SNARE

System iNtrusion Analysis & Reporting Environment

Guide to Snare for Windows for v4.2/4.3

INTERSECT ALLIANCE

About this guide

This guide introduces you to the functionality of the Snare agent for Windows operating systems. The development of 'Snare for Windows' will allow event logs collected by the Windows operating system (including 2003, XP, Vista, Server 2008, Server 2008 R2, Windows7) to be forwarded to a remote audit event collection facility. The Snare Enterprise Agent for Windows (i.e the purchased agent) supports the above operating systems as well as Windows8, Windows8.1, Server 2012 and Server 2012 R2). Snare for Windows will also allow a security administrator to fully remote control the application through a standard web browser if so desired.

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.

Agents are available for Windows (2003/XP/Vista/2008/2008 R2/Windows7/Windows8/2012/2012 R2), Linux, Solaris, Epilog, MSSQL 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 10 Snare Server* for further details. A feature of the Snare Server is the Agent Management Console that provides the ability to audit and manage the configuration of the Snare Agents within your environment, further discussed in *Snare Agent Management Console* on page 35.

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

2. Enterprise vs OpenSource

Intersect Alliance issues two types of agents:

- Enterprise Agents - licensed and supported by Intersect Alliance and its partners. If you need to address an audit or regulatory compliance requirement, work with sensitive or private information or require a supported security platform, then the Snare Enterprise Agents are recommended.
- OpenSource Agents – audit and event log collection with source code available under the terms of the GNU Public License. The OpenSource agents provide a stable solution, but do not include all the features offered by the Enterprise Agents.

When deciding which type of Agent your organisation should use, the following questions should be considered:

1. **Support** – If you require a supported security platform then you need to use the Enterprise Agent. The OpenSource agent is provided to the OpenSource community free of charge and as issued. The Enterprise Agents include maintenance, upgrades, and bug fixes to the product and customer support for your organisation.
2. **Complete and Factual** – If your organisation needs to know that every log will be captured and forwarded with integrity then you need to use the Enterprise Agents. The OpenSource agent does not support TCP, custom event logs, UTC or registry audits.
3. **Sensitivity and Confidentiality** – Should your organisation work with sensitive data, then you need to use the Enterprise Agents which includes the ability to support best practices and encryption protocols.

The following table highlights the feature sets available in these agents.

Agent Feature	Enterprise	OpenSource
Regulatory Compliance Helps gather information to comply with NISPOM, PCI, SOX or other regulations.	✔	
Vendor Support Product maintained, updated and supported for compliance.	✔	
Windows2012 / Windows8 Agent supported on all Windows platforms, including W2012 and W8 platforms.	✔	
Capture Custom Windows Event Logs Capture and transmit all logs including Application and Services logs in addition to the Windows Event Logs.	✔	
Event Log Caching Caching of events in case of a network disruption, ensuring that the events are not lost	✔	
TCP Confirmed log message delivery with Smart TCP - no lost or missing logs.	✔	

Encryption with TLS/SSL*or 3DES Protecting the confidentiality and integrity of log messages in transit.	✔	
Monitor Registry Events Ability to apply auditing to sections of the registry and report changes.	✔	
Dynamic DNS Provides uninterrupted real time 24x7 operation.	✔	
USB Devices External device monitoring, such as USB devices and removable media on Windows XP,2003,2008,2012 operating systems	✔	
Enhanced Event Throttling Configure events per second (EPS) rate controls and provide alerts when EPS limits are reached.	✔	
UTC Use UTC time zone normalization to ensure the correct sequencing of events by standardizing across geographies and time zones.	✔	
Agent Heartbeat Heartbeats are sent out, letting the collecting device know that the agent is operational. Logging options include tracking audit events on service operations and local policy changes.	✔	
Multiple Destinations Log message simulcasting enables the distribution of events to multiple destinations.	✔	
Single MSI A single smart MSI for all Windows platforms ensuring simplified and error free distribution	✔	
Easily Tailorable to Event Log Format Native Snare and multiple syslog headers options to support different SIEM systems.	✔	
Centralized Configuration Management with the Snare Agent Management Console For the mass management, monitoring and configuration of the agent.	✔	
Group Policy Support Group Policy Objects (e.g. ADM files) can be used to configure the agent in an easy and widely supported way without the need for setting "Preferences", a.k.a. tattooing	✔	
Monitor Agent Configuration Changes This feature adds another layer of security by allowing administrators to remotely monitor changes to the agent's configuration.	✔	
Regular expression for General Search Match Allows matching event text using Perl Compatible Regular Expression syntax giving more flexible search options.	✔	
Truncation of Verbose Event Text To reduce server resource wastage, events may be truncated by matching on simple text phrases.	✔	

Log Server Connection Status The Current Events page displays the connection status of the logging server(s).	✔	
Alternate Syslog destination options RFC5424 compliant	✔	
Syslog destination options RFC3164 compliant	✔	✔
Light on Resources 1. Small deployment footprint (E.G.1.5Mb) 2. Minimal Host resource requirements (E.G.<5% of CPU) 3. Minimal Host memory requirements (E.G. less than 20Mb)	✔	✔
Real Time Event Filtering The Snare Agents can find, filter and forward events which contribute to the organisation's security requirements, while ignoring others, thus greatly reducing network traffic and back end server and analysis resources measured in EPS	✔	✔
Installer Easy to use installer / Silent install option	✔	✔
UDP "Fire and forget" message delivery.	✔	✔
Locale Date Information If your organisation has locations and different timezones then the Agent can optionally send events with a UTC timestamp and a US English Locale to ensure the integrity of the log record from its source.	✔	✔
Stability The event collection minimizes any interference with the host's operating system and applications so that the service can be as stable and independent as possible.	✔	✔
Latency and Real Time Operation in real time mode, so as the events are generated, they are automatically sent to the SIEM server without delay or the risk of compromise of modification.	✔	✔
Remote Control Interface Snare allows you to remotely control the agents when the audit/event logging configuration of the target system needs to be dynamically changed.	✔	✔
Native OS Audit Control The Snare agents are able to configure the native event sub-system, and if so desired, allow the generation of only specific events required by the security policy.	✔	✔
Upgrading Upgrade option to preserve existing configuration settings	✔	✔

3. Overview of the Snare Agents

Snare operates through the actions of a single component; the ***SnareCore*** service based application (*snarecore.exe*). The ***SnareCore*** service interfaces with the Windows event logging sub-system to read, filter and send event logs from the primary Application, System and Security event logs to a remote host. Please note that where available, the agent is also capable of reading, filtering and sending logs from the DNS Server, File Replication Service, DFS-Replication and Directory Service logs, as well as any Custom event log sources such as those under Applications and Services Logs. In addition to regular event logs, ***SnareCore*** will collect USB connect and disconnect notifications.

Once gathered, the logs are then filtered according to a set of objectives chosen by the administrator, and passed over a network using the UDP or TCP protocol, using optional TLS/SSL encryption, to a remote server. The ***SnareCore*** service can be remotely controlled and monitored using a standard web browser (see Figure 1a and Figure 1b for example screens).

The Custom event log capability, TCP protocol capability, TLS/SSL support and the ability to send events to multiple hosts is only available to users who have purchased the Enterprise Agents. See Chapter 11 About Intersect Alliance for further details.

The ***SnareCore*** service reads event log data from the core Windows event sources listed above, plus USB device notifications. ***SnareCore*** converts the binary/encoded event log record to a human-readable format. If a SYSLOG or Snare Server is being used to collect the event log records, the event records will be TAB delimited. This format is further discussed in ***Appendix A*** Event output format *on page* 46. The net result is that a raw event, as processed by the SnareCore service may appear as follows:

Example:

```
Test_Host MSWinEventLog 0 Security 3027 Fri May 24 09:30:43 2013 593
Security    Administrator User Success Audit LE5678WSP Detailed
Tracking    A process has exited:Process ID: 656     User Name:
Administrator     Domain: LE5678WSP Logon ID: (0x0,0x6C52)
```

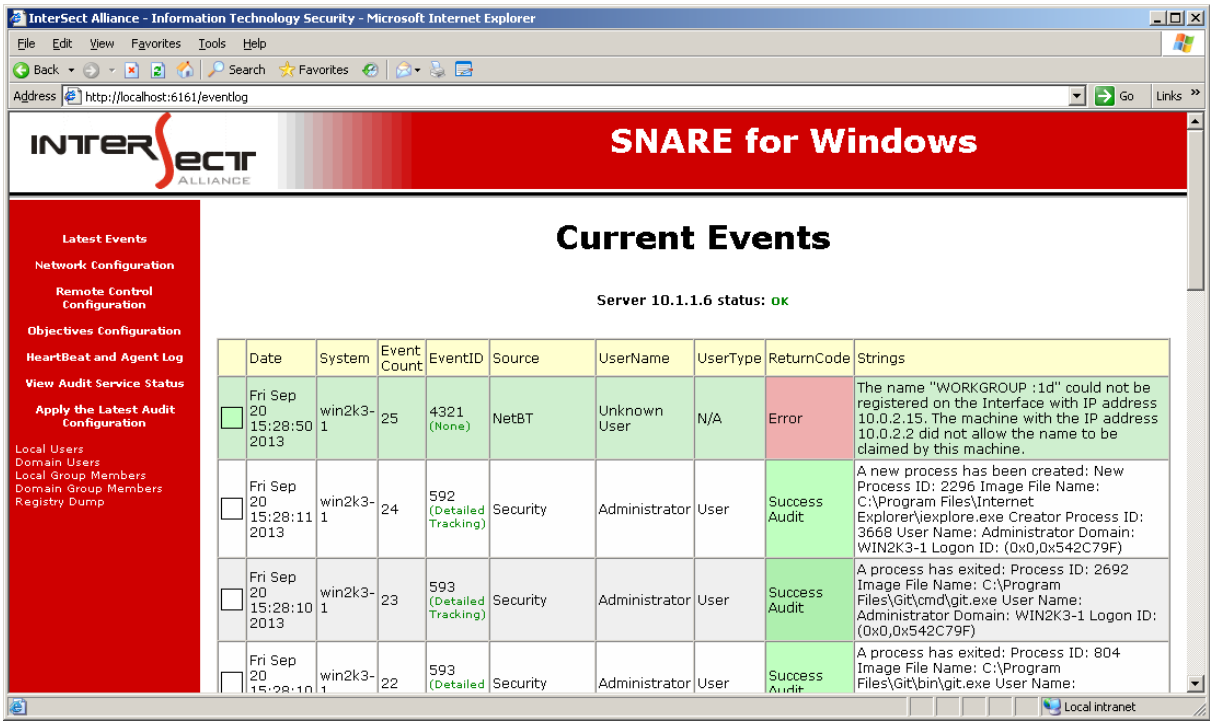


Figure 1a Main event window (Windows 2003)

