SNARE

System iNtrusion Analysis & Reporting Environment

User Guide to
Snare Enterprise Agent for MSSQL
v1.2, 1.3, 1.4

INTERSECT ALLIANCE

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 Enterprise Agent for MSSQL' will now allow for events generated by Microsoft SQL Server to be forwarded to a remote audit event collection facility. Snare Enterprise Agent 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

The team at Intersect Alliance have developed auditing and intrusion detection solutions on a wide range of platforms, systems and network devices including Windows, Linux, Solaris, AIX, IRIX, PIX, Checkpoint, IIS, Apache, MVS (ACF2/RACF), and many more. We have in-depth experience within National Security and Defence Agencies, Financial Service firms, Public Sector Departments and Service Providers. This background gives us a unique insight into how to effectively deploy host and network intrusion detection and security validation systems that support and enhance an organisation's business goals and security risk profile.

Native intrusion detection and logging subsystems are often a blunt instrument at best, and when your security team strives to meet departmental, organisational, industry or even national security logging requirements, a massive volume of data can be generated. Only some of this data is useful in evaluating your current security stance. Intersect Alliance has written software 'agents' for a wide range of systems that are capable of enhancing the native auditing and logging capabilities to provide advanced log filtering, fast remote delivery using secure channels, remote control of agents from a central collection server, and a consistent web based user interface across heterogeneous environments.

Through hard-won experience collecting log data in enterprises worldwide, Snare's capabilities have evolved over many years to provide an unmatched cohesive approach to event log management in a trusted package, that is promoted as an industry standard solution for log collection and distribution by a wide range of event management applications (SIEMs, SEMs, SIMs and LMs) and Service providers (MSSPs). The agents have an enterprise-level feature set, yet are designed to be light on disk space, memory and CPU to ensure that your servers can meet security requirements without compromising their ability to stick to core business.

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 Enterprise Agent for MSSQL will also allow a security administrator to fully remote control and monitor the application through a standard web browser.

Other Snare agents are also available for Windows (2003/XP/Vista/2008/Windows7/Windows8/2012), Linux, Solaris, Epilog and many more.

Agents are available for Windows (2003/XP/Vista/2008/Windows7/Windows8/2012), Linux, Solaris, Epilog and many more. The agents are capable of sending data to a wide variety of target collection systems, including our very own **'Snare Server'**. See *Chapter 6 SNARE Server* for further details.

Welcome to **'Snare'** - **System iNtrusion Analysis & Reporting Environment**.

2 Overview of SNARE for MS SQL Server

Snare Enterprise Agent for MSSQL operates through the actions of the *SnareMSSQL.exe* service. This 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 Enterprise Agent for MSSQL can also be used to monitor SQL instances running on a failover cluster. See *Chapter 3-Agent Installation* and *Chapter 5.3-Objectives Configuration* for more information on configuring objectives.

The ***SnareMSSQL*** service is controlled and monitored using a standard web browser. This web interface can be used either locally or remotely to control the operation of the ***SnareMSSQL*** Agent. See *Chapter 5-The Remote Control Interface* for more information on gaining access to the ***SnareMSSQL*** web interface.

Figure 1: The SnareMSSQL Web Interface

3 Agent Installation

Snare Enterprise Agent for MSSQL 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 core component SnareMSSQL.exe.

The SnareMSSQL.exe 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 2003/2008/2008R2/2012 or XP/Vista/Win7.

Snare Enterprise Agent for MSSQL has two distinct deployment scenarios:

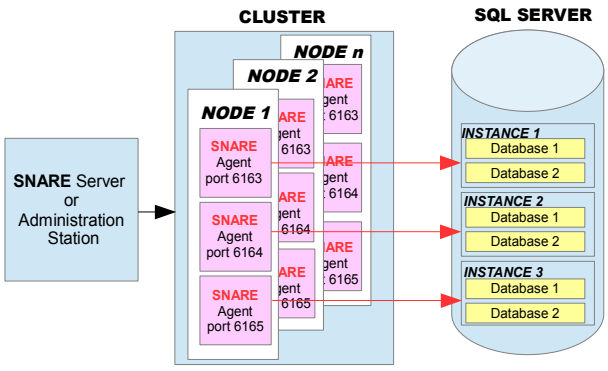
- **Stand alone scenario**

  This scenario involves a single system running one or more instances of MS SQL Server. The 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 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 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. Each agent will be installed with its own unique administration port-number starting with 6163 and progressing to 6164,6165 etc. Each agent that is tied to a clustered SQL instance will follow that instance as part of a automatic failover or a manual migration. If you have standalone



  instances on the same server then the web management port will be the last port in the sequence from the install.

- **High availability and standalone instances on clusters**

Microsoft introduced some new variations of clusters called High Availability instances that can run on Microsoft Clusters. For all intensive purposes these operate like a standalone machine and you will have one Snare MSSQL Agent per machine for these types of instances. The Snare MSSQL agent was updated as of 1.4.1 to support these additional configurations.

If at any point you install additional SQL clustered instances on the cluster you will need to perform a re installation of the Snare MSSQL agent to ensure that all instances are covered correctly and that each agent has the correct web management port assigned.

3.1 Prerequisites

The ***SnareMSSQL*** Agent has the following requirements:

- For stand alone instances,
  - Windows 2000/2003/XP/Vista/2008/Win7/2008R2/2012, 32 or 64 bit architecture
  - Microsoft SQL Server 2000,2005,2008,2012 and 2014 are supported, 32 or 64 bit architecture
- For clustered instances,
  - Windows Server 2003/2008/2008R2/2012, 32 or 64 bit architecture arranged in a failover cluster
  - Microsoft SQL Server 2005, 2008, 2012 and 2014 , 32 or 64 bit architecture in either a single or multiple instance deployment, including clustered and stand alone instances.
- The drive where Snare for MSSQL Agent is installed requires a minimum of 10MB of free space. Additional free space is required to operate the agent and collect trace files. See *Total Trace Size* for more information on objective space requirements.

3.2 Wizard Install

Download the SnareEnterpriseAgent-MSSQL-v{Version}-SUPP-MultiArch.exe.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 SnareEnterpriseAgent-MSSQL-v{Version}-SUPP-MultiArch.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:

3.2.1 Welcome to the SnareMSSQL Setup Wizard

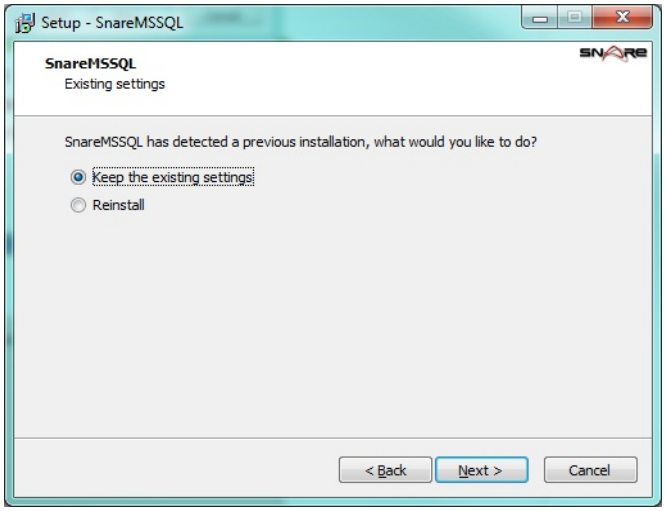
This screen provides a brief overview of the product you are about to install.

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

3.2.2 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.

3.2.3 Existing Install (Upgrade only)

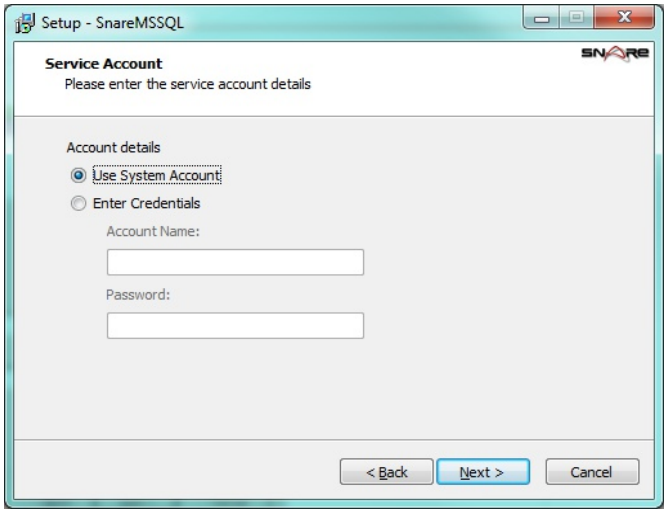


If the Wizard detects a previous install of the SnareMSSQL agent, you will be asked how to proceed.

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.

3.2.4 Service Account

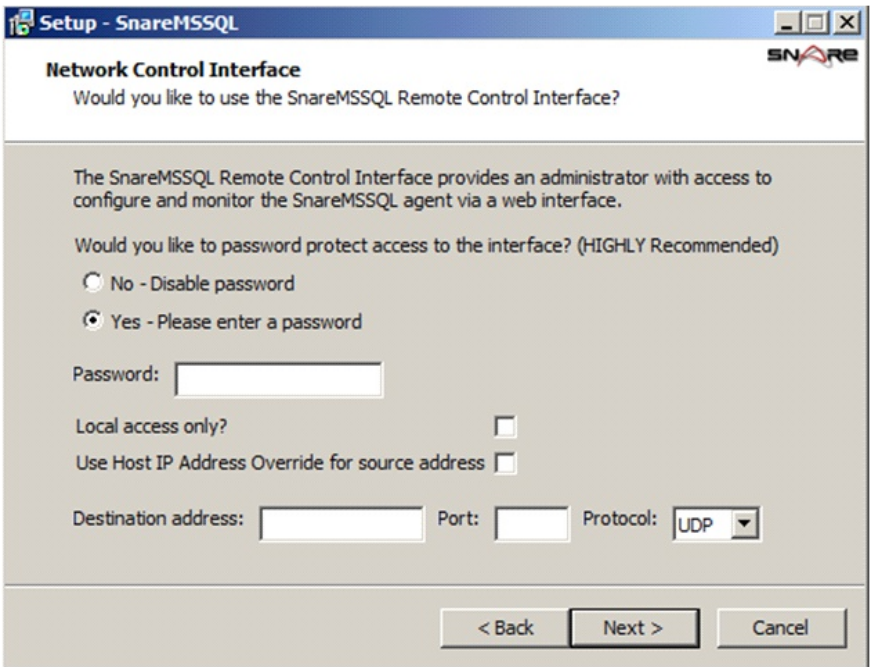


Snare Enterprise Agent for MSSQL requires a service account to operate. It uses this account for two main purposes:

- **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 and the SYSADMIN role in MSSQL Server (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.
    - **Failover cluster scenario**. Using database credentials in the GUI may pose a security risk in a clustered environment as the hash of the credentials will traverse the local network when the configuration synchronizes over the LAN. If this is a concern we recommend that only the service account credentials are used. For comparability the option is available to use database credentials. For some clustered environments operating on Windows 2012 and MSSQL 2012 or 2014 you may have to specify a separate service account other then the built in SYSTEM account as it may not have enough privileges to operate. This service account will need to have the relevant local administrative privileges and be granted the SYSADMIN role in MSSQL server to operate.

