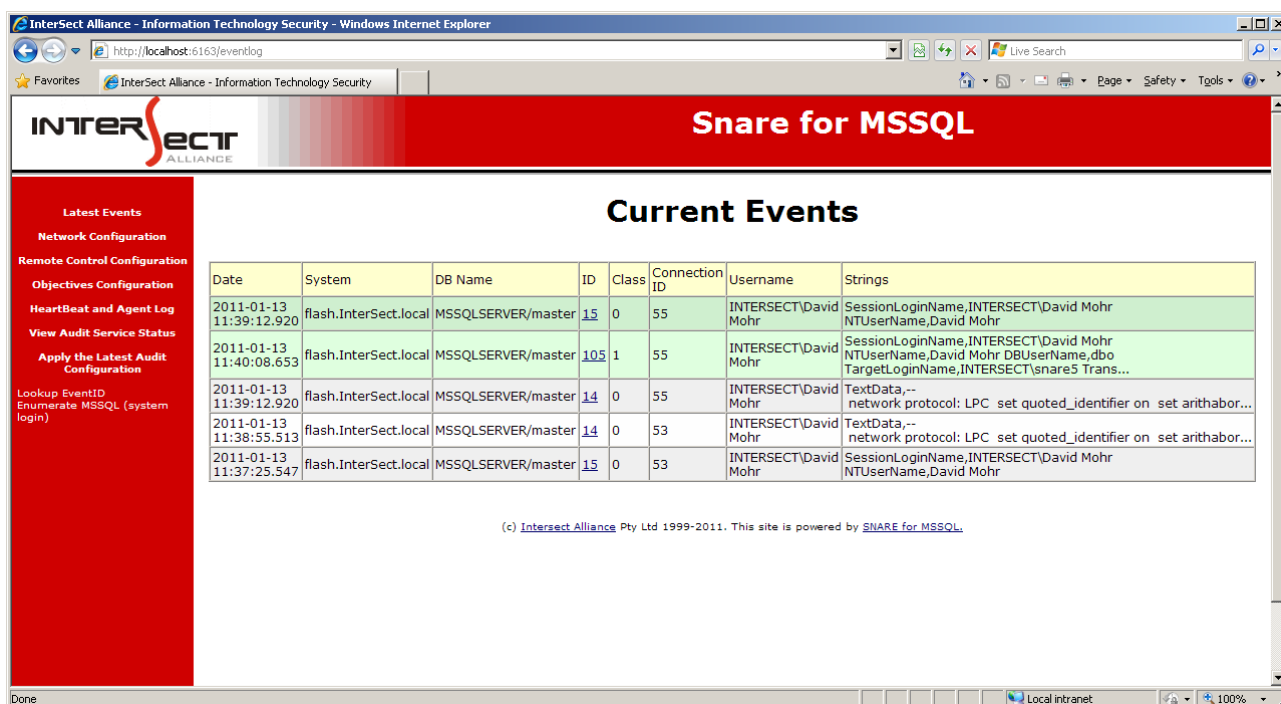
The *SnareMSSQL* service status can be viewed by selecting the “View Audit Server Status” menu item as shown in . This will display whether the *SnareMSSQL* service is active, along with some basic information about the agent.



Figure 9: View Audit Server Status

5.11 Latest Events

The “Latest Events” window contains the events that the *SnareMSSQL* service has received and kept after filtering. This display is NOT a display from the event log file, but rather a temporary display from a **shared memory** connection between the SNARE remote control interface and the *SnareMSSQL* service. The SNARE remote control interface will always begin with a clear event log after each restart. A key feature of the *SnareMSSQL* service is that events do not have to be stored locally on the host (except for a temporary buffer stored by Microsoft SQL Server), but rather sent out over the network to one or more remote hosts.