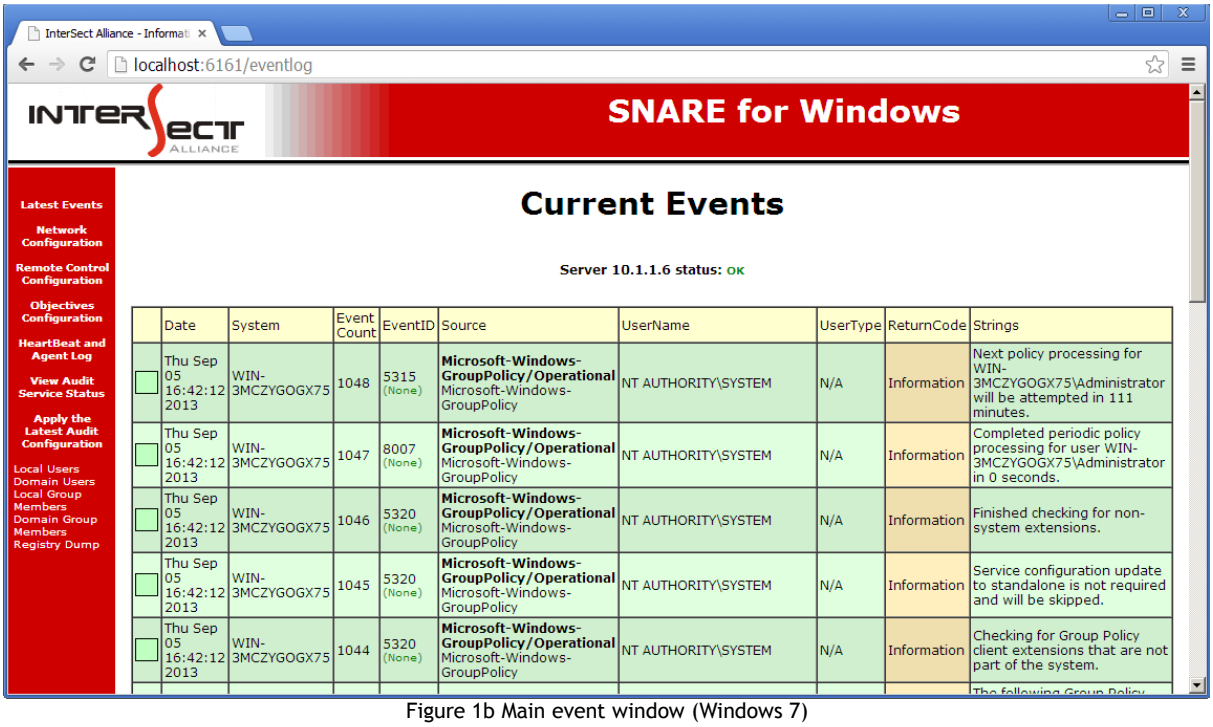


Figure 1b Main event window (Windows 7)

4. Installing and running Snare

Snare is provided as a single-file self-extracting archive, and has been designed with an installation wizard and advanced silent install options to allow for easy installation and configuration of all critical components. The self-extracting archive installs all components of Snare, including icons, changelog documentation, and the snarecore.exe binary.

The snarecore.exe binary implements the "**SnareCore**" service, which is responsible for reading event log records, filtering the events according to the objectives, providing a web based remote control and monitoring interface and providing all the necessary logic to allow the binary to act as a service defined in any of the supported versions of Windows (including 64 bit versions).

Organisations that wish to remotely deploy pre-configured Snare agents to workstations and servers, without physically moving from system to system, may appreciate the MSI (Microsoft Installer utitlity) functionality. The Snare Enterprise Agent supports being used as a single smart MSI for all Windows platforms and releases ensuring simplified and error free distribution. Refer to documentation on the Intersect Alliance website, *Snare for Windows Custom MSI*.

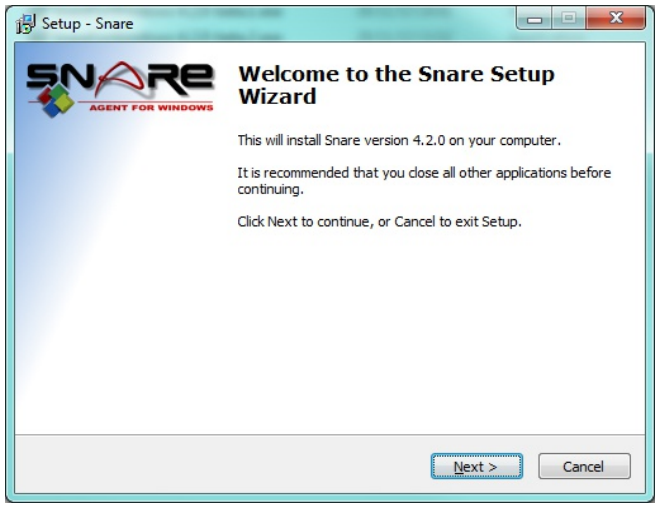
Creating a MSI file for Snare is only available to users who have purchased the Enterprise Agents. See Chapter 11 About Intersect Alliance for further details.

4.1 Wizard Install

Download the SnareEnterpriseAgent-Windows-v*{Version}*-SUPP-MultiArch.exe file from the Intersect Alliance website (where *{Version}* is the most recent version of the file available).

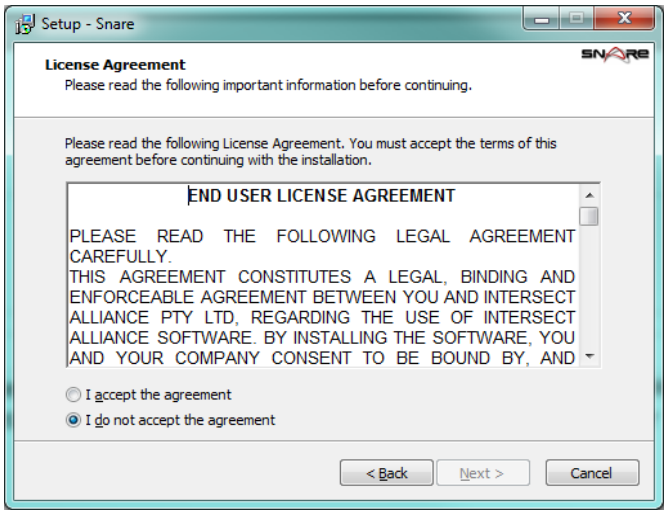
Ensure you have administrator rights, double-click the SnareEnterpriseAgent-Windows-v*{Version}*-SUPP-MultiArch.exe file. This is a self extracting archive, and will not require WinZip or other programs. You will be prompted with the following screens:

Welcome to the Snare Setup Wizard



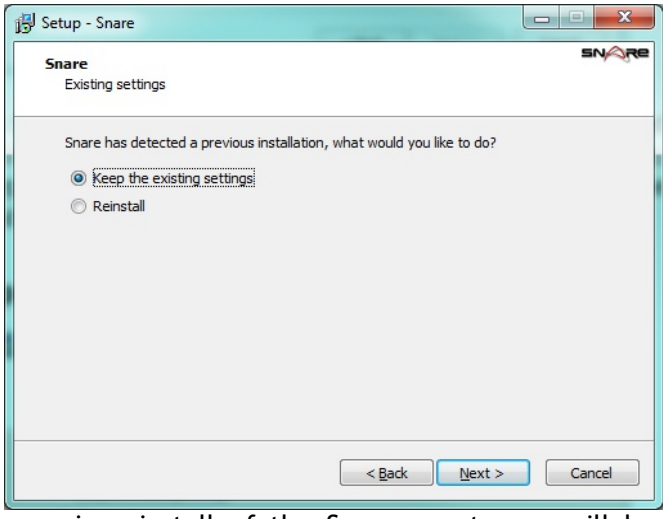
This screen provides a brief overview of the product you are about to install. Where available, select "Next" to continue the installation, "Back" to return to the previous screen or "Cancel" to abort the installation.

License Page



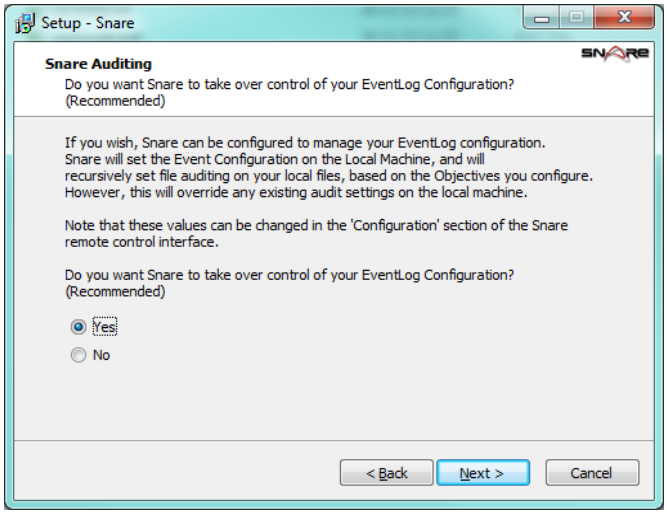
The License Page displays the End User License Agreement (EULA) for supported versions of the agent or the GNU General Public License (GPL) for the OpenSource release. Please read the document carefully and if you accept the terms of the agreement, select "I accept the agreement" and the "Next" button will be enabled allowing the installation to continue.

Existing Install (Upgrade only)



If the Wizard detects a previous install of the Snare agent, you will be asked how to proceed. Selecting "Keep the existing settings" will leave the agent configuration intact and only update the Snare 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.