For more information, see *Chapter 5.3.2-Creating an Objective*.

3.2.5 Remote Control Interface



This screen provides a means to configure the 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. We strongly recommend that this option is not used on production systems as it will leave the agent vulnerable to unauthorised access.

- "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. It is recommended that you use a strong complex password and it complies with your corporate policies.

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 system owner of the SnareMSSQL resource.

From version 1.4.0 the following fields are available:

- **Use Host IP Address Override for source address**

  Enabling this setting will use the first network adapter as listed in the network configuration as the source of the IP address.

- **Destination address**

  The name or IP address can be entered and comma delimited when several addresses are required.

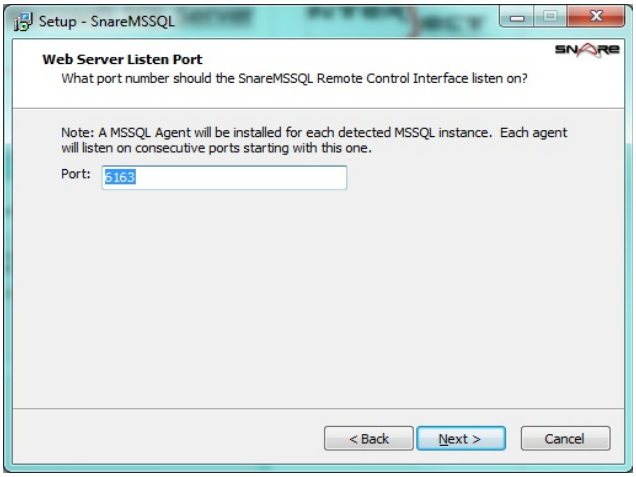
- **Port**

  Configure the port, for example Snare Server users should only send events to port 6161 in native UDP or TCP, or 6163 for TLS/SSL, and Syslog via port 514.

- **Protocol**

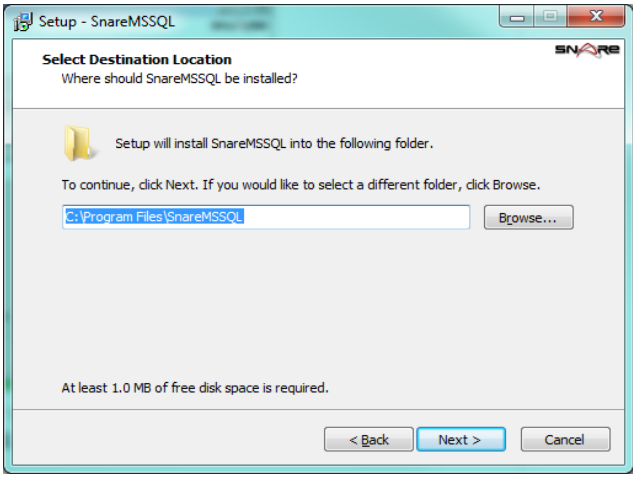
  Select the protocol (UDP,TCP,TLS) you would like the agent to use when sending events.

3.2.6 Select Web Server Listen Port



This specifies the IP port the agent listens on to provide a configuration GUI. If multiple SQL instances exist on a clustered system, multiple agents will be installed listening on ports sequentially incrementing from this port. The default for the MSSQL Agent is 6163.

3.2.7 Select Destination Location

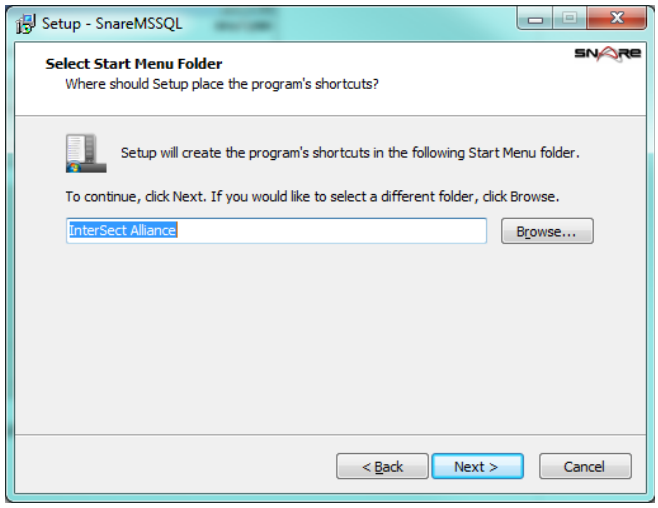


This screen provides a means to select the folder where the Agent will be installed. If the folder name specified does not exist, it will be created. In a failover cluster scenario, this location will be created on all available nodes.

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 5.2*). It is recommended that this location be able to handle the disk IO associated with collecting the trace files. Refer to *Total Trace Size* for more information on space requirements for trace files.

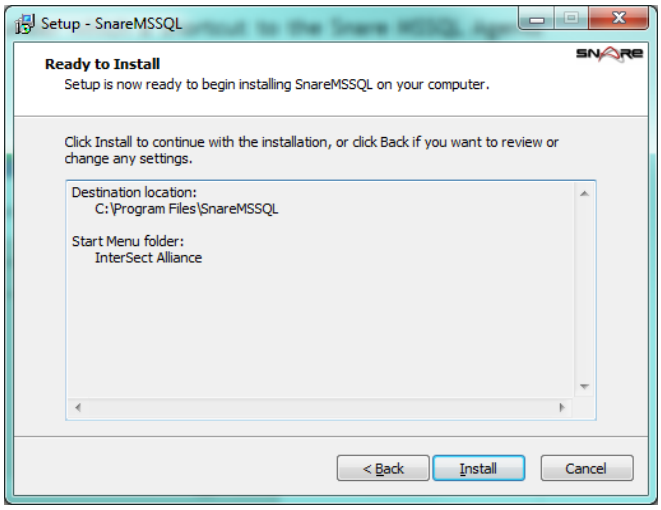
By default, the installation wizard will install the directory 'SnareMSSQL' under the *Program Files* folder. If a different destination is desired, select the "Browse" button, or directly enter the full path name.

3.2.8 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.

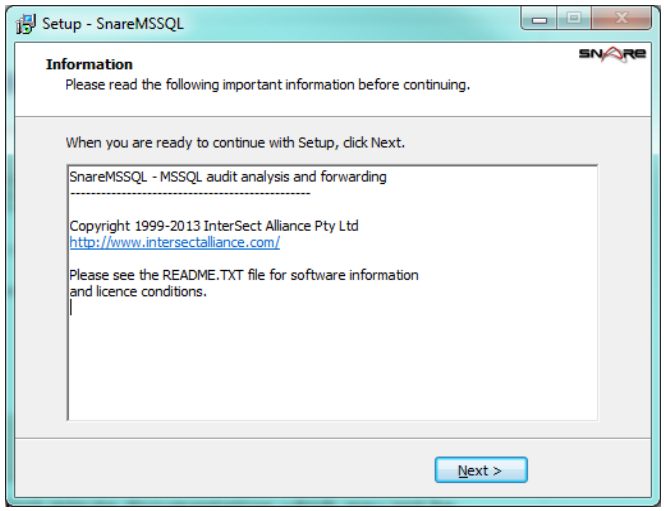
3.2.9 Ready to Install



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.

3.2.10 Information



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

3.2.11 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 Snare Enterprise Agent for MSSQL.

3.3.1 Command line options

The Snare Enterprise Agent for MSSQL 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 Snare Enterprise Agent for MSSQL 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.

  The following options are available from version 1.4.0:

- **/UseHostIP** – To enable the address resolution feature, to use the host IP address. Value 0 for off, and 1 to allow.
- **/Destination**– Set the IP address or hostname which the event records are sent.
- **/DestPort** – Set the destination port for e.g Snare, syslog.
- **/Protocol** –Set the protocol you would like the agent to use when sending events. Values 0 (UDP),1(TCP),2 (TLS/SSL).
- **/RemoteLocal** - To allow remote connections to the agent from localhost only. Value 0 for off, and 1 to allow. Ensure /RemoteAllow and /AccessKey are also set with this option.
- **/RemoteAllow** – To enable the remote access of the agent. Value 0 for off, and 1 to allow.
- **/Audit** – Set whether Snare is to automatically set the system audit configuration. Set this value to 0 for no or 1 for Yes (default).

- **/AccessKey** - Set the password for the remote access of the agent.

3.3.2 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 Snare Enterprise Agent for MSSQL using the Wizard.
2. Using the web interface configure the agent's Network, Remote Control and Heartbeat settings.
3. Configure one or more objectives 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 INFILE where <*INFfile*> is any file name for output, 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*.