The screenshot shows a web browser window titled "Intersect Alliance - Information Technology Security - Windows Internet Explorer" with the URL "http://localhost:6163/eventlog". The page header is "INTERSECT ALLIANCE Snare for MSSQL". The main content area is titled "Current Events" and contains a table with the following data:

Date	System	DB Name	ID	Class	Connection ID	Username	Strings
2011-01-13 11:39:12.920	flash.Intersect.local	MSSQLSERVER/master	15	0	55	INTERSECT\David Mohr	SessionLoginName,INTERSECT\David Mohr NTUserName,David Mohr
2011-01-13 11:40:08.653	flash.Intersect.local	MSSQLSERVER/master	105	1	55	INTERSECT\David Mohr	SessionLoginName,INTERSECT\David Mohr NTUserName,David Mohr DBUserName,db TargetLoginName,INTERSECT\snare5 Trans...
2011-01-13 11:39:12.920	flash.Intersect.local	MSSQLSERVER/master	14	0	55	INTERSECT\David Mohr	TextData,-- network protocol: LPC set quoted_identifier on set arithabor...
2011-01-13 11:38:55.513	flash.Intersect.local	MSSQLSERVER/master	14	0	53	INTERSECT\David Mohr	TextData,-- network protocol: LPC set quoted_identifier on set arithabor...
2011-01-13 11:37:25.547	flash.Intersect.local	MSSQLSERVER/master	15	0	53	INTERSECT\David Mohr	SessionLoginName,INTERSECT\David Mohr NTUserName,David Mohr

At the bottom of the page, there is a copyright notice: "(c) Intersect Alliance Pty Ltd 1999-2011. This site is powered by [SNARE for MSSQL](#)."

Figure 10: Viewing Current Events

The “Latest Events” window is restricted to a list of the last 20 entries and cannot be cleared, except by restarting the agent.

The window will automatically refresh every 30 seconds. New entries will be highlighted in green as the page is refreshed.

6 SNARE Server



The SNARE Server collects events and logs from a variety of operating systems, applications and appliances including, but not limited to: Windows NT/2000/XP/2003/Vista/2008/Win7, Solaris, AIX, Irix, Linux, Tru64, ACF2, RACF, CISCO Routers, CISCO PIX Firewall, CyberGuard Firewall, Checkpoint Firewall1, Gauntlet Firewall, Netgear Firewall, IPTables Firewall, Microsoft ISA Server, Microsoft IIS Server, Lotus Notes, Microsoft Proxy Server, Apache, Squid, Snort Network Intrusion Detection Sensors, IBM SOCKS Server, and Generic Syslog Data of any variety.

In addition to the above, the benefits of purchasing the SNARE Server include:

- Official support mechanism for the SNARE open source agents. Note that official SNARE agent support is not offered through *any* other channels.
- All future SNARE Server versions and upgrades included as part of an annual maintenance fee.
- Ability to collect any arbitrary log data, either via UDP or TCP protocols.
- Proven technology that works seamlessly with the SNARE agents.
- SNARE reflector technology that allows for all collected events to be sent, in real time, to a standby/backup SNARE Server.
- Ability to continuously collect large numbers of events. SNARE Server collection rates exceed 60,000 events per minute using a low end, workstation class, Intel based PC on a 100Mbps network.
- Automatic archiving of events to compressed text format after a configurable event time period. This is to prevent the database from slowing down due to storage of old events.
- Ability to drill down from top level reports. This reduces the amount of data “clutter” and allows a system administrator to fine tune the reporting objectives.
- Ability to create “cloned” objectives that allow very specific reporting against any collection profile. These reports, along with all SNARE Server objectives, may be scheduled and emailed to designated staff.
- The SNARE Server uses extensive discriminators for each objective, allowing system administrators to finely tune reporting based on inclusion or exclusion of certain parameters.
- Very simple, single CD installation for those users not requiring a hardware based appliance.

The SNARE Server uses a hardened version of the Linux operating system base for stability and its ability to use a myriad of stable and functional open source tools. A SNARE Server user, however need not be concerned with managing a Linux server. The SNARE Server, once installed, is a fully contained appliance, and does not require any system administrator level maintenance. The SNARE Server will operate on commonly available Intel based PCs, with hardware specifications shown on the next page.

There are supported versions of the SNARE agents which are only available through the purchase of a SNARE Server. Functionality includes, but is not limited to, ability to send events via TCP as well as UDP, and the ability to send events to many destinations, not just one host.