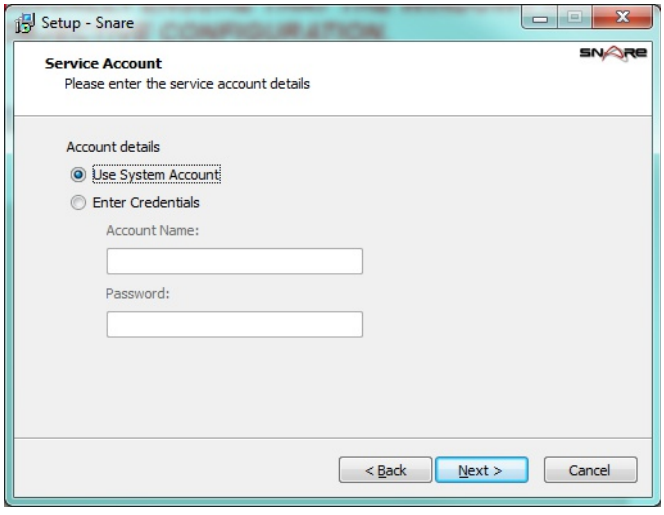
Auditing



The Snare agent has the ability to automatically configure the audit settings of the local machine to match the configured objectives. To enable this feature, select "Yes".

NB: VERY IMPORTANT: IF YOU DO NOT SELECT THIS OPTION AND/OR THE WINDOWS ACTIVE DOMAIN GROUP POLICIES OVERWRITE THE AUDIT SETTINGS, THEN YOU WILL NEED TO MANUALLY ENSURE THAT THE WINDOWS AUDIT SETTINGS MATCH YOUR DESIRED OBJECTIVE CONFIGURATION.

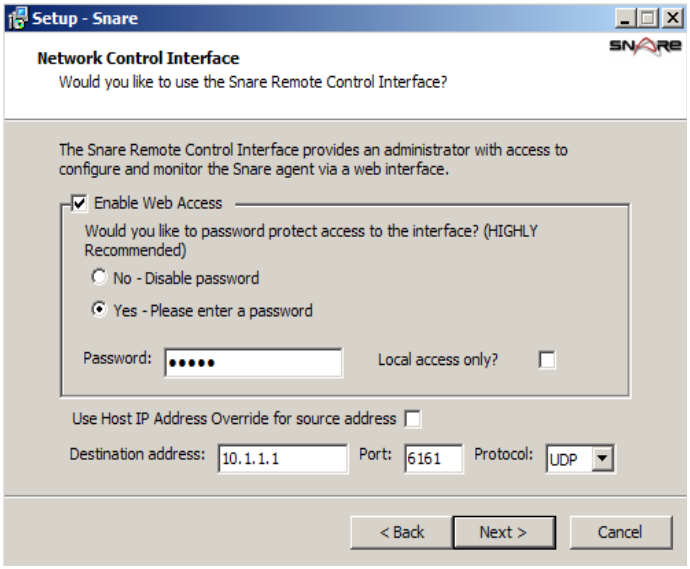
Service Account



The Snare agent requires a service account to operate. The default option is to use the in-built SYSTEM account.

Network Control Interface

This screen provides a means to configure the Snare Agent's web interface, named the Remote Control Interface for first time use. Other settings that may be set include network configuration settings that are also available from the Remote Control Interface | Network Configuration screen.



Select from the following options to configure the **Snare** web interface:

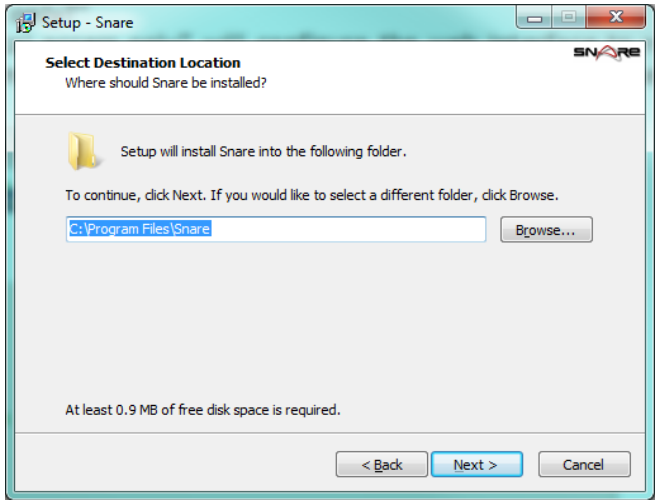
- **"Enable Web Access"**
  Select this option to enable the web interface.
  The following options may also be configured:
  - **No - Disable password**
    The web interface will operate without a password, allowing unauthenticated access to the configuration options.
  - **Yes - Please enter a password**
    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.
  - **Local access only?**
    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.

The following settings are available from version 4.3.0:

- **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.
- **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.

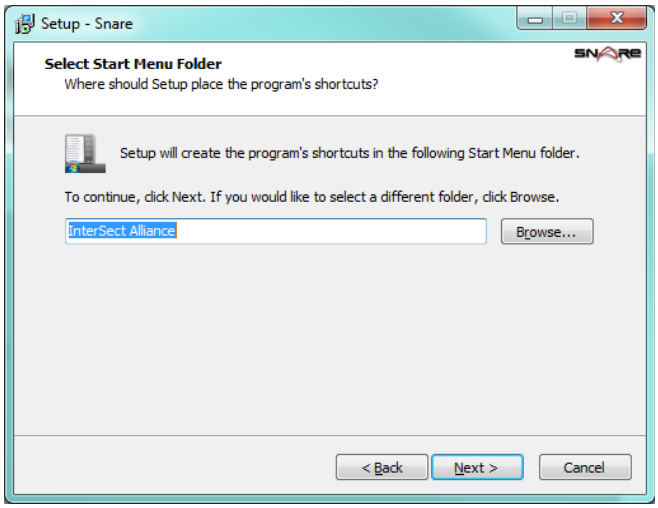
NOTE: If the Enable Web Access option is NOT selected, all configuration changes will need to be made by directly modifying registry settings and the service will need to be restarted for any changes to take effect.

Select Destination Location



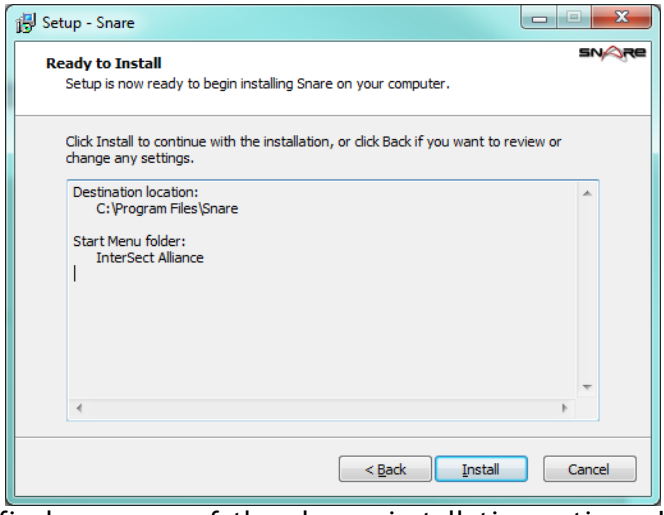
This screen provides a means to select the folder where the Snare Agent will be installed. If the folder name specified does not exist, it will be created. It is important that this folder has at least enough space available to install the agent.
By default, the installation wizard will install Snare 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



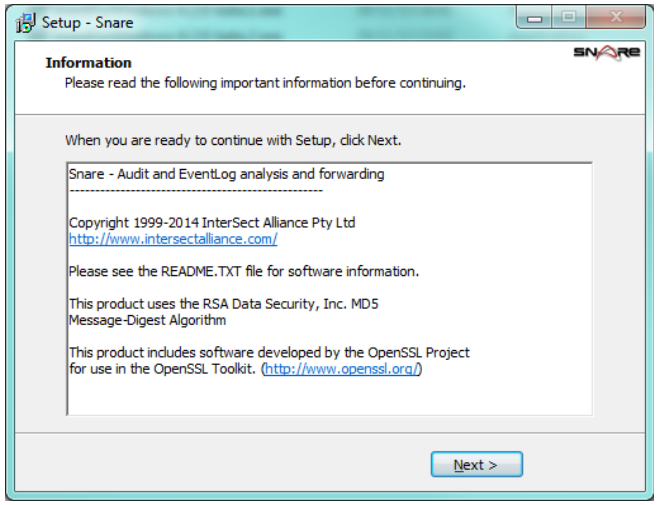
Select the program group within the *Start Menu* under which a shortcut to the Snare Agent's remote control interface will be created.

Ready to Install



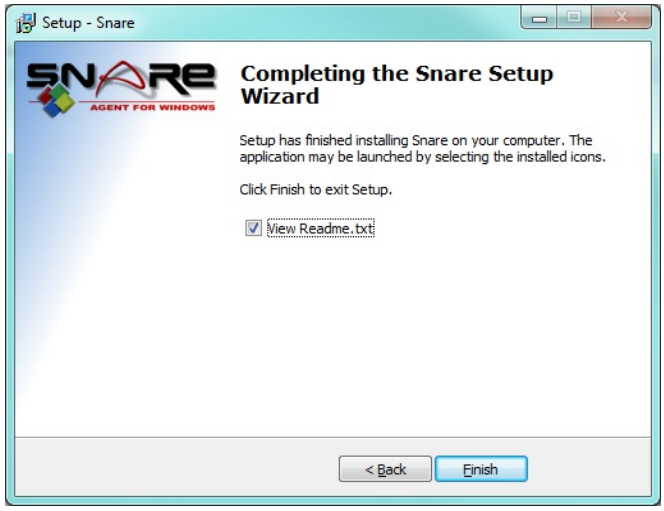
This screen provides a final summary of the chosen installation options. If the options listed are incorrect, select the "Back" button to return to previous screens and change their configuration. Select the "Install" button to proceed with the listed choices, or "Cancel" to abort the installation without 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 Snare 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.