3.3.3 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:

SnareEnterpriseAgent-MSSQL-v{Version}-SUPP-MultiArch.exe /verysilent /suppressmsgboxes /LoadInf="Settings.INF"

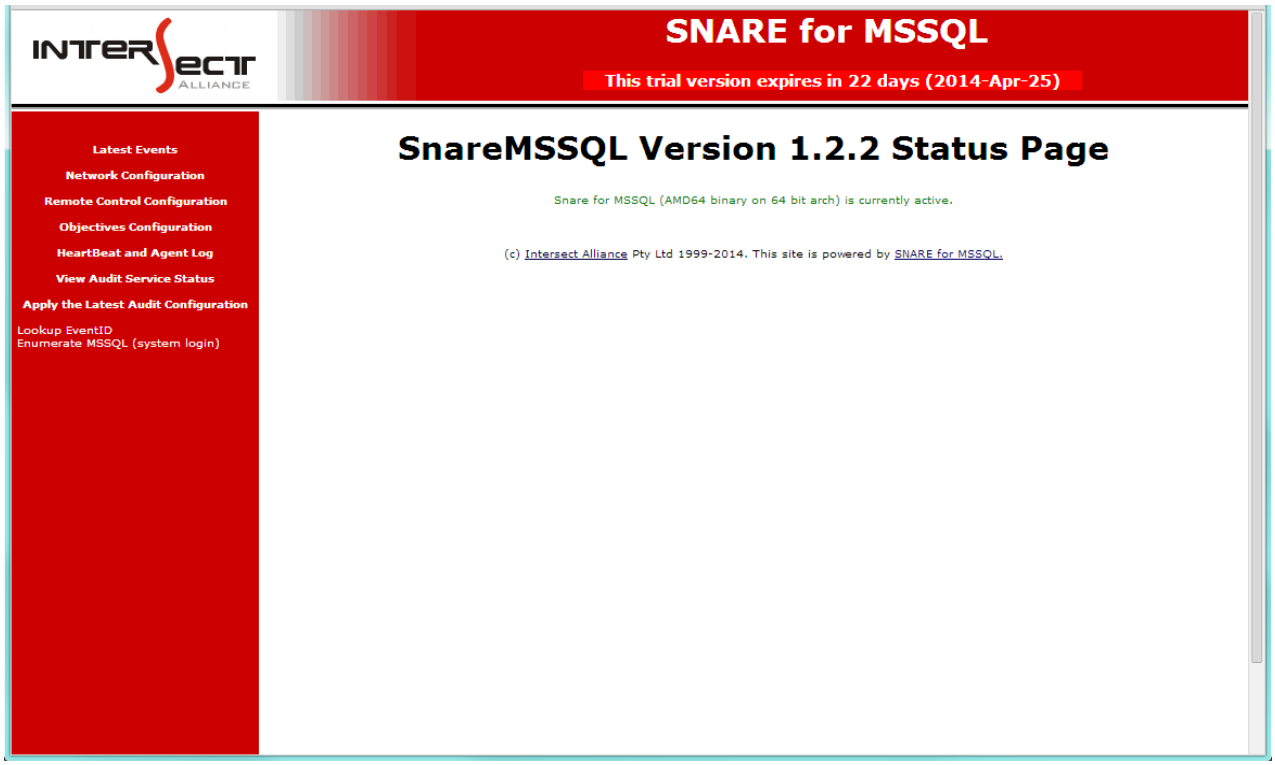
This will install the ***SnareMSSQL*** application with the options specified in the Settings.INF file and will not display any pop-up windows. This option is suitable for packaging and non-interactive installations. For deployment in a failover cluster scenario, this command only needs to be run on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

To install the agent setting the network configuration:

SnareEnterpriseAgent-MSSQL-v{Version}-SUPP-MultiArch.exe /usehostip=1 /destination=10.1.1.1 /destport=514 /protocol=0 /reinstall /verysilent /remoteallow=1 /audit=0

3.4 Evaluation Version

Intersect Alliance offers a trial version of the agents providing full functionality for a limited time for evaluation purposes. *If this evaluaton agent version is installed*, the following will be included in the header of each screen:



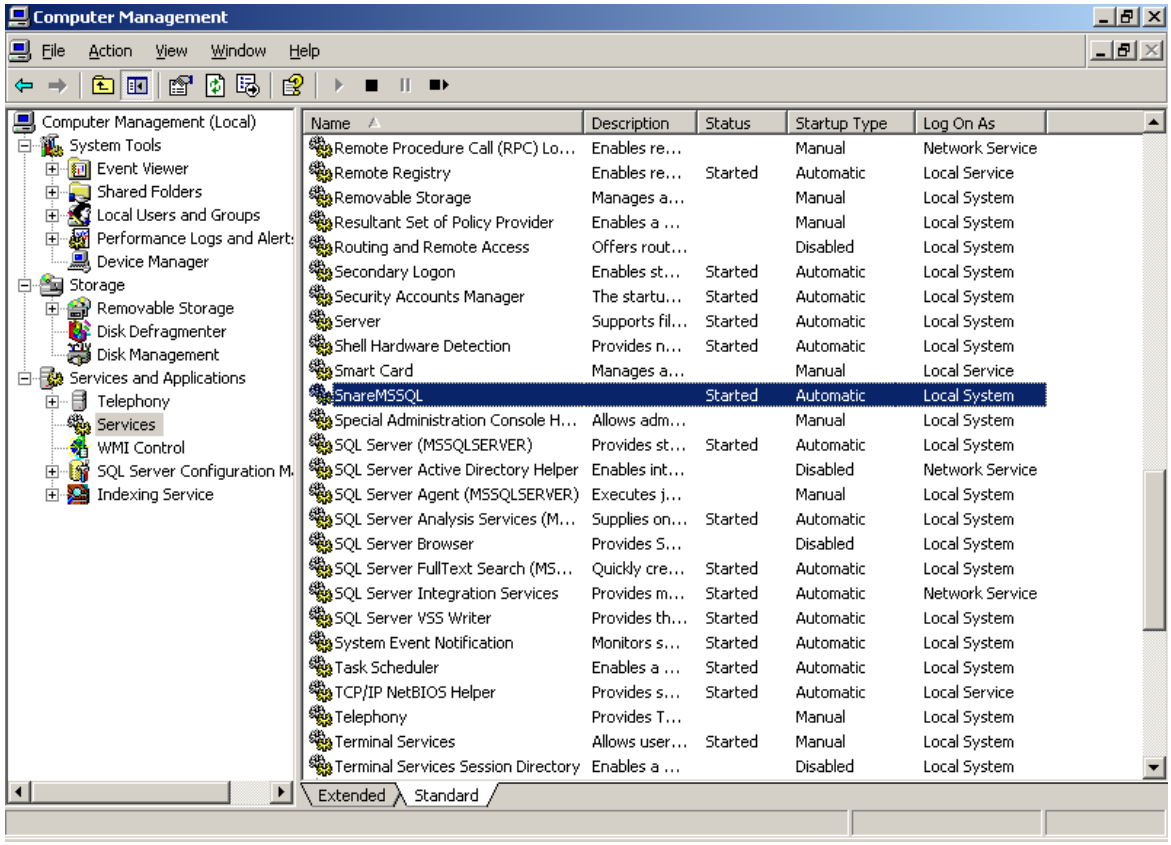
This indicates on what date, and the number of days the agent will cease to log to a server. When this date is passed, the following will be displayed:

This trial version expired on 2014-Apr-24. No further events will be logged to the server.

The **Latest Events** page will continue to update with current events, however no further events will be transmitted to the server. This can only be rectified by purchasing the Snare Enterprise Agent for MSSQL via your Snare representative, and upgrading your agent to ensure your settings and objectives are not lost.

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* 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, for example *SnareMSSQL$NamedInst*.

Once the ***SnareMSSQL*** Service is running, its status can be viewed via the remote control web interface.

5 The Remote Control Interface

The Remote Control Interface is accessible via a web browser from the local machine by entering http://localhost:6163/[1] or http://{computer-name}:{port-number}/, where 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. For example,

- Contact the machine "**SQLSERVER**" on port **6163**:

  http://SQLSERVER:6163/

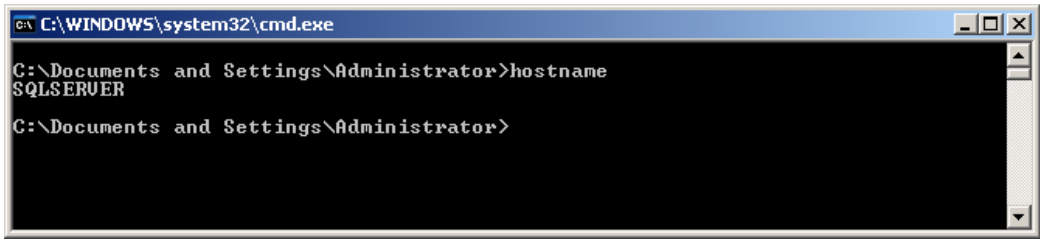
- Contact the machine "**10.5.33.183**" on port **6163**:

  http://10.5.33.183:6163/

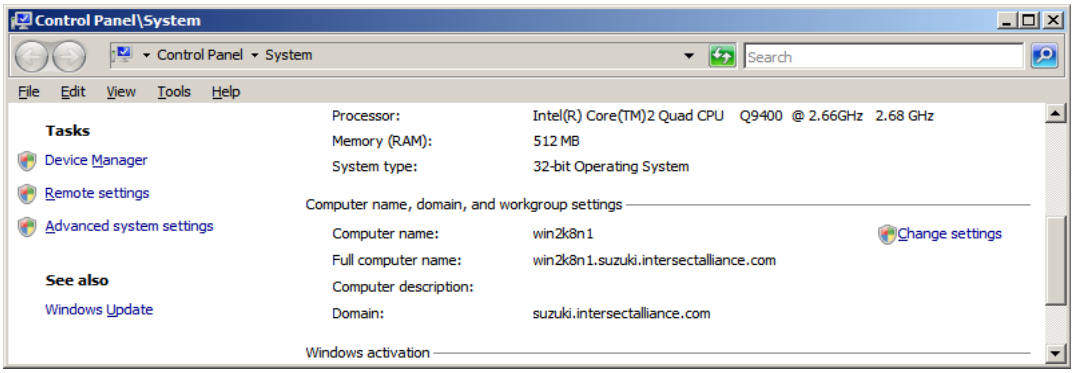
The Remote Control Interface is turned on by default. If you previously configured a password, you will need this to log in, along with the username **snare**.