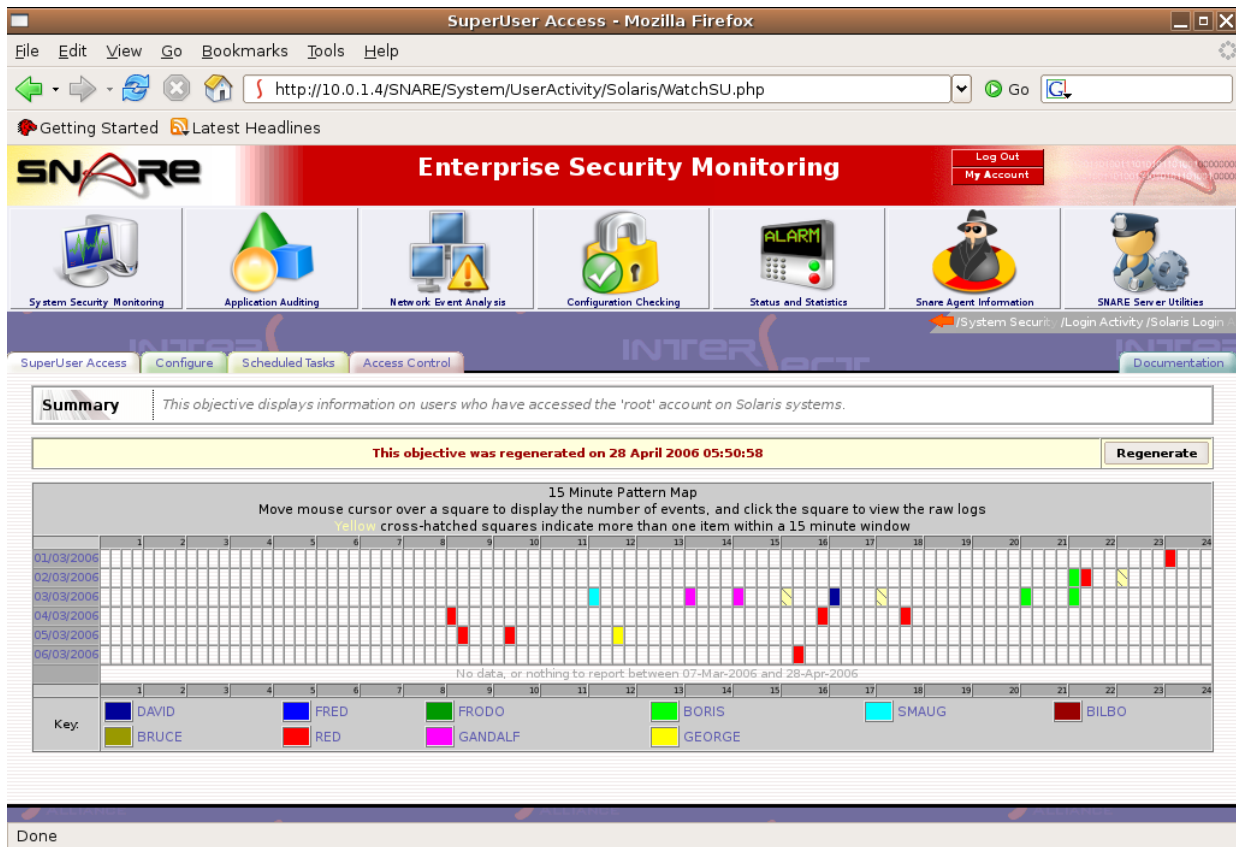


Figure 11: Screen shot from the SNARE Server

7 About Intersect Alliance



Intersect Alliance is a team of leading information technology security specialists. In particular, Intersect Alliance are noted leaders in key aspects of IT Security, including host intrusion detection. Our solutions have and continue to be used in the most sensitive areas of Government and business sectors.

The Intersect Alliance business strategy includes demonstrating our commitment and expertise in IT security by releasing open source products such as SNARE, and the proprietary SNARE Server. Intersect Alliance intend to continue releasing tools that enable users, administrators and clients worldwide to achieve a greater level of productivity and effectiveness in the area of IT Security, by simplifying, abstracting and/or solving complex security problems.

Visit the Intersect Alliance website for more information at www.intersectalliance.com.