4.2 Silent Install

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

Command line options

The Snare installer has a number of command line options to support silent, automated installations:

- **/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 created: *filename* and *filename*.Snare.log. The Wizard installation log will be written to *filename* and a detailed Snare installation log will be written to *filename*.Snare.log.
- **/LoadInf="*INFfile*"** – The *INFfile* is a template file produced by another Snare 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 Snare files, all configuration settings will remain untouched and the "LoadInf" file will be ignored.

The following are available from v4.3.0:

- **/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.

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 agent using the Wizard.
2. Using the web interface, configure the agent's Network and Remote Control settings.
3. Configure one or more objectives.

4. Ensure you have administrator rights, open a command prompt and browse to the directory where Snare is installed.
5. Run the following commands:
   - **SnareCore.exe -x**
     Export the information and error messages, along with the INF file contents to the screen.
   - **SnareCore.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:

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

This will install the ***Snare*** 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.

To install the agent setting the network configuration:

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

4.3 Running Snare

Upon installation of the Snare agent, an 'Intersect Alliance' menu item is available from the All Programs Windows menu. The Snare remote control launch menu is then available from All Programs->Intersect Alliance->Snare for Windows.

The Remote Control Interface may also be accessed via a web browser from the local machine by visiting the URL http://localhost:6161/. The Remote Control Interface is turned on by default, and also password protected for security reasons. The default username and password are:
Username: snare
Password: snare

*If you previously configured a password, you will need this to log in, along with the username '**snare**'.*

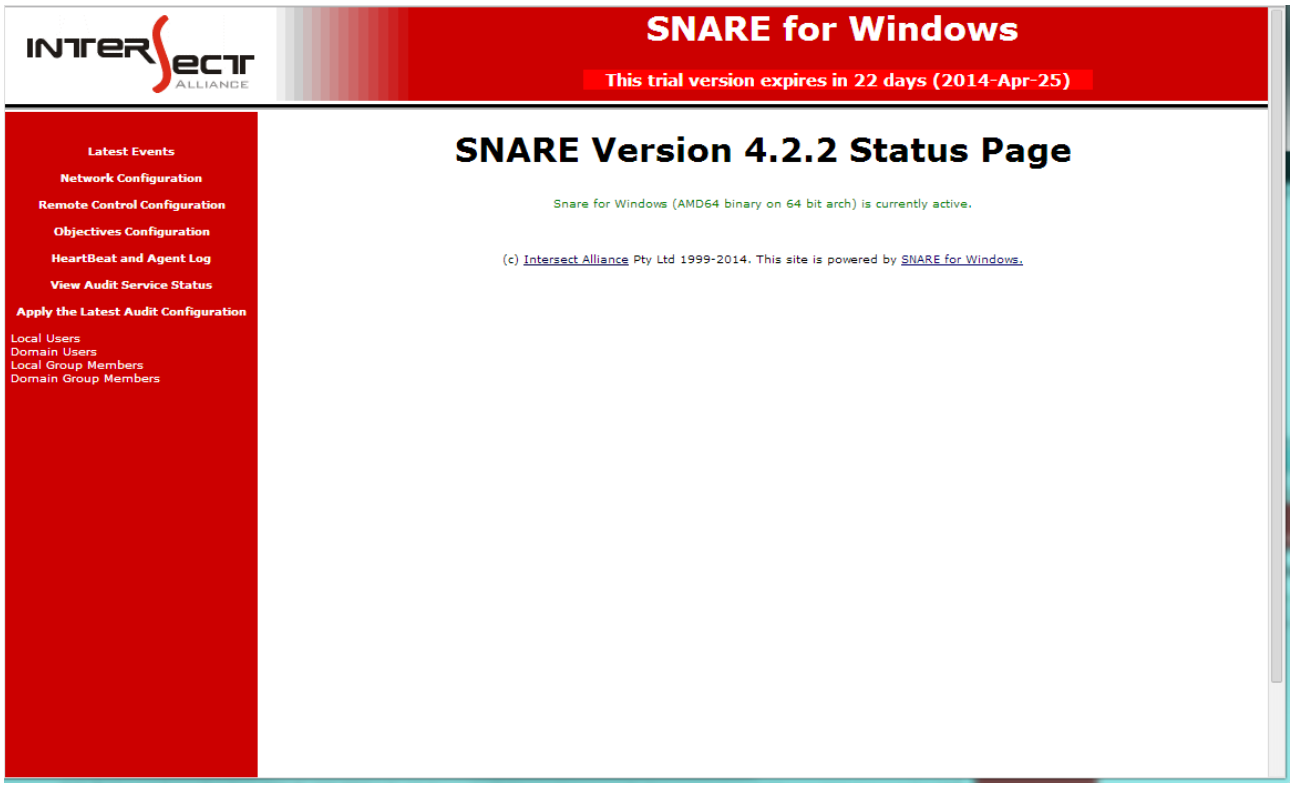
Note: The default password is not encrypted at this time. Ensure you change the default Snare password immediately after installation so that it is encrypted, for security purposes. It is recommended you use a strong complex password of at least 12 characters. To update the password go to the Remote Control Configuration page and update the password.

Issues with SnareCore service

For events to be passed to a remote host, the ***SnareCore*** service must be running. Ensure the ***SnareCore*** service is active by selecting Services from the **Administrative Tools** or **Computer Management** menus. If Snare is not running, double click on the service name, then select **Automatic** from the Startup Type list so that the service is started automatically when the host is rebooted and then click the **Start** button. Click **OK** to save the settings.

4.4 Evaluation Version

Intersect Alliance offers a trial version of the agents providing full functionality for a limited time for evaluation purposes. If this 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:

The **Latest Events** page will continue to update with current events, however no further events will be transmitted to the server.

To continue enjoying the benefits of Snare, please contact Intersect Alliance to purchase a licensed solution.

See Appendix D for upgrading your Evaluation Agent to the Enterprise Agent.

5. Setting the audit configuration

The configurations for Snare for Windows agents is stored in the system registry. The registry is a common storage location of configuration parameters for Windows programs and other applications. The registry location contains all the details required by Snare to successfully execute. Failure to specify a correct configuration will not 'crash' the ***SnareCore*** service, but may result in selected events not being able to be read and the agent not working as specified.

Note manual editing of the registry location is possible, but care should be taken to ensure that it conforms to the required Snare format. Also, any use of the web based Remote Control Interface to modify selected configurations, will result in manual configuration changes being overwritten. Details on the configuration format for the registry can be viewed in ***Appendix B*** - Snare Windows registry configuration description *on page* 47.

The most effective and simplest way to configure the ***SnareCore*** service is to use the Snare web based Remote Control Interface. The audit configuration settings can be selected from the menu items on the left-hand side (see Figure 2).

5.1 Auditing control

The audit configuration parameters to consider are found in the Network Configuration page shown in Figure 2. Note that some of the following options are only available to users who have purchased the Enterprise Agents, as not all features are part of the OpenSource toolset.

From version 4.2.0 of the Snare for Windows agent the Network Configuration page includes various settings appended to each parameter, for example (SGP), (AGP), (LR), (D) explained in Group Policy.

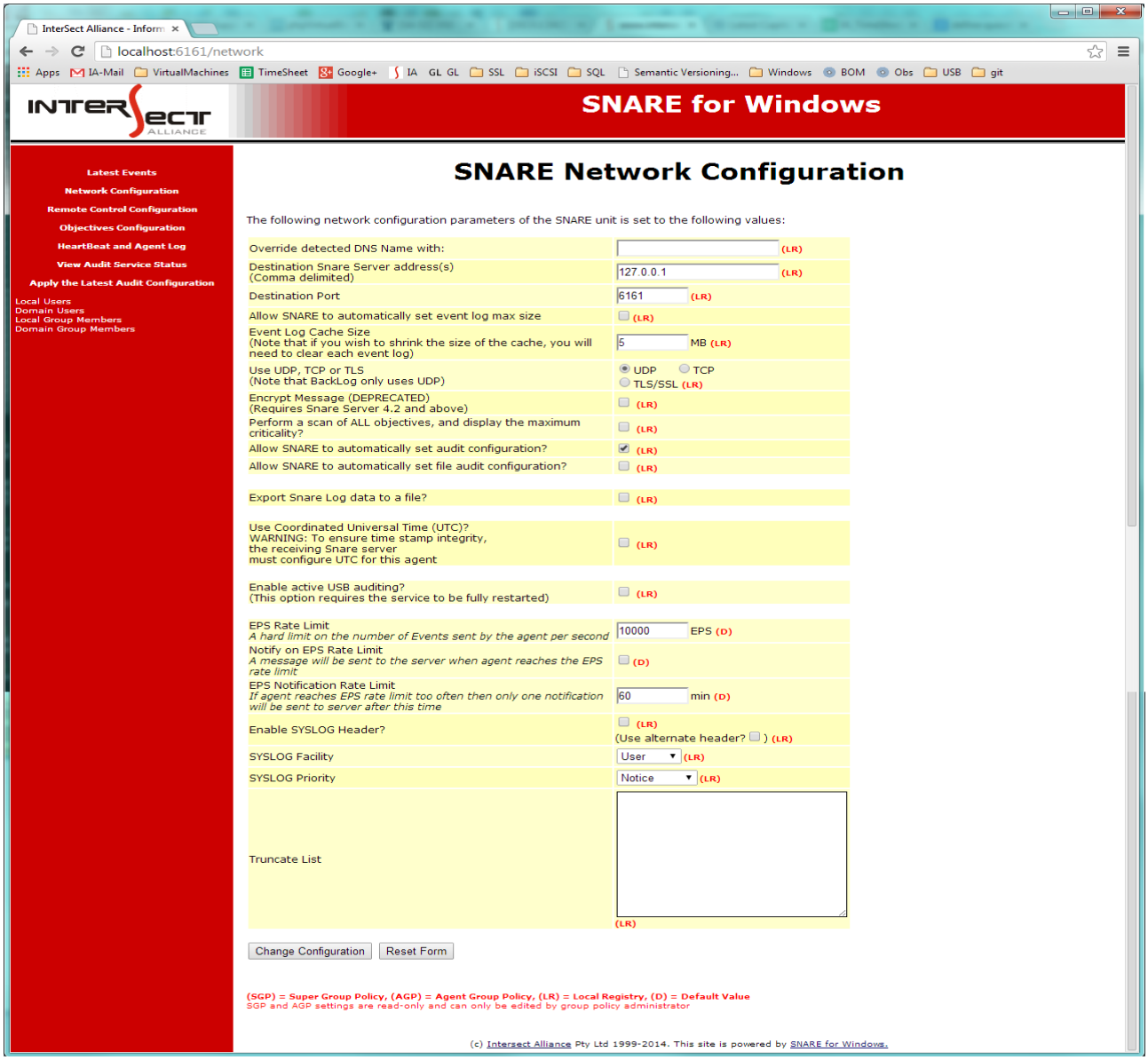


Figure 2 Network Configuration Window

- ***Override detected DNS Name with:*** Can be used to override the name that is given to the host when Windows is first installed. Unless a different name is required to be sent in the processed event log record, leave this field blank and the SnareCore service will use the default host name set during installation. Note that executing the command hostname on a command prompt window will display the current host name allocated to the host.