5.0.1 Determine computer name

To determine the name of a computer, open a command prompt and type the command "hostname":

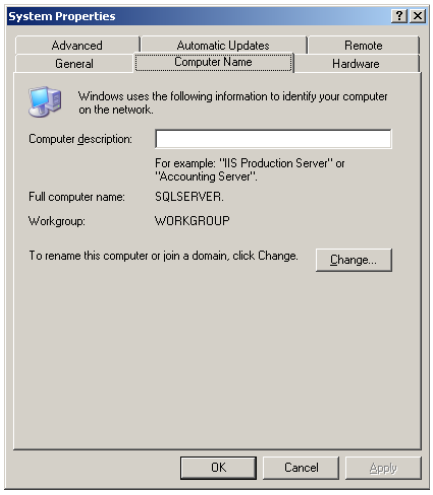


Alternatively, to determine the name of a computer in a stand alone deployment scenario, browse to **Control Panel->System** and find the text after the label "Computer name":



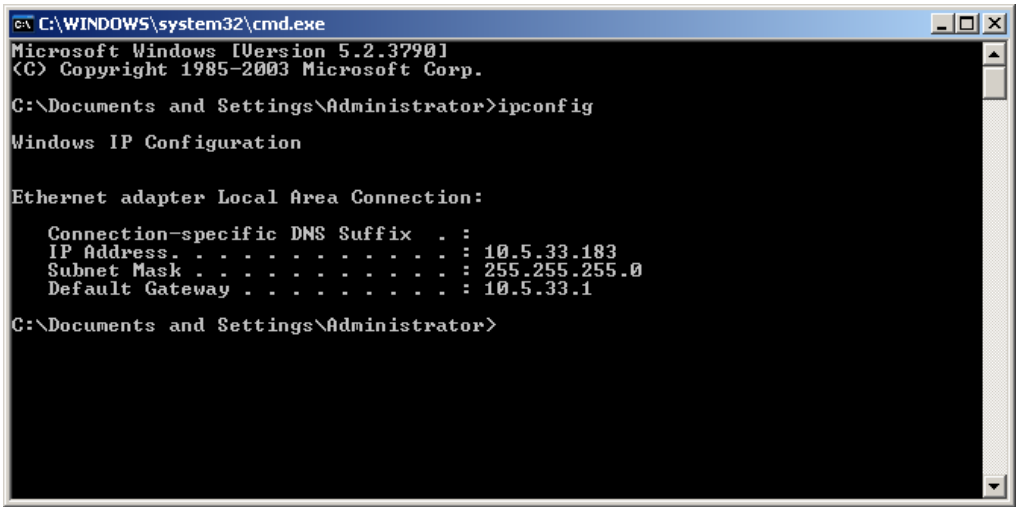
1 6163 is the default port for the ***SnareMSSQL*** web interface. If a different port has been chosen, please replace this with the chosen number.

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



5.0.2 Determine IP address

Open a command prompt and type **ipconfig** and get the text after the label **IP Address**.



5.1 Remote Control Configuration

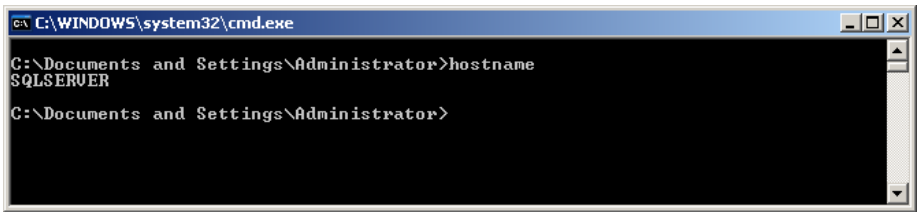
A critical function of the ***SnareMSSQL*** service is its ability to be remote controlled. The ***SnareMSSQL*** service employs a custom designed web server to allow configuration through a browser. The parameters which may be set for remote control operation are shown in Figure 2 and discussed in detail below:

Figure 2: Remote Control Configuration

- ***Restrict remote control of SNARE agent to certain hosts:*** Use this setting to restrict access to the ***SnareMSSQL w***eb 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 spoofing[1]. It is advisable that this security measure be used in conjunction with other countermeasures.

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.

- From version 1.4.0, the following setting is available, ***Use Host IP Address Override for source address***. Enabling this setting will use the first network adapator as listed in the network configuration as the source of the IP address. The agent will periodically (about ten minutes) check this setting and pick up any changes that occur via a manual change of IP or DHCP reassignment. The value of the IP address will be displayed in ***Override detected DNS Name with*** once selected. If the host does not have a valid IP address, i.e. DHCP has not been responded to, then the syslog message will default to the system's hostname which is the default setting for the agent.
- ***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. It is recommended for security purposes that if you allow network connectivity then you restrict this to designated management systems.
- ***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. It is recommended that a strong complex password is always used to avoid unauthorised access to the Snare SQL configuration.
- ***Change Web Server default (6163) port:*** The default ***SnareMSSQL*** web server port (6163) and 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.



For clustered environments each Snare SQL Agent instance will install using a default sequential port number starting from 6163 and continue based on the number of instances installed. Ie 6163, 6164, 6165 etc. As mentioned above these are configurable and can be changed to another unique port-number if required.

- ***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. 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 include the specific web port-number ie http://mysite.com:6163 to reach the web server.

To save and set changes to these settings, and to ensure the audit daemon has received the new configuration perform the following:

1. Click on **Change Configuration** to save any changes.
2. Click on the **Apply the Latest Audit Configuration** menu item and select **Reload Settings**.

Alternatively, the service may also be restarted by rebooting the system or by selecting restart service from within Windows. Whilst the SnareMSSQL Service is restarting, no events will be collected.

5.2 Network Configuration

The Network Configuration page as shown below is used to specify how and where Snare will output its event logs. The audit configuration parameters available are as follows:

- ***Path to write trace files:*** 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. For Microsoft Windows Server 2012/2012R2 (with SQL Server 2012 or 2014) installs and some Windows server 2008R2 installs the group policy controls on the c:\Program Files\SnareMSSQL location may cause problems with writing the trace files due to inherited disk permissions from the c:\Program Files location. To address this adjust the setting to use another disk path that is writable by the agent, for example C:\SnareTrace. For some high activity systems this location may add additional disk busy utilization. If this is excessive then move this location to an appropriate raided location.
- ***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. ***SnareMSQL*** configures each objective to use a specific amount of disk space as specified by this setting. 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.
- ***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.
- ***Destination Snare Server address(s):*** 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. If your server is syslog based then change this port to 514 along with the UDP protocol. For non Snare Servers that require TCP connectivity then use a different port other than 6161 along with the TCP protocol setting.