Appendix A - Event output format

The *SnareMSSQL* service reads data from the Windows operating system via the Trace Logs. It converts the binary audit data into text format and separates information out into a series of TAB delimited tokens. The token delimiter may not be specified as something other than TAB. A 'token' is simply data, such as 'date' or 'user'. Groups of tab separated tokens make up an audit event, which may look something like this, depending on whether the *SnareMSSQL* service has SYSLOG header functionality active.

Example:

```
flash.InterSect.local  MSSQLLog  2011-01-13 14:56:42.670
09.00.1399 14 0 53  MSSQLSERVER/master  INTERSECT\David
Mohr  TextData,-- network protocol: LPC  set quoted_identifier on
set arithabort off  set numeric_roundabort off  set ansi_warnings on
set ansi_padding on  set ansi_nulls on  set concat_null_yields_null
on  set cursor_close_on_commit off  set implicit_transactions off
set language us_english  set dateformat mdy  set datefirst 7  set
transaction isolation level read committed  NTUserName,David Mohr
```

The format of the event log record is as follows:

1. **Hostname** (as entered using the SNARE front end).
2. **Event Log Type**. 'MssqlLog' for SNARE for Microsoft SQL Server.
3. **Date and Time**. This is the timestamp for when the event was issued.
4. **Version**. The version of MS SQL server being monitored.
5. **Event Class**. This is the Microsoft SQL Server Event ID, indicating what action was taken.
6. **Event Sub Class**. The sub-class provides more specific information about the action undertaken.
7. **SPID**. The Session Process ID.
8. **Instance/Database Name**. The name of the active database when the event was generated.
9. **UserName**. The user that caused the event. This is either a Windows username or a Microsoft SQL Server username
10. **Text**. This is the text verbatim from the trace log event. Newlines and Tabs are replaced with spaces.

Appendix B - SnareMSSQL registry configuration description

Details on the audit configuration are discussed in the **Audit Configuration** section. The purpose of this section is to discuss the makeup of the configuration items in the registry. The SNARE configuration registry key is located at **HKEY_LOCAL_MACHINE\SOFTWARE\Intersect Alliance\SnareMSSQL**, and this location may not be changed. If the configuration key does not exist, the *SnareMSSQL* service will create it during installation, but will not actively audit events until a correctly formatted objective(s) is present.

SNARE can be configured in several different ways, namely:

- Via the remote control interface (Recommended).
- By manually editing the registry (NOT Recommended).

The format of the audit configuration registry subkeys is discussed below.

[Config]	This subkey stores the general agent configuration data.
Delimiter	REG_SZ Stores the field delimiting character, ONLY if syslog header has been selected. If more than one char, only first char will be used. If none set, then TAB will be used. This is a HIDDEN field, and only available to those users that wish to set a different delimiter when using the SYSLOG header. This selection option will not be found in the SNARE front end or the web pages.
Clientname	REG_SZ If no value has been set, "hostname" command output will be displayed. Must be no more than 100 chars, otherwise will truncate.
TracePath	REG_SZ The location where SNARE will store its trace files.
OutputFilePath	REG_SZ The location where SNARE will store a local copy of audit events.
FileExport	REG_DWORD Determines whether event records should be written to <code>OutputFilePath</code> . Set this value to 1 to enable file logging. Will default to FALSE (0) if not set.
FileSize	REG_DWORD The size, in megabytes, of any files written to <code>OutputFilePath</code> .
TraceSize	REG_DWORD The size of any trace files written by MS SQL Server
TraceCount	REG_DWORD The number of trace files maintained by MS SQL Server
LookupTimeout	REG_DWORD The frequency, in minutes, with which the SnareMSSQL agent will recheck the members of any groups specified in the User Search Filter
Heartbeat	REG_DWORD The frequency, in minutes, with which the agent will send out a heartbeat message. A value of zero (0) will disable this feature.
AgentLog	REG_DWORD A flag determining which Agent Logs should be recorded: Service (1), Trace (2) and Debug(4).