  Dynamic DNS Names feature ***(ENTERPRISE AGENT ONLY)*** - The Enterprise Agent automatically re-queries the DNS server for any IP Address changes every ten minutes.

- ***Use Host IP Address Override for source address: [Available v4.3]***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.

- ***Destination Snare Server address(s):*** The ability to send events to multiple hosts is only available to Enterprise Agents. The name or IP address can be entered and comma delimited when several addresses are required.
- ***Destination Port:*** Snare Server users should only send events to port 6161 in native UDP or TCP, or 6163 for TLS/SSL. To send data via Syslog port 514 is recommended unless the destination is configured differently to receive on a non standard UDP port. To configure rsyslog to use TLS/SSL encrypted messages refer to http://www.rsyslog.com/doc/rsyslog_tls.html .
- ***Allow SNARE to automatically set event log max size (ENTERPRISE AGENT ONLY):*** Select this option to set the event log cache size.
- ***Event Log Cache Size (ENTERPRISE AGENT ONLY):*** Modify the default Windows event log size, allowing you to easily configure the desired cache size. Combined with TCP or TLS/SSL, this option will allow the agent to cache messages if there is a network failure or the destination server is otherwise unavailable. Ensure the ***"Allow SNARE to automatically set event log max size"***check box is set.
- ***Use UDP, TCP (ENTERPRISE AGENT ONLY) or TLS (ENTERPRISE AGENT ONLY):*** Select the protocol you would like the agent to use when sending events. Using TCP will provide reliable message delivery. UDP by the protocol nature may result in messages being lost and not captured by the syslog destination server. TLS/SSL will encrypt a TCP connection to the destination server, protecting messages from eavesdropping while in transit. For TLS/SSL, the TCP feature TCP_NODELAY is enabled, and prevents TCP buffering by the Operating System, thereby reducing the lag when the agent is sending events via TCP.
- ***Encrypt Message (ENTERPRISE AGENT ONLY):*** Relevant to users of Snare Server version 4/5. Encrypt messages between the agent and a Snare Server. This option requires matching Remote Access Passwords on both the agent and the Snare Server. This feature has been deprecated in favour of TLS/SSL support which provides stronger encryption.
- ***Perform a scan of ALL objectives, and display the maximum criticality?:*** Enabling this setting will cause the agent to scan through each defined objective, and save the highest criticality value encountered. The event will be sent with this criticality value. Turning off this option will send the event as soon as ONE match is detected, which may reduce the CPU usage of the Snare agent, but the criticality value may not be the highest possible value. Users of the 'Snare Server' software can safely choose to ***turn off*** this option, as the Snare Server does not use the Windows criticality value.
- ***Allow SNARE to automatically set audit configuration?:*** For effective auditing it is recommended that the audit configuration parameter shown in Figure 2 is enabled.

  Event Log Retention. There is a risk in event auditing, that the Windows event logs may fill up. If this is the case, then no further events are able to be read and the auditing function effectively stops. If the **"Allow SNARE to automatically set audit configuration"** checkbox is set then Snare will set all the event logs to overwrite the logs as required. This will therefore prevent the event log sub-system from stopping. To prevent the agent from modifying the retention settings, use the *LeaveRetention* registry value defined in *Appendix B - Snare Windows registry configuration description*.

  Auditing of Categories. If the **Allow SNARE to automatically set audit configuration**

checkbox is set then the system will also select the required event log parameters to meet those objectives (see below) which have been set. This will alleviate any problems associated with ensuring that the correct audit event categories have been selected, based on those event IDs which are required to be filtered. This is also the most optimized setting in terms of system performance.

NB: VERY IMPORTANT: IF YOU DO NOT SELECT THIS OPTION AND/OR THE WINDOWS ACTIVE DOMAIN GROUP POLICIES OVERWRITE THE AUDIT SETTINGS, THEN YOU WILL NEED TO MANUALLY ENSURE THAT THE WINDOWS AUDIT SETTINGS MATCH YOUR DESIRED OBJECTIVE CONFIGURATION.

- ***Allow SNARE to automatically set file audit configuration?:*** Enables the file system auditing to be controlled by the Snare objective settings. In order for Windows to collect file and registry access records, not only must the correct audit category be selected, but also the correct object auditing parameters must also be set. Setting this field will automatically set these parameters, based on the objectives which have been set. It is highly recommended that this checkbox be selected.

  For *file auditing*, enter the target file or directory into the General Search Term of the objective, e.g. c:\payroll\.

  For *registry auditing* (HKEY_LOCAL_MACHINE only), enter "MACHINE\keyname" into the General Search Term of the objective, e.g. MACHINE\SOFTWARE\InterSect Alliance\AuditService, as shown in Figure 3.

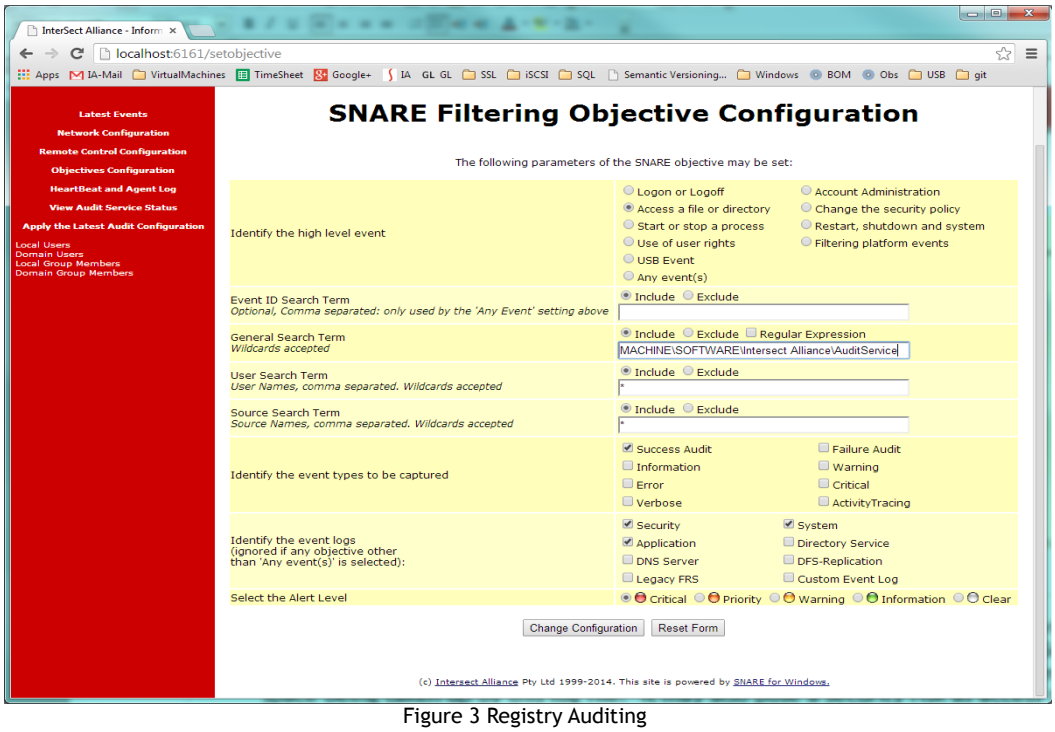
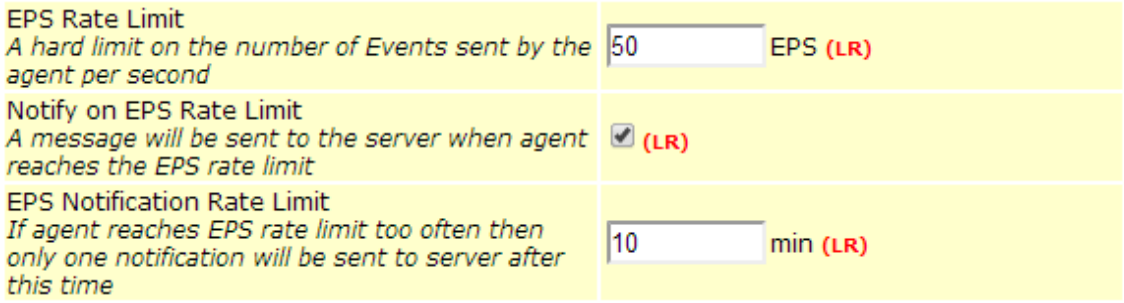


Figure 3 Registry Auditing

- ***Export Snare Log data to a file?:*** Log events to a file (separate to the event viewer log files). Note that if this selection is made the log files must be managed, since Snare will not rotate or otherwise manage these files. Failure to do so may result in a huge amount of disk space being taken up by this log file. It may also pose a security risk as access to the file will

need to be managed. The log can be found in system32 directory, e.g. c:\windows\system32\LogFiles\Snare.

- ***Use Coordinated Universal Time (UTC)?: (ENTERPRISE AGENT ONLY)*** Enables UTC timestamp format for events instead of local machine time zone format.
- ***Enable active USB auditing?: (ENTERPRISE AGENT ONLY)*** A series of plug and play and drive events can be captured and managed by an objective. A new objective is required to capture USB events as USB events will NOT be captured by default.
- ***EPS Rate Limit: (ENTERPRISE AGENT ONLY)*** 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. For example, if EPS rate limit is set to 50 (as below) then Snare for Windows will only send maximum 50 log messages in a second to any destination server.
- ***Notify on EPS Rate Limit: (ENTERPRISE AGENT ONLY)*** 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: (ENTERPRISE AGENT ONLY)*** 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. For example, if EPS notification rate limit is set to 10 minutes then only one EPS notification message will be sent to destination server(s) regardless of how many times Snare for Windows reaches the EPS rate limit.