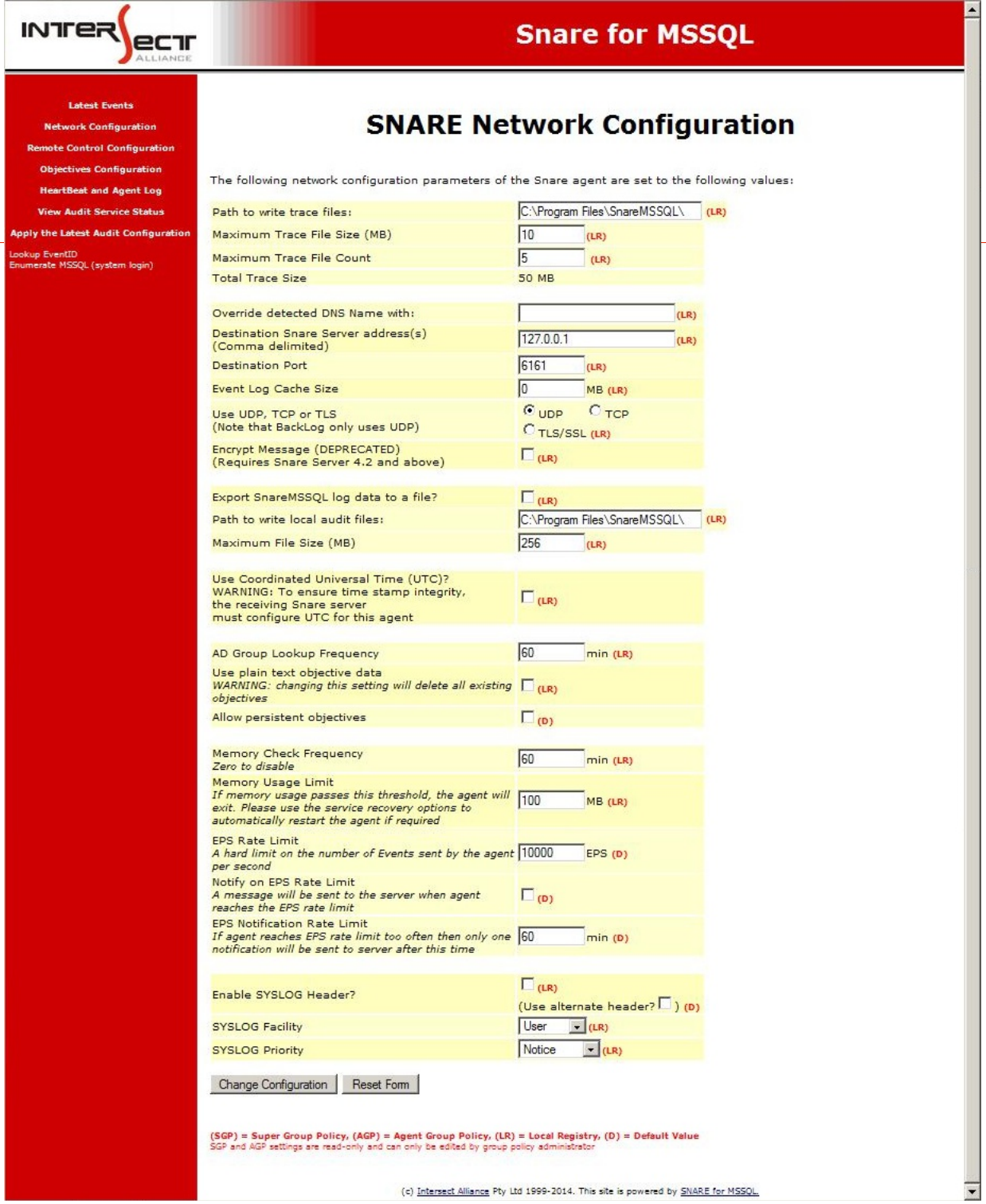


Figure 4: Network Configuration page

- ***Event Log Cache Size:*** 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 network connections.
- ***Use UDP,TCP or TLS:*** Select the protocol you would like the agent to use when sending events. UDP by the protocol nature may result in messages being lost and not captured by the syslog destination server. TCP will provide reliable message delivery 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. TLS/SSL will encrypt a TCP connection to the destination server, protecting messages from eavesdropping while in transit.
- ***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. ***WARNING: Please note this log file will be induce a large amount of local disk IO on busy SQL Server installations. Only use if necessary or the performance impacts are understood.***
- ***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.
- ***Use Coordinated Universal Time (UTC)?:*** Enables UTC timestamp format for events instead of local machine time zone format.
- ***AD Group Lookup Frequency:*** Objectives allow the use of Active Directory group identifiers in the User Search Term (see section *User Search Term*). This setting defines the frequency, in minutes, that the agent will recheck the members of any groups identified.
- ***Use plain text objective data:*** By default all MSSQL objectives are stored in encrypted form. If this option is selected then objectives are stored as plain text in the registry settings and all existing (encrypted) objectives will be deleted and all new objectives will be stored as plain text. This option is not recommended because it less secure. However these plain text objectives can be used to copy/paste in administrative objectives and GPO.
- ***Allow persistent objectives:*** Persistent objectives are system specific objectives that are not exported during the silent installation wizard (-x option). If this option is checked then whenever a new objective is created within Objectives Configuration a parameter called ***'Make the objective Persistent'*** is available. If ***'Make the objective Persistent'*** check box is selected then the newly created objective will be stored separately in the registry under 'PersistentObj' registry key and all the objectives under 'PresistentObj' are NOT exported using silent installlation wizard. Persistent objective is an option to create system specific objectives and decreasing the load during silent installation. NOTE: the objectives are not deleted from the registry by selecting the '***Allow persistent objectives'*** during an uninstall.

- ***Memory Check Frequency:*** The number of minutes set when the memory usage limit of the MSSQL agent will be checked.
- ***Memory Usage Limit:*** This is the maximum memory the MSSQL agent can utilize during any stage of execution. If memory usage of MSSQL agent passes this threshold then agent will exit once it checks the memory usage as per 'Memory Check Frequency' setting. Please use the service recovery options (Services->Right Click on SnareMSSQL->Properties->Recover tab) to automatically restart the agent if required. This option makes sure that agent does not utilize unrestricted memory.
- ***EPS Rate Limit:*** This is a hard limit on the number of Events sent by the agent per second to any destination server. This EPS rate limit applies only to sending the events NOT capturing the events. The EPS rate limit is to help to reduce the load on slow network links or to reduce the impact on the destination SIEM servers during unexpected high event rates.
- ***Notify on EPS Rate Limit:*** If this option is selected then a message will be sent to the server when agent reaches the EPS rate limit. The message also include the EPS rate limit value.
- ***EPS Notification Rate Limit:*** This is the time (in minutes), during that if agent reaches the EPS limit multiple times then only one EPS rate limit message will be sent to the server. This setting only works if 'Notify on EPS Rate Limit' is checked.
- ***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:*** This option allows the agent to tag messages with an appropriate SYSLOG facility level. Discussion of the "SYSLOG Facility" option is beyond the scope of this document. Consult your SYSLOG man page on your Unix server or other SYSLOG server documentation for further information on this field.
- ***SYSLOG Priority:*** This option allows the agent to tag messages with an appropriate SYSLOG priority level. Discussion of the "SYSLOG Priority" option is beyond the scope of this document. Consult your SYSLOG man page on your Unix Server or your SYSLOG server documentation for further information on this field. 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.

To save and set changes to these settings, and to ensure the audit daemon has received the new configuration perform the following:

1. Click on **Change Configuration** to save any changes.
2. Click on the **Apply the Latest Audit Configuration** menu item and select **Reload Settings**.

Alternatively, the service may also be restarted by rebooting the system or by selecting restart service from within Windows. Whilst the SnareMSSQL Service is restarting, no events will be collected.

5.3 Objectives Configuration

The primary function of the Snare Enterprise Agent for MSSQL 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.

5.3.1 Objectives List

Once an objective is configured, the "Objectives Configuration" window will display a list of configured objectives as shown in Figure 3: Objectives Configuration List. 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.

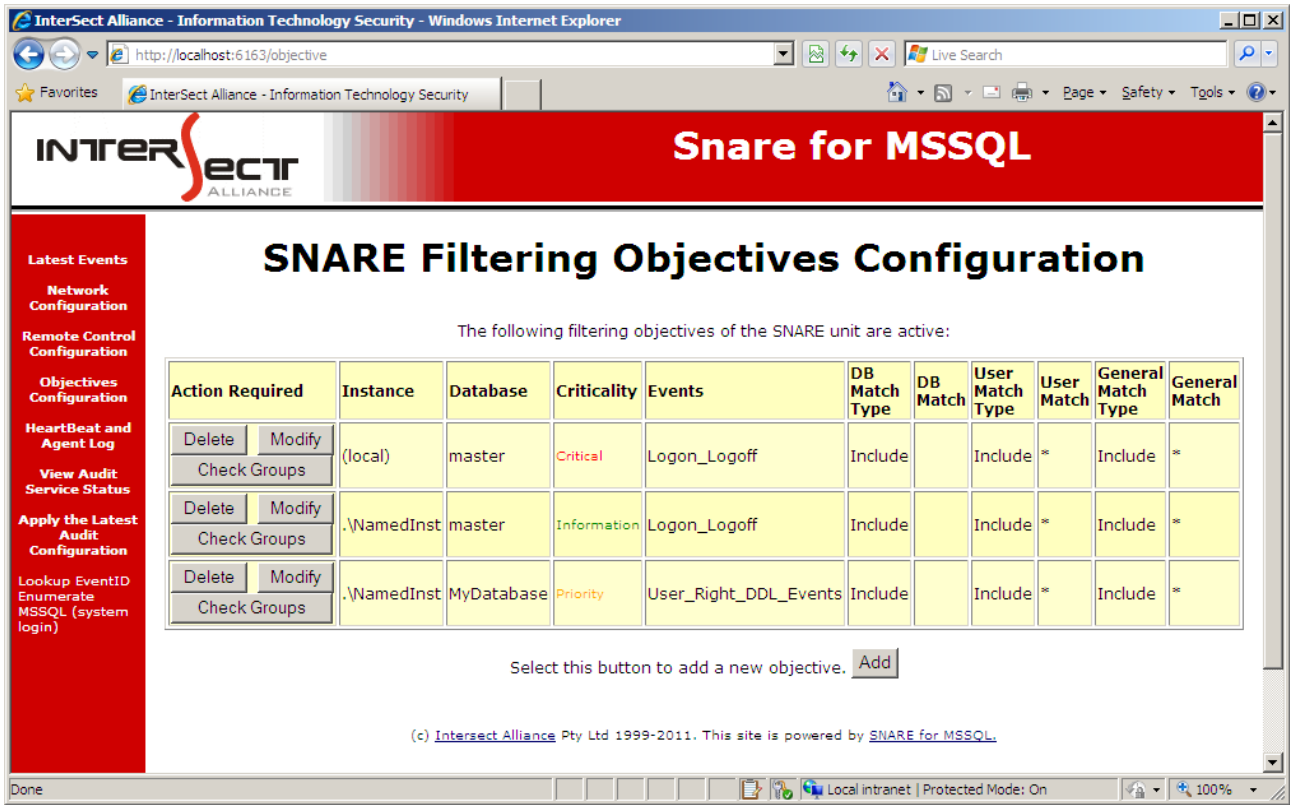


Figure 3: Objectives Configuration List

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.

5.3.2 Creating an Objective

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. 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.