[Objective]	This subkey stores all the filtering objectives.
Objective# (where # is an integer number)	Objectives are of type REG_BINARY and contain an <u>encrypted copy</u> of the individual settings comprising an objective. Manual configuration of an objectives is unsupported.
[Network]	This subkey stores the general network configurations.
Destination	REG_SZ A comma separated list of destinations, which should be a maximum of 100 characters each. It details the IP address or hostname which the event records will be sent (NB: multiple hosts only available in supported agent).
DestPort	REG_DWORD The Destination Port number. This value must be in 1-65535 range. Will default to 514 if a SYSLOG header has been specified.
Syslog	REG_DWORD Determines whether a SYSLOG header will be added to the event record. Set this value to 0 for no SYSLOG header. Will default to TRUE (1) if not set.
SyslogDest	REG_DWORD The SYSLOG Class and Criticality. This value will default to 13 if not set, or out of bounds.
SocketType	REG_DWORD Determines the protocol used (0 for UDP, 1 for TCP)
CacheSizeM	REG_DWORD The size, in megabytes, of the cache maintained by the SnareMSSQL agent if communication with the network destination is lost (TCP only).
EncryptMsg	REG_DWORD Determines if outgoing messages should be encrypted.
[Remote]	This subkey stores all the remote control parameters.
Allow	REG_DWORD Determines the availability of the remote control feature. If not set or out of bounds, will default to 0/NO (ie; not able to be remote controlled).
WebPort	REG_DWORD The web server port, if it has been set to something other than port 6161. It is of type REG_DWORD. If not set or out of bounds, it will default to port 6161.
WebPortChange	REG_DWORD Set to either 0 or 1 to signal whether the web port should be changed or not. 0 = no change.
Restrict	REG_DWORD Determines whether the remote users should be restricted via IP address or not. 0 = no restrictions.
RestrictIP	REG_SZ The comma separated list of IP address allowed to access the web interface.
AccessKey	REG_DWORD Determines whether a password is required to access the remote control interface. It is set to either 0 or 1, with 0 signifying no password is required.
AccessKeySet	REG_SZ Stores a hash of the password.

Appendix C - Objectives and security event IDs

The SNARE application has a number of built in Objectives. These Objectives have been designed to 'trap' certain Microsoft SQL Server event IDs, allowing the user to easily create some of the more common objectives without having to know the specific event IDs they require. The terms listed with square brackets can be used in the Event ID Search Term.

The following table lists the individual events belonging to each high level event group¹.

Event ID	Event Name	Event Description
Query Tracking [query]		
40	SQL:StmtStarting	Occurs when the Transact-SQL statement has started.
41	SQL:StmtCompleted	Occurs when the Transact-SQL statement has completed.
Login/Logout [loginout]		
14	Audit Login	Occurs when a user successfully logs in to SQL Server.
15	Audit Logout	Occurs when a user logs out of SQL Server.
20	Audit Login Failed	Indicates that a login attempt to SQL Server from a client failed.
Transaction Tracking [transaction]		
50	SQL Transaction	Tracks Transact-SQL BEGIN, COMMIT, SAVE, and ROLLBACK TRANSACTION statements.
181	TM: Begin Tran starting	Occurs when a BEGIN TRANSACTION request starts.
182	TM: Begin Tran completed	Occurs when a BEGIN TRANSACTION request completes.
183	TM: Promote Tran starting	Occurs when a PROMOTE TRANSACTION request starts.
184	TM: Promote Tran completed	Occurs when a PROMOTE TRANSACTION request completes.
185	TM: Commit Tran starting	Occurs when a COMMIT TRANSACTION request starts.
186	TM: Commit Tran completed	Occurs when a COMMIT TRANSACTION request completes.
187	TM: Rollback Tran starting	Occurs when a ROLLBACK TRANSACTION request starts.
188	TM: Rollback Tran completed	Occurs when a ROLLBACK TRANSACTION request completes.
191	TM: Save Tran starting	Occurs when a SAVE TRANSACTION request starts.
192	TM: Save Tran completed	Occurs when a SAVE TRANSACTION request completes.