- ***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. Is there a requirement to incorporate a SYSLOG header? Some SYSLOG services cannot correctly parse our default SYSLOG header, so an alternative header **Use alternate header?** is also available ***(ENTERPRISE AGENT ONLY)***. Selecting this option is recommended with ArcSight and other SIEM systems. Snare Server users should only send events to port 6161, or 6163 for TLS/SSL, and should NOT enable this option.
- ***SYSLOG Facility:*** Specifies the subsystem that produced the message. The list displays default facility levels that is compatible with Unix.
- ***SYSLOG Priority:*** If 'SYSLOG' is used, the agent can be configured to use a static, or dynamic priority value. 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. (Note you may wish to ensure the "'***Perform a scan of ALL objectives, and display the maximum criticality?"*** checkbox is also selected).

- ***Truncate List: (ENTERPRISE AGENT ONLY)*** Some events generated by windows can be triggered often and contain verbose information which may not be of much interest to the audit subsystem. To reduce the load on the target servers, these events may be truncated. This means the event isn't discarded from an audit point of view, but reduces the amount of unnecessary message detail sent across the network. Each line in this text box will compare to each event text and begin the truncation from the *first* character of the match.

For example placing the following text in the text box:

```
to complete the installation
```

would cause an event like below:

```
Windows update Hotfix for Windows (KB2664825) requires a computer restart to
complete the installation. (Command line: ""C:\windows\SysNative\wusa.exe"
"C:\ProgramData\Package
Cache\9F35FB1FD995814D2F4FDEB95A5D8B40F8F499A6\packages\localdbMsu\Windows6.1-
KB2664825-v3-x64.msu" /quiet /norestart")
```

to become:

```
Windows update Hotfix for Windows (KB2664825) requires a computer restart
<truncated 222 bytes>
```

5.2 Objectives Configuration

A major function of the Snare system is to filter events. This is accomplished via the advanced auditing 'objectives' capability. Any number of objectives may be specified and are displayed on the **Objectives Configuration** page (Figure 4). These objectives will be processed by the agent in the order they appear, that is, top to bottom. Use the up and down arrows in the **Order** column to reorganize your objectives into the appropriate order. An objective may be viewed or modified within the **Create or Modify an Objective** page as shown in Figure 5.

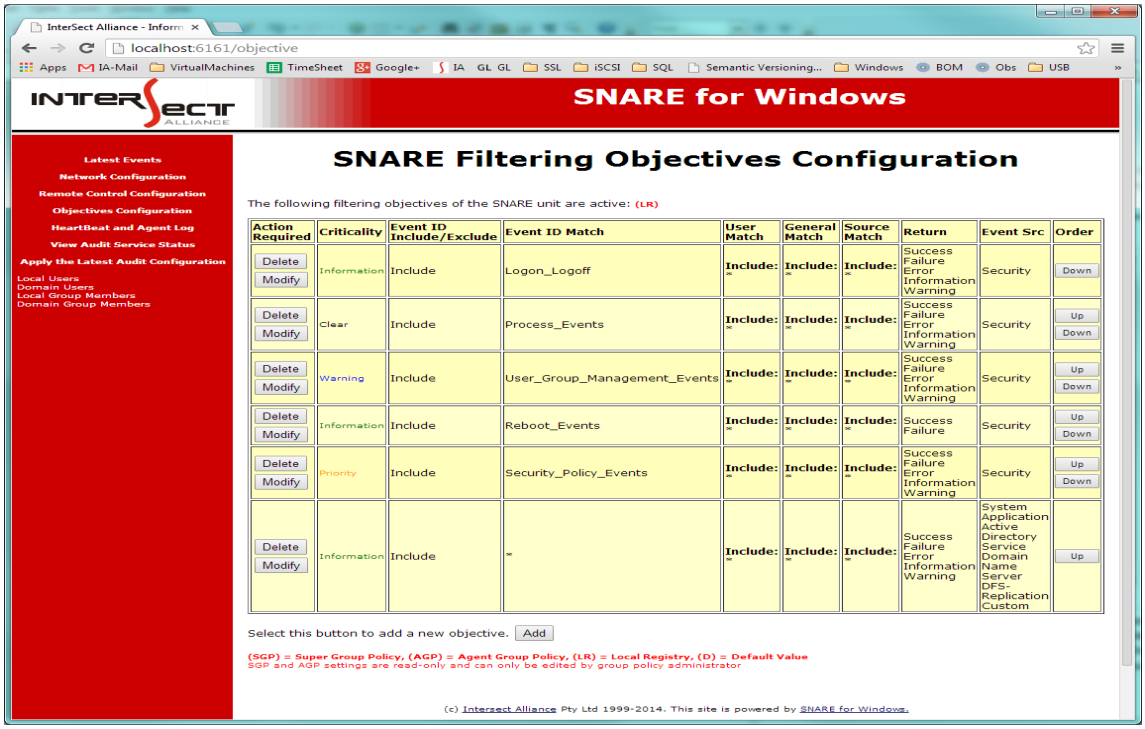


Figure 4 Objectives Configuration

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. Only **Windows Security Event Log** events are contained within the high level groups. Details on which Windows Event Log event IDs are used to generate the following objectives can be found in *Appendix C - Objectives and security event IDs* *on page 52:*

- Logon or Logoff.
- Access a file or directory.
- Start or stop a process.
- Use of user rights.
- Account administration.
- Change the security policy.
- Restart, shutdown and system.
- USB events
- Any event(s)

Note that the groups above are provided to service the most common security objectives that are likely to be encountered. If other event types are required, then the **Any event(s)** objective will allow fully tailored objectives to be set. From each of these groups, a level of importance can be applied. These criticality levels are **critical**, **priority**, **warning**, **information** and **clear**. These security levels are provided to enable the Snare user to map audit events to their most pressing business security objectives and to quickly identify the criticality of an event via the coloured buttons on the Snare remote control interface, on the Objective Configuration page as shown in Figure 5.

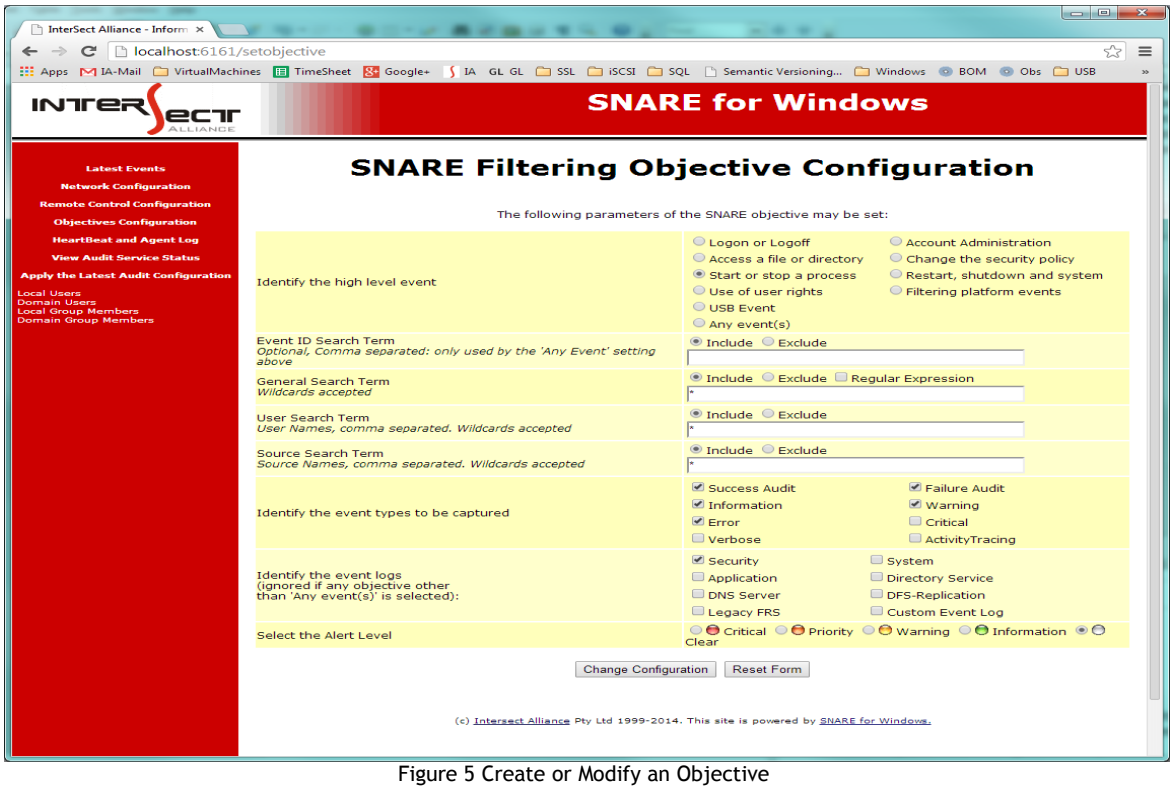


Figure 5 Create or Modify an Objective

The following filters can be applied to incoming audit events:

- Filter on the **EventID Match Type** field
  This allows the user to select whether to include or exclude messages that match this objective. If an objective is set to 'Exclude', matching event logs will be immediately discarded. Please note, objectives are processed from the top of the list to bottom, so it is important to place any Exclude objectives at the top of the list to ensure unwanted events are discarded. Also ensure the **Perform a scan of ALL objectives** configuration option is disabled in the **Network Configuration** window.

- Filter on the **EventID Search Term** field
  Each event contains a unique number known as the **Event ID**. If the high level event **Any event(s)** is selected, then the user is able to filter on the EventID field. If multiple events are required, the user may enter the event IDs as a comma separated string. **Example:** 562,457,897. Using the wildcard character '*' will select all events. Use the wildcard with caution since ALL events will be collected and passed to the remote host. For all other high

level events, this field is ignored and automatically managed by the agent.