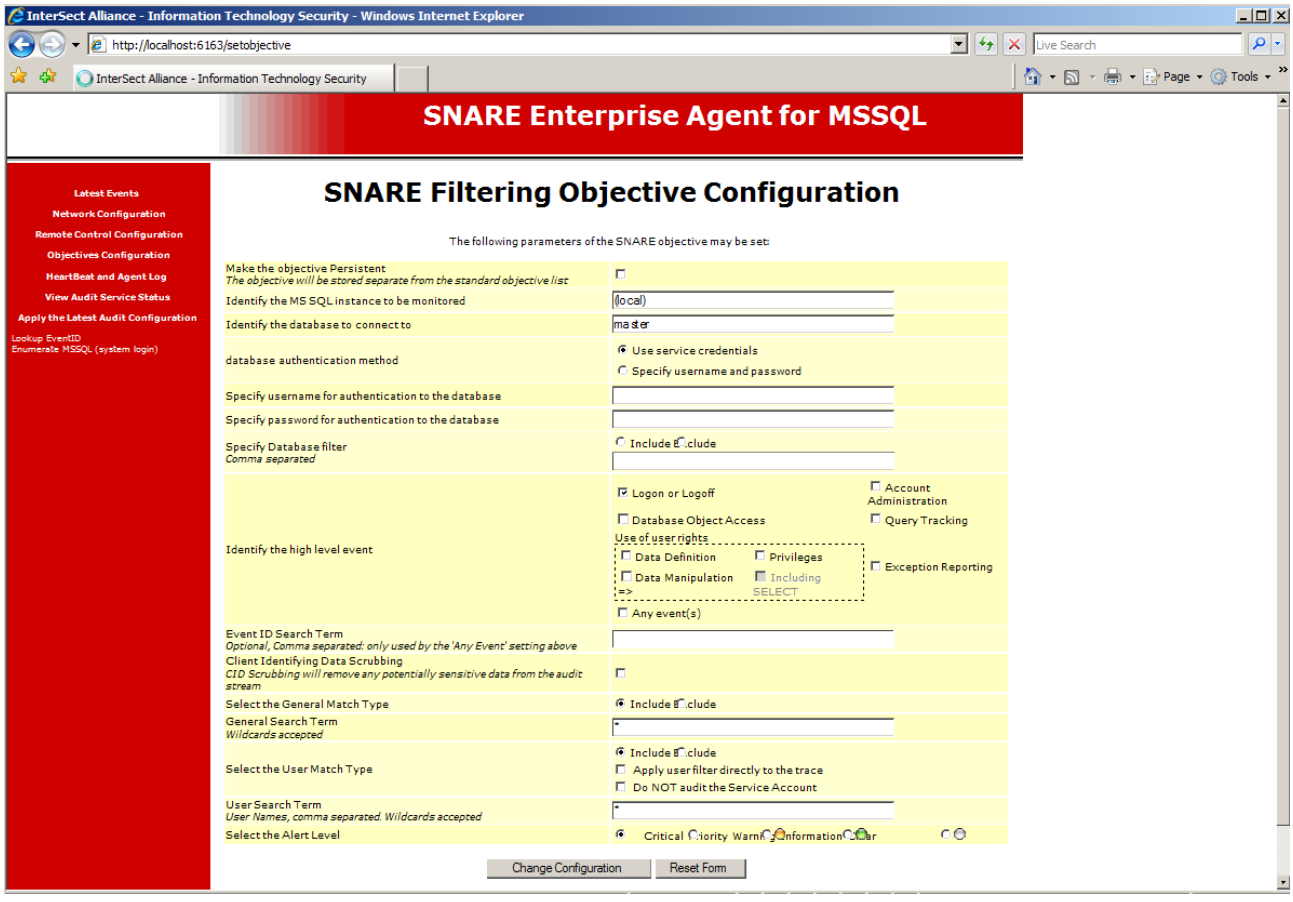


Figure 4: Creating an Objective

The following parameters of the objective may be set when creating an objective:

- ***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. This can be an Active Directory account or a built in SQL Server account. All accounts must be granted the SYSADMIN SQL Server role to allow access to the relevant trace audit functions.
- ***Specify username for authentication to the database:*** In SnareMSSQL, each objective in a stand alone deployment scenario provides settings to customize its connection to the database. Specifying the username (and password setting) allows 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. This is included in the SYSADMIN role SQL Server configuration by default. For more information on the required rights to perform "SP_TRACE_CREATE", consult your MS SQL Server documentation. If you are using a custom service account then this account must be granted the SYSADMIN role in order to function correctly.
- ***Specify password for authentication to the database:*** See above.
- ***Specify Database Filter:*** 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.

  The **Database Filter Search Term** allows the user to specifically identify which databases(comma separated) should be monitored. Search terms may not contain any wildcards, instead exact database names should be listed. For example, to monitor events from the "Finance" and "Inventory" databases:

  Database Filter Search Term: **Finance,Inventory**

- ***Identify the high level event:*** 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. Events included:
  - 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 define 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*** 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

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".

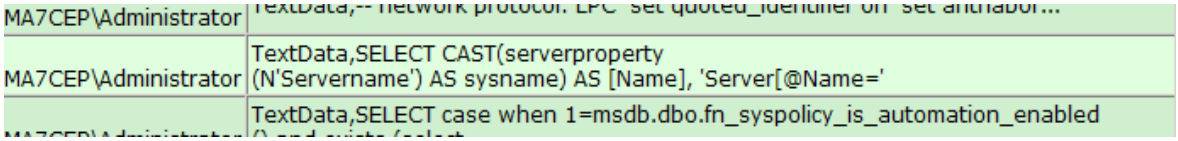
- ***Client Identifying Data Scrubbing:*** Select this checkbox and the agent will adjust any event messages enclosed by double quotes and single quotes with hashes (#) for that objective.

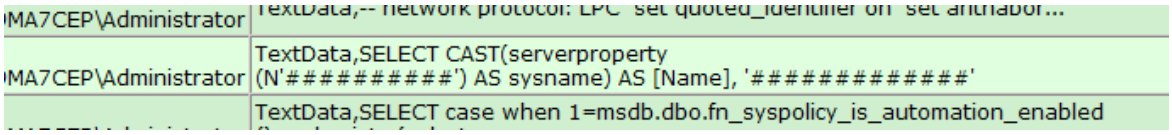
  Example: This is a test event about user "admin" and table "security" with id of 'bruce'.

  If the checkbox is ticked, then the above message will become the following before sent to a remote server:

  This is a test event about user "#####" and table "########" with id of '#####.

  Example: Latest event will hide the data in quotes and replace as hashes as below:





- ***Select the General Match Type:*** This determines how the **General Search Term** filter will be applied. If "Include" is selected (the default), then any event failing to match the search term is discarded by the agent. If "Exclude" is selected, then any event matching the search term is discarded by the agent.

- ***General Search Term:*** This field 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. Search terms are not case sensitive.

  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***

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:*** This determines how the **User Search Term** filter will be applied. If "Include" is selected (the default), then any event failing to match the search term (eg username of miero) is discarded by the agent. If "Exclude" is selected, then any event matching the search term is discarded by the agent.

  Each MSSQL event is associated with a user account and the following options facilitate to filter the events on the basis of user accounts:

  Apply user filter directly to the trace - Events that will pass the filter will be either included or excluded in the trace file

  Do NOT audit the Service Account-Apply the filter on the service account running the agent.

- ***User Search Term:*** This field 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. Both user and group related search terms are not case sensitive. Notice the square brackets for AD groups.

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]**

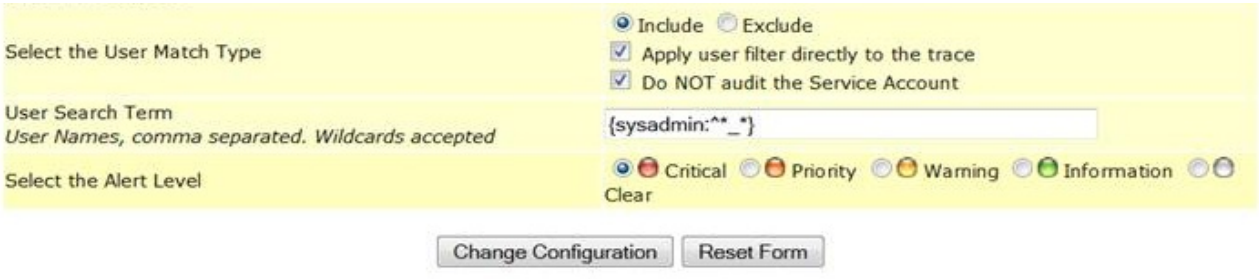
*Example: Exclude the user accounts in the serveradmin AD group that start with svc_*

User Search Term: **[serveradmin:^svc_*]**

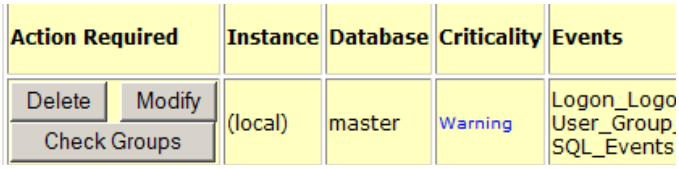
Example: Exclude the SQL Server accounts in the sysadmin SQL role

User Search Term: **{sysadmin:^*_*}**

Notice the curly/set brackets are for SQL Server.



To display the results, select Objectives Configuration | Check Groups.



The Group member results will be displayed as shown below.

Example: Exclude all service accounts from the audit logs starting with svc and a one way trust

User Search Term: **[sysadmin:^svc_*]**

The group details of the sysadmin role in SQL Server contained the following users:
- sa
- svc_sqlserver
- mydomain\adminsqlgroup
- altdom\adminsqlgroup

A one way trust is in place from the altdom domain to the mydomain, I.e. the altdom domain does not trust the mydomain but the mydomain trusts the altdom domain.
In this case the altdom domain is not queryable from the MSSQL Agent and will fail to determine the contents of the altdom\adminsqlgroup. The filter will be applied to all enumerated user accounts and an error displayed for any group that can not be enumerated.
If your environment has accounts from other untrusted domains and you wish filtering to be applied to include or exclude them, then the accounts from the other domain will have to be explicitly defined in the local sysadmin SQL role so the agent can detect them and filtering can be applied correctly.

- ***Select the 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.

To save and set changes to these objective settings, and to ensure the audit daemon has received the new configuration perform the following:

1. Click on **Change Configuration** to save any changes.
2. Click on the **Apply the Latest Audit Configuration** menu item and select **Reload Settings**.

Alternatively, the service may also be restarted by rebooting the system or by selecting restart service from within Windows. Whilst the SnareMSSQL Service is restarting, no events will be collected.

5.4 HeartBeat and Agent Log

The agent can send out regular heartbeats, letting the collecting device know that the agent is working without having to make contact. Agent logs are available which allow the agent to send status messages to the collection device, such as memory usage, service start and stop messages, and any errors or warnings triggered during operations. Configuration for heartbeat and logs is performed on the Snare HeartBeat and Agent Log Configuration page by selecting the ***HeartBeat and Agent Log*** menu item (see Figure 5).The parameters are discussed in detail below:

- **Agent Logging Options**. Select the type of agent logs required:

  Service logs – relate to the running agent service . Service tracking enables the agent to send audit events related to the agent service operations including starting, stopping, web server started, memory usage and configuration fingerprints.

  Policy Change logs – logs when operating system parameters are modified, such as Writing AgentLog Registry, Writing Objective Registry. The Policy Change tracking tells the agent to send an audit event any time it attempts to make a change to the local security policy and it will also report on any attempts to access the agent web interface or write agent configuration changes.

  Debug logs provide low level trace information used to debug the agent, and usually not required on a production machine.

- **Agent Heartbeat Frequency**. The frequency in which notification is sent to the server on the state of the agent. The frequency can be in minutes, hours or days. By default the heartbeat frequency is disabled.
- **Export HeartBeat data to a file?.** Enable this option to export the HeartBeat data to a file. Set the path to the destination of the file in ***Path of HeartBeat file*** setting.
- **Path of HeartBeat file.** If data is exported to a file, then the path destination of the file is set here.