¹ More information on these events can be found at <http://msdn2.microsoft.com/en-us/library/ms186265.aspx>

Use of User Rights - Privileges [user-rights-use-priv]		
132	Audit Server Principal Impersonation Event	Occurs when there is an impersonation within server scope, such as EXECUTE AS LOGIN.
133	Audit Database Principal Impersonation Event	Occurs when an impersonation occurs within the database scope, such as EXECUTE AS USER or SETUSER.
170	Audit Server Scope GDR Event	Indicates that a grant, deny, or revoke event for permissions in server scope occurred, such as creating a login.
171	Audit Server Object GDR Event	Indicates that a grant, deny, or revoke event for a schema object, such as a table or function, occurred.
172	Audit Database Object GDR Event	Indicates that a grant, deny, or revoke event for database objects, such as assemblies and schemas, occurred.
112	Audit App Role Change Password Event	Occurs when a password of an application role is changed.
102	Audit Statement GDR Event	Occurs every time a GRANT, DENY, REVOKE for a statement permission is issued by any user in SQL Server.
103	Audit Object GDR Event	Occurs every time a GRANT, DENY, REVOKE for an object permission is issued by any user in SQL Server.
Use of User Rights Data Manipulation Language (DML) [user-rights-use-dml]		
114	Audit Schema Object Access Event	Occurs when an object permission (e.g. INSERT or UPDATE) is used, successfully or unsuccessfully.
Use of User Rights - Data Manipulation Language (DML) including SELECT		
114	Audit Schema Object Access Event	Occurs when an object permission (SELECT) is used, successfully or unsuccessfully.
Use of User Rights- Data Definition Language [user-rights-use-ddl]		
113	Audit Statement Permission Event	Occurs when a statement permission (such as CREATE TABLE) is used.
118	Audit Object Derived Permission Event	Occurs when a CREATE, ALTER, and DROP object commands are issued.
Account Admin [account-admin]		
104	Audit AddLogin Event	Occurs when a SQL Server login is added or removed
105	Audit Login GDR Event	Occurs when a Windows login right is added or removed
106	Audit Login Change Property Event	Occurs when a property of a login, except passwords, is modified
107	Audit Login Change Password Event	Occurs when a SQL Server login password is changed. Passwords are not recorded.
108	Audit Add Login to Server Role Event	Occurs when a login is added or removed from a fixed server role

109	Audit Add DB User Event	Occurs when a login is added or removed as a database user (Windows or SQL Server) to a database
110	Audit Add Member to DB Role Event	Occurs when a login is added or removed as a database user (fixed or user-defined) to a database
111	Audit Add Role Event	Occurs when a login is added or removed as a database user to a database
Object Access [object-access]		
128	Audit Database Management Event	Occurs when a database is created, altered, or dropped.
129	Audit Database Object Management Event	Occurs when a CREATE, ALTER, or DROP statement executes on database objects, such as schemas.
130	Audit Database Principal Management Event	Occurs when principals, such as users, are created, altered, or dropped from a database.
131	Audit Schema Object Management Event	Occurs when server objects are created, altered, or dropped.
134	Audit Server Object Take Ownership Event	Occurs when the owner is changed for objects in server scope.
135	Audit Database Object Take Ownership Event	Occurs when a change of owner for objects within database scope occurs.
152	Audit Change Database Owner	Occurs when ALTER AUTHORIZATION is used to change the owner of a database and permissions are checked to do that.
153	Audit Schema Object Take Ownership Event	Occurs when ALTER AUTHORIZATION is used to assign an owner to an object and permissions are checked to do that.
164	Object:Altered	Occurs when a database object is altered.
173	Audit Server Operation Event	Occurs when Security Audit operations such as altering settings, resources, external access, or authorization are used.
175	Audit Server Alter Trace Event	Occurs when a statement checks for the ALTER TRACE permission.
176	Audit Server Object Management Event	Occurs when server objects are created, altered, or dropped.
177	Audit Server Principal Management Event	Occurs when server principals are created, altered, or dropped.
178	Audit Database Operation Event	Occurs when database operations occur, such as checkpoint or subscribe query notification.
180	Audit Database Object Access Event	Occurs when database objects, such as schemas, are accessed.

A comprehensive list of events generated by Microsoft SQL Server can be found on the Microsoft Developer Network at <http://msdn2.microsoft.com/en-us/library/ms186265.aspx>