- **General Search Term** field
  This allows the user to further refine a search based on the event record payload. For most high level events, this option will search all the fields of an event record, except the header. For simple searches (i.e. not a regular expression), there is NO need to use the wildcard character at the start or end of this field as it is automatically added to the search term when the objective is saved. The exception to this rule is when the **Access a file or directory** high level event is selected and the A**utomatically set file audit configuration** option is enabled. In this situation, the **General Search** field is used to identify the file, directory or registry location that requires auditing.

  Example: To monitor for a file being opened for reading, the objective **Access a file or directory** would be selected and the actual directory would be entered into this field as follows: **C:\Example**\. The agent will then recursively apply auditing to the destination folder, ensuring that any files or directories below **C:\Example** would be subject to audit and trapped.

  Tip: If setting a file search parameter, it is important that the FULLY QUALIFIED directory name is entered so that the Snare system can set the appropriate auditing. For example, C:\TEMP\SECRET* will work, but SECRET* will not.

  The search string may be treated as a Perl Compatible Regular Expression if the checkbox is selected. This allows more powerful/refined text matching and targeted bjectives allowing sophisticated forensic analysis and reporting, particularly when small details get lost in noisy log environments. Some common useful regular expressions include:

  Event contains email address:
  ```
  ([a-z0-9_\.-]+)@([\da-z\.-]+)\.([a-z\.]{2,6})
  ```

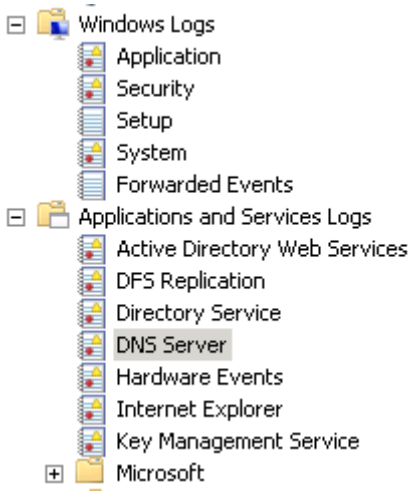
  Event contains URL:
  ```
  (https?:\/\/)?([\da-z\.-]+)\.([a-z\.]{2,6})([\/\w \.-]*)*\/?
  ```

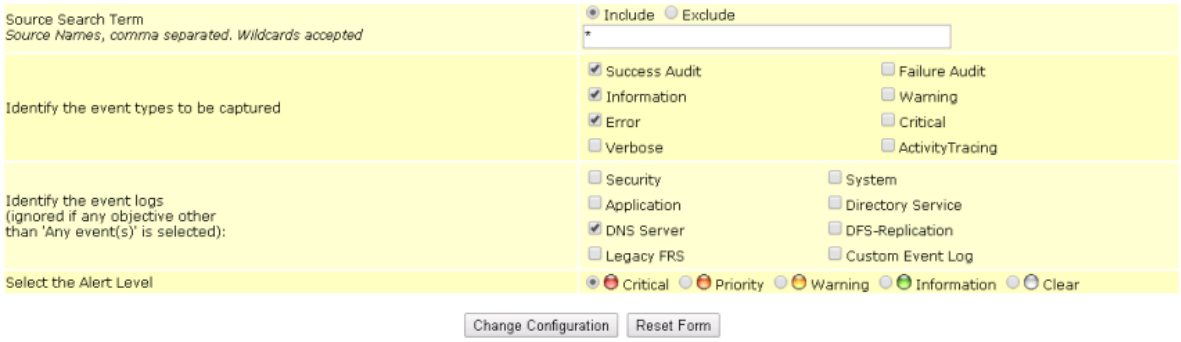
  Event contains IP address:
  ```
  (?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)
  ```

  Event contains hex-numbers:
  ```
  #?([a-f0-9]{6}|[a-f0-9]{3})
  ```

- **User Search Term**
  An event record may be selected or discarded based on a userid, or partial match of a userid. If no users are entered AND the **Include Search Term Users** radio button has been selected, then ALL users will be audited. If a term is entered in this field, then an event record will be trapped or discarded based on a valid match and whether the **Include** or **Exclude** radio buttons have been selected. There is no need to use the wildcard character at the start and end of this field as it is automatically added when the objective is saved. Multiple users may be entered using a comma separated list.

- **Source Search Term**
  This feature is relevant for Windows Vista/2008 and above, where much of the key information is buried in the Applications and Services logs. For example to include the events in DNS Server as displayed below, then the Source Search Term should be set to * and the Event Logs should be checked for DNS Server.

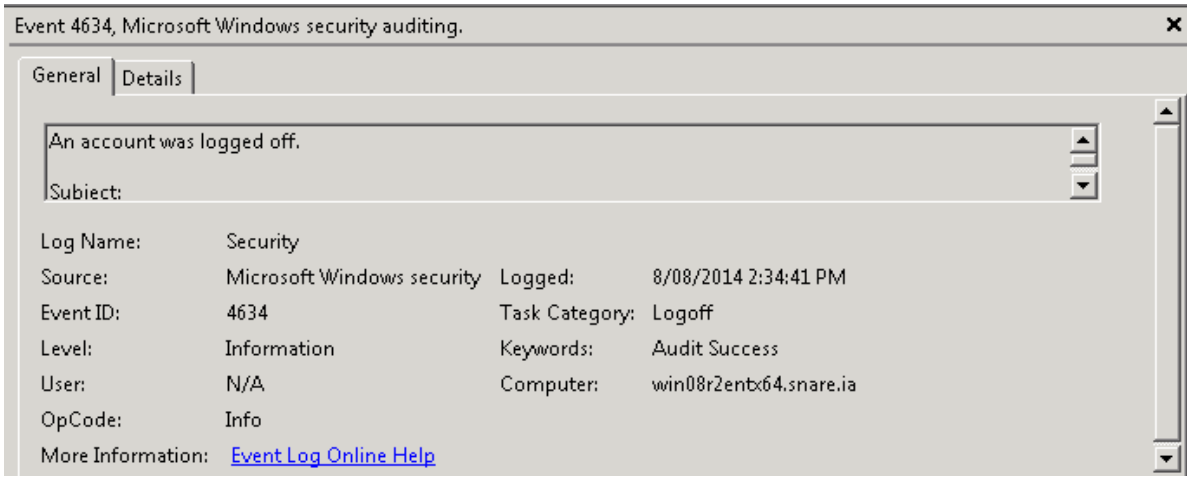




The Source column in Latest Events is composed of-the bold part is the Channel name eg DNS Server, followed by the Source Name eg Microsoft-Windows-DNS-Server-Service

	Date/Time	System	Event Count	EventID	Source	UserName	UserType	ReturnCode	Strings
	Fri Aug 08 14:15:17 2014	win08r2entx64.snare.ia	16007	7036 (None)	**System** Service Control Manager	N/A	N/A	Information	The DNS Server service entered the stopped state.
	Fri Aug 08 14:15:17 2014	win08r2entx64.snare.ia	16006	3 (None)	**DNS Server** Microsoft-Windows-DNS-Server-Service	N/A	N/A	Information	The DNS server has shut down.

- **Identify the event types to be captured**
  Windows uses many different audit event types, including Success Audit, Failure Audit, Information, Warning, Error, Critical, Verbose, Activity Tracing. Below is an example of a logged event in Event Viewer. The *Level:* field displays this event type as Information.



  If it is unclear which type of event is required, then selecting all of the check box0es will ensure that no events are lost. Note if none of the checkboxes are selected, then NO events will be trapped.

- **Identify the Event Logs**
  Windows collects logs from a number of event log sources. On Windows Servers, all six primary event logs may be found, however on pre-Vista Workstation installations only three of these event logs (Security, System and Application) are available. Collecting events from Windows Logs is available for OpenSource agents, however collecting logs for Custom Event Logs and Applications and Services Logs is ***only available with the Enterprise Agents***. Refer to the Windows Event Viewer in Figure 6.

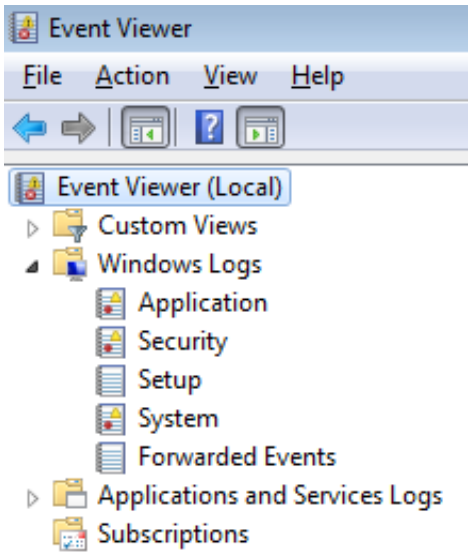
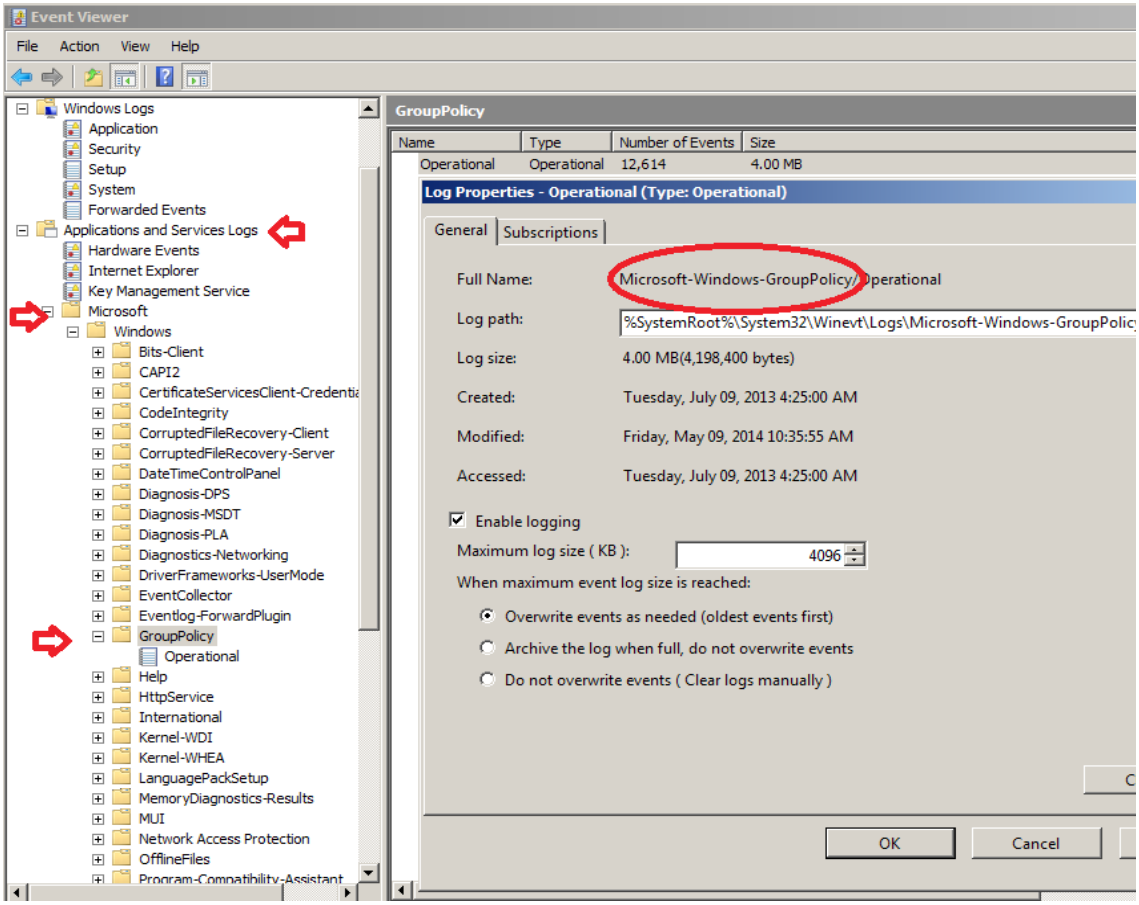