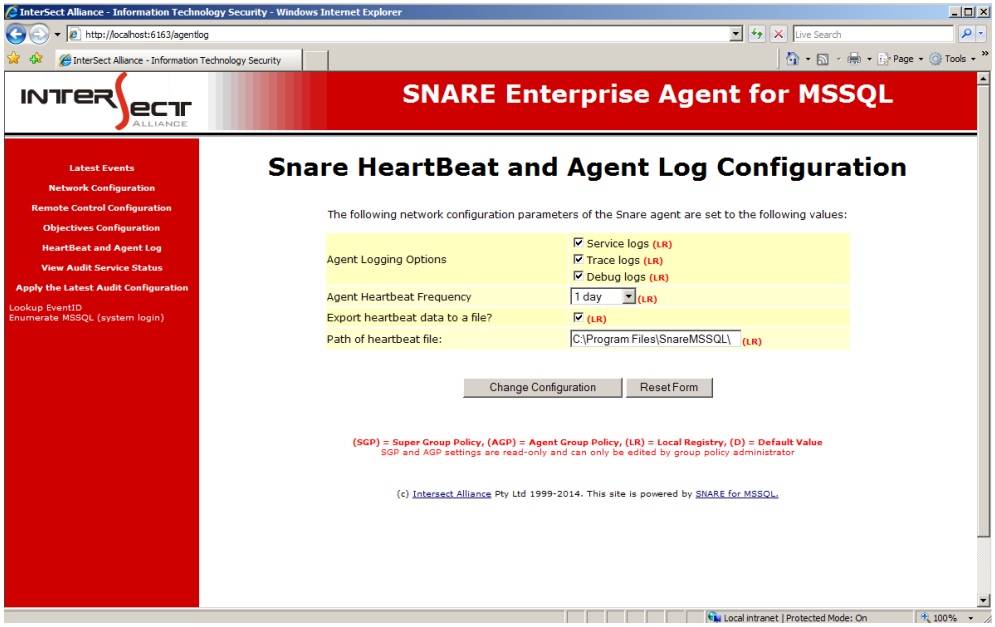


Figure 5: HeartBeat and Agent Log

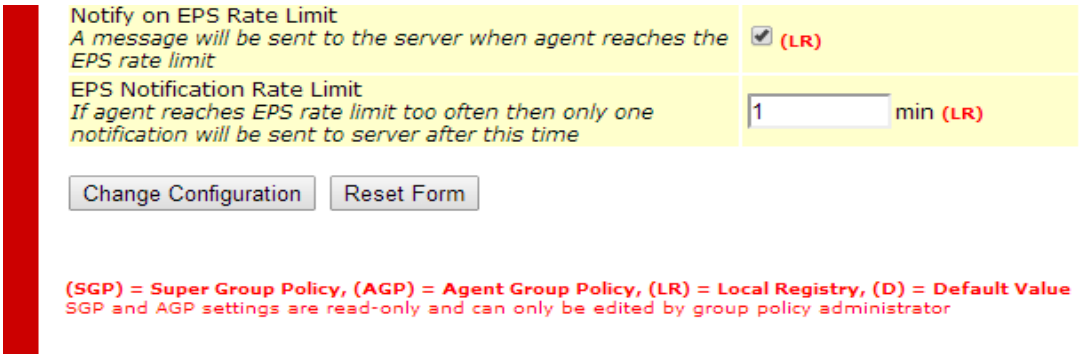
To save and set changes to these settings, and to ensure the audit daemon has received the new configuration perform the following:

1. Click on **Change Configuration** to save any changes.
2. Click on the **Apply the Latest Audit Configuration** menu item and select **Reload Settings**.

Alternatively, the service may also be restarted by rebooting the system or by selecting restart service from within Windows. Whilst the SnareMSSQL Service is restarting, no events will be collected.

5.5 Group Policy

The configuration of the agents can be managed using Group Policy Objects. As discussed in *Appendix B*, the Snare Agent policy key is located at **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Intersect Alliance\SnareMSSQL** and uses exactly the same settings and structure as the standard registry location. The agent gives the policy location the highest precedence when loading the configuration (that is, any policy settings will override local settings) and as long as there is a complete set of configuration options between the policy and standard registry locations, the agent will operate as expected.



At the end of each configuration setting, one of the following abbreviations are shown: (SGP), (AGP), (LR), (D). These are sources from where the parameter is set, and are defined as follow:

- **Super Group Policy (SGP):** If different types of snare agents (Snare for Windows, Snare Epilog, Snare Enterprise Agent for MSSQL) are running on a network then super group policy can be applied and all the agent will adhere to this policy. The registry path of SPG is **Software\Policies\InterSect Alliance\Super Group Policy**
- **Agent Group Policy (AGP):** This is regular group policy applied to all Snare for Windows agents. The registry path is same as explained in the beginning of this section.
- **Local Registry (LR):** These are setting assigned to the agent during installation and applied to the agent when none of the SPG and AGP are applied to the agent.
- **Default (D):** If due to any reason agent cannot read either of SPG, AGP or LR registry values then if assigns the default settings referred as (D).

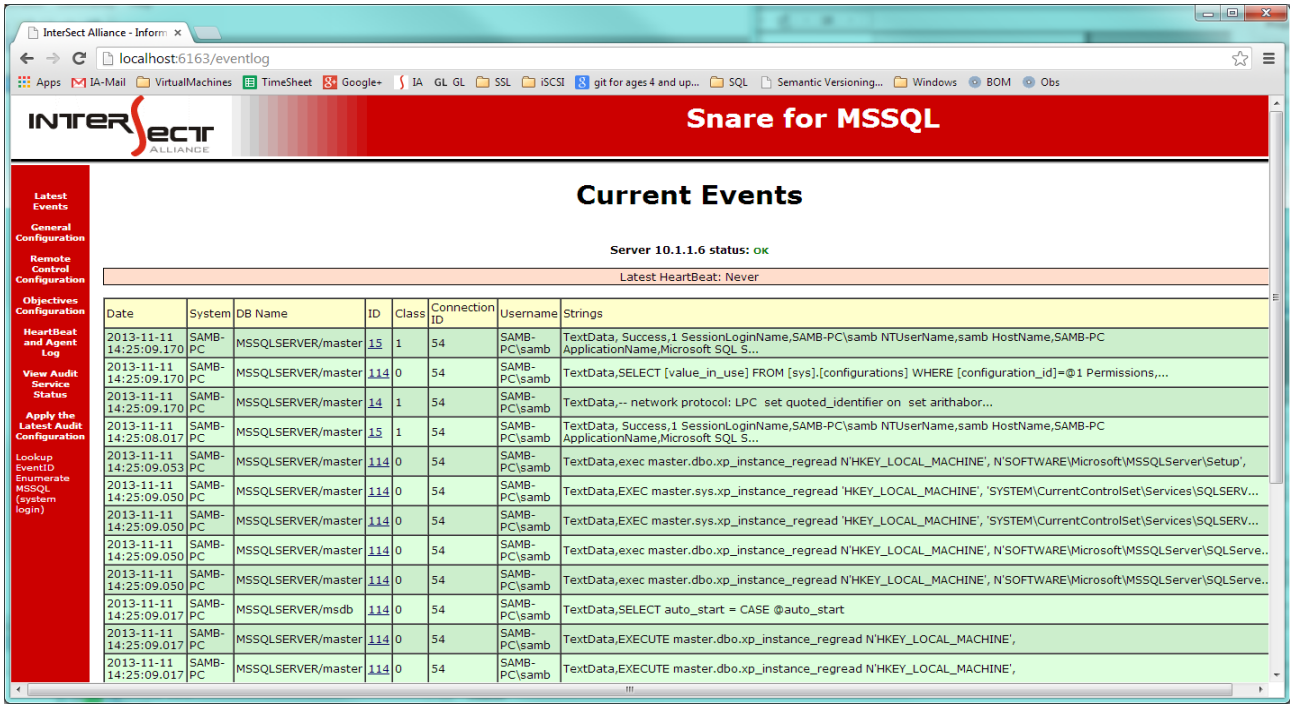
Below is a sample of an Administrative Template (ADM) file that can be loaded into a Group Policy Object to assist with selecting and setting configuration options.

```
CLASS MACHINE

        CATEGORY !!"InterSect Alliance Snare MSSQL Settings"

            #if version >= 4

                EXPLAIN !! "Contains examples of different policy types.\n\nShould
                display policy settings the same as \nADMX File - Example Policy
                settings category."

            #endif


        CATEGORY !!"Config"

        ;sets policy under "Software\Policies\InterSect Alliance\SnareMSSQL\Config"


            POLICY !!"Override detected DNS Name"

                #if version >= 4

                    SUPPORTED !!"This setting works with all agents"

                #endif


                EXPLAIN !!"This setting specifies the Hostname of the client.\n\n Must
                be not more than 100 chars, otherwise will be truncated."

                KEYNAME "Software\Policies\InterSect Alliance\SnareMSSQL\Config"


                PART !!"Override detected DNS Name with:" EDITTEXT EXPANDABLETEXT

                    VALUENAME "Clientname"

                END PART

            END POLICY

        END CATEGORY   ;CONFIG_CATEGORY
```

5.6 Latest Events

Selecting the **Latest Events** menu item displays 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.



Date	System	DB Name	ID	Class	Connection ID	Username	Strings
2013-11-11 14:25:09.170	SAMB-PC	MSSQLSERVER/master	15	1	54	SAMB-PC\samb	TextData, Success,1 SessionLoginName,SAMB-PC\samb NTUserName,samb HostName,SAMB-PC ApplicationName,Microsoft SQL S...
2013-11-11 14:25:09.170	SAMB-PC	MSSQLSERVER/master	114	0	54	SAMB-PC\samb	TextData,SELECT [value_in_use] FROM [sys].[configurations] WHERE [configuration_id]=@1 Permissions,...
2013-11-11 14:25:09.170	SAMB-PC	MSSQLSERVER/master	14	1	54	SAMB-PC\samb	TextData,-- network protocol: LPC set quoted_identifier on set arithabor...
2013-11-11 14:25:08.017	SAMB-PC	MSSQLSERVER/master	15	1	54	SAMB-PC\samb	TextData, Success,1 SessionLoginName,SAMB-PC\samb NTUserName,samb HostName,SAMB-PC ApplicationName,Microsoft SQL S...
2013-11-11 14:25:09.053	SAMB-PC	MSSQLSERVER/master	114	0	54	SAMB-PC\samb	TextData,exec master.dbo.xp_instance_regread N'HKEY_LOCAL_MACHINE', N'SOFTWARE\Microsoft\MSSQLServer\Setup',
2013-11-11 14:25:09.050	SAMB-PC	MSSQLSERVER/master	114	0	54	SAMB-PC\samb	TextData,EXEC master.sys.xp_instance_regread 'HKEY_LOCAL_MACHINE', 'SYSTEM\CurrentControlSet\Services\SQLSERV...
2013-11-11 14:25:09.050	SAMB-PC	MSSQLSERVER/master	114	0	54	SAMB-PC\samb	TextData,EXEC master.sys.xp_instance_regread 'HKEY_LOCAL_MACHINE', 'SYSTEM\CurrentControlSet\Services\SQLSERV...
2013-11-11 14:25:09.050	SAMB-PC	MSSQLSERVER/master	114	0	54	SAMB-PC\samb	TextData,exec master.dbo.xp_instance_regread N'HKEY_LOCAL_MACHINE', N'SOFTWARE\Microsoft\MSSQLServer\SQLServe..
2013-11-11 14:25:09.050	SAMB-PC	MSSQLSERVER/master	114	0	54	SAMB-PC\samb	TextData,exec master.dbo.xp_instance_regread N'HKEY_LOCAL_MACHINE', N'SOFTWARE\Microsoft\MSSQLServer\SQLServe..
2013-11-11 14:25:09.017	SAMB-PC	MSSQLSERVER/msdb	114	0	54	SAMB-PC\samb	TextData,SELECT auto_start = CASE @auto_start
2013-11-11 14:25:09.017	SAMB-PC	MSSQLSERVER/master	114	0	54	SAMB-PC\samb	TextData,EXECUTE master.dbo.xp_instance_regread N'HKEY_LOCAL_MACHINE',
2013-11-11 14:25:09.017	SAMB-PC	MSSQLSERVER/master	114	0	54	SAMB-PC\samb	TextData,EXECUTE master.dbo.xp_instance_regread N'HKEY_LOCAL_MACHINE',

Figure 6: 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 or when the Latest Events option is selected. New entries will be highlighted in green as the page is refreshed.

5.7 View Audit Service Status

The service status can be viewed by selecting the **View Audit Server Status** menu item as shown below This will display whether the Snare for MSSQL service is active, along with some basic information about the agent including the version number.

Figure 7: View Audit Service Status

6 SNARE Server

The Snare Server is a log collection, analysis, reporting, forensics, and storage appliance that helps your meet departmental, organisational, industry, and national security requirements and regulations. It integrates closely with the industry standard Snare agents, to provide a cohesive, end-to-end solution for your log-related security requirements.

The Snare Server, as shown in Figure 8 collects events and logs from a variety of operating systems, applications and appliances including, but not limited to: Windows (NT through 2012), 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.

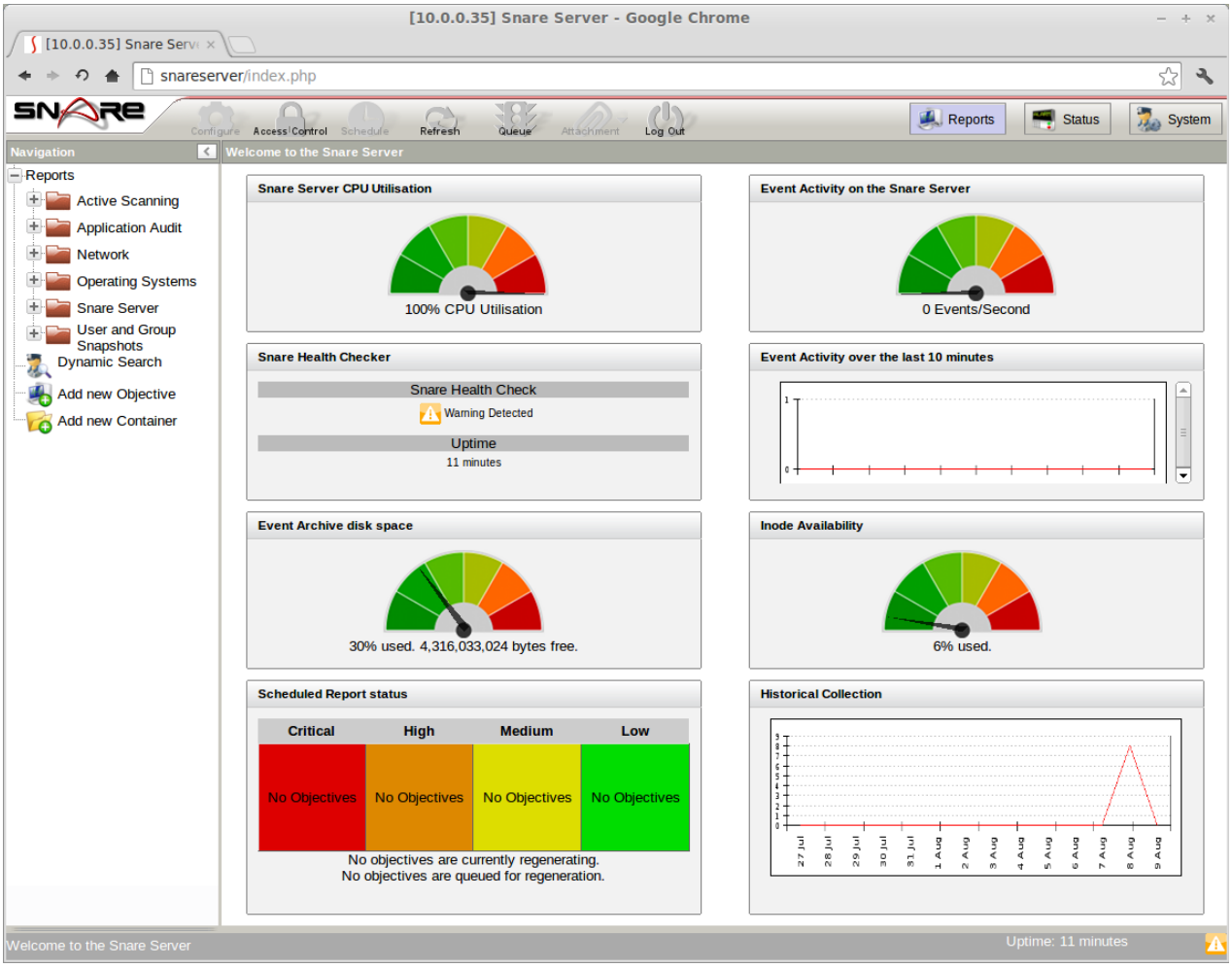


Figure 8: Welcome to the Snare Server

Some of the key features of the Snare Server include:

- Ability to collect any arbitrary log data, either via UDP or TCP
- Secure, encyrpted channel for log data using TLS
- 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, or a third party collection system
- 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.
- 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 'clone' existing objectives in order to significantly tailor the reporting criteria. 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 a wide variety of parameters.
- Very simple download and installation
- Flexibility when dealing with unique customer requirements
- A strategic focus on low end hardware means that Snare can achieve outstanding results with minimal hardware cost outlay
- Snare gives you useful data, out of the box, with default objectives tuned for common organizational needs
- Ability to manage Enterprise Agents
- All future Snare Server versions and upgrades included as part of an annual maintenance fee.

The Snare Server is an appliance solution that comes packaged with a hardened, minimal version of the Linux operating system to provide baseline computing functionality, which means you do not need to purchase additional operating system licenses, database licenses, or install additional applications in order to get up and running. Like your android phone, or your home router, any operating-system level management and maintenance is either automated, or is available within the web-based interface.

For further information on the Snare Server refer to the *Snare Server User Guide* on the Intersect Alliance website.

7 About Intersect Alliance

Intersect Alliance, part of the Prophecy International Holdings Group, 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.

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.

Intersect Alliance welcomes and values your support, comments, and contributions.

For more information on the Enterprise Agents, Snare Server and other Snare products and licensing options, please contact us as follows:

The Americas +1 (800) 834 1060 Toll Free | +1 (303) 771 2666 Denver

Asia Pacific +61 8 8213 1200 Adelaide Australia

Europe and the UK +44 (797) 090 5011

Email intersect@intersectalliance.com

Visit 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.

Registry Path	**Setting Description**
`[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 `OutputFilePath`. 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 `OutputFilePath`.
`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).
`UseUTC`	REG_DWORD Timestamp logs using Coordinated Universal Time instead of local time if set to 1.

Registry Path	Setting Description
[Objective]	**This subkey stores all the filtering objectives.**
Objective# (where # is an integer number)	Objectives are of type REG_BINARY and contain an *encrypted copy* 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 (default via agent console). 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.
RateLimit	This value is of type REG_DWORD, and determines the upper limit for events per second (EPS) that the agent will send to server. This feature only appears in supported agents.
NotifyMsgLimit	This value is of type REG_DWORD having value 0 or 1, and determines whether to send or not the EPS notification to server (1 means send and 0 means not to send) whenever agent reaches EPS RateLimit. This feature only appears in supported agents.
NotifyMsgLimitFrequency	This value is of type REG_DWORD, and determines the frequency of events per second notification. The value is treated in minutes and only one EPS notification message is sent to server regardless of how many times agent reaches EPS limit during these minutes. This feature only appears in supported agents.
[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

Registry Path	Setting Description
	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 group[1].

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.

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

191	TM: Save Tran starting	Occurs when a SAVE TRANSACTION request starts.
192	TM: Save Tran completed	Occurs when a SAVE TRANSACTION request completes.
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