Figure 6 Windows Event Viewer

If in doubt, there will be no harm done in selecting all event log types, except that ***SnareCore*** will now read from, and attempt to filter, from all the selected event logs and this will have some slight negative performance impact. Please note, if any high level event except for **Any event(s)** is selected, then this item is ignored as it is set automatically by the high level event.

- ***Custom Event Log (ENTERPRISE AGENT ONLY)*** - For custom logs, when you create or modify an objective, you will need to select this check box and then specify the specific name of the log in the Source Search Term.

  To find the specific name, open the Event Viewer, browse to the event log you wish to capture, and open the Properties dialog. For example, the Group Policy as seen below. Here you will see the full name, e.g. Microsoft-Windows-GroupPolicy/Operational.



  You only need to enter the first part leading up to the forward slash in the Source SearchTerm, "Microsoft-Windows-GroupPolicy" in the Filtering Objective Configuration as shown below.

SNARE Filtering Objective Configuration

The following parameters of the SNARE objective may be set:

Identify the high level event	○ Logon or Logoff ○ Account Administration ○ Access a file or directory ○ Change the security policy ○ Start or stop a process ○ Restart, shutdown and system ○ Use of user rights ○ Filtering platform events ○ USB Event ◉ Any event(s)
Event ID Search Term *Optional, Comma separated: only used by the 'Any Event' setting above*	◉ Include ○ Exclude
General Search Term *Wildcards accepted*	◉ Include ○ Exclude ☐ Regular Expression *
User Search Term *User Names, comma separated. Wildcards accepted*	◉ Include ○ Exclude *
Source Search Term *Source Names, comma separated. Wildcards accepted*	◉ Include ○ Exclude Microsoft-Windows-GroupPolicy
Identify the event types to be captured	☑ Success Audit ☑ Failure Audit ☑ Information ☑ Warning ☑ Error ☑ Critical ☐ Verbose ☐ ActivityTracing
Identify the event logs (ignored if any objective other than 'Any event(s)' is selected):	☐ Security ☐ System ☐ Application ☐ Directory Service ☐ DNS Server ☐ DFS Replication ☐ Legacy FRS ☑ Custom Event Log
Select the Alert Level	◉ Critical ○ Priority ○ Warning ○ Information ○ Clear

Change Configuration | Reset Form

After saving your configuration, and as your expected events are logged, the latest events will then display the custom logs.

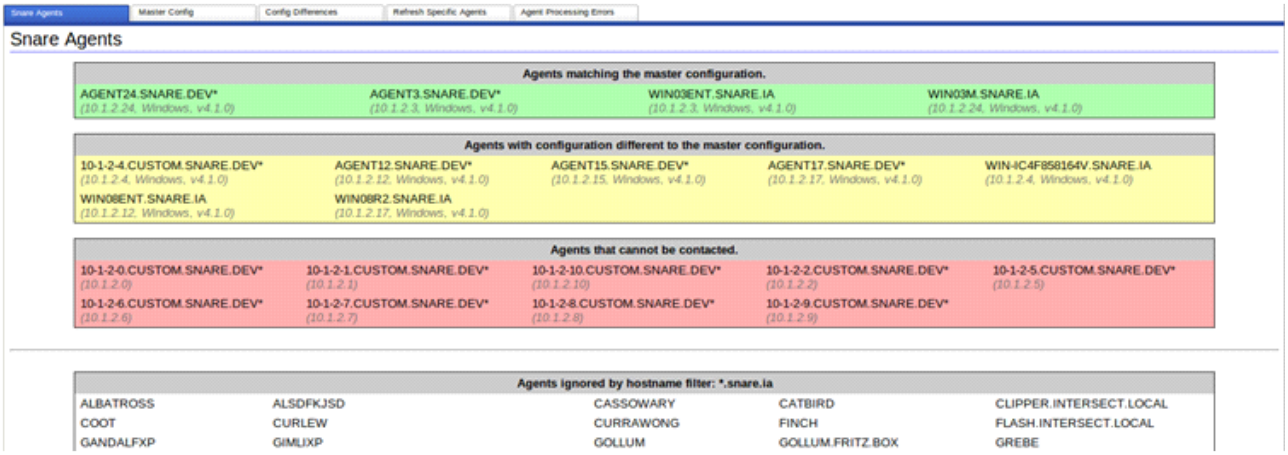
	Date/Time	System	Event Count	EventID	Source	UserName	UserType	ReturnCode	Strings
	Fri Aug 08 16:21:47 2014	win08r2entx64.snare.ia	13115	64 (None)	**Application** Microsoft-Windows-CertificateServicesClient-CertEnroll	NT AUTHORITY\SYSTEM	N/A	Information	Certificate enrollment for Local system successfully load policy from policy server
	Fri Aug 08 16:21:44 2014	win08r2entx64.snare.ia	13114	5315 (None)	**Microsoft-Windows-GroupPolicy/Operational** Microsoft-Windows-GroupPolicy	NT AUTHORITY\SYSTEM	N/A	Information	Next policy processing for SNARE\WIN08R2ENTX64$ will be attempted in 5 minutes.
	Fri Aug 08 16:21:44 2014	win08r2entx64.snare.ia	13113	8004 (None)	**Microsoft-Windows-GroupPolicy/Operational** Microsoft-Windows-GroupPolicy	NT AUTHORITY\SYSTEM	N/A	Information	Completed manual processing of policy for computer SNARE\WIN08R2ENTX64$ in 1 seconds.
	Fri Aug 08 16:21:44 2014	win08r2entx64.snare.ia	13112	5016 (None)	**Microsoft-Windows-GroupPolicy/Operational** Microsoft-Windows-GroupPolicy	NT AUTHORITY\SYSTEM	N/A	Information	Completed Security Extension Processing in 406 milliseconds.
	Fri Aug 08 16:21:44 2014	win08r2entx64.snare.ia	13111	4016 (None)	**Microsoft-Windows-GroupPolicy/Operational** Microsoft-Windows-GroupPolicy	NT AUTHORITY\SYSTEM	N/A	Information	Starting Security Extension Processing. List of applicable Group Policy objects: (Changes were detected.) Default Domain Controllers Policy Default Domain Policy
	Fri Aug 08 16:21:44 2014	win08r2entx64.snare.ia	13110	5016 (None)	**Microsoft-Windows-GroupPolicy/Operational** Microsoft-Windows-GroupPolicy	NT AUTHORITY\SYSTEM	N/A	Information	Completed Registry Extension Processing in 31 milliseconds.

Once the above parameter settings have been finalized for your Objective, click **OK** to save the configuration to the registry. To ensure the ***SnareCore*** service has received the new configuration, the ***SnareCore*** service MUST be restarted via the **Windows Services control panel** or via the **Apply the latest audit configuration** menu item in the Remote Control Interface.

5.3 Managing the Agent configuration

Snare Agent Management Console

The most effective and simplest way to configure the SnareCore service is to use the Snare web based Remote Control Interface, see *Chapter 8 - Network Control Interface*. If remote control is enabled, the process of configuring large numbers of agents can be further simplified by taking advantage of the Snare Server **Agent Management Console**. See *User Guide to the Snare Agent Management Console* on the Intersect Alliance website.



Manage Snare Agents from the Snare Server

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\AuditService** 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.

In the end of each setting, one of these characters are shown: (SGP), (AGP), (LR), (D). These are sources from where the setting can come and are explained as following.

- **Super Group Policy (SGP):** If different types of Snare agents (Snare for Windows, Snare Epilog, Snare for MSSQL) are running on a network then super group policy can be applied and all the agents 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).

Super group policy is useful when different types of Snare agents (Snare Epilog, Snare for Windows and Snare for MSSQL) are running on a network. Using super group policy, network domain administrators can update the settings of all types of Snare agents running on a network using Microsoft ® Group Policy Editor.
For example, network domain administrators can use Microsoft ® Group Policy Editor to update all types of Snare agents on network to send the log to Snare Server running at 10.1.1.1 on TCP port 6161. Once this super group policy is applied, all Snare agents will then send logs to Snare Server running at 10.1.1.1 on TCP port 6161.

Snare for Windows group policy is also useful when there is a need to update the settings of all Snare for Windows running in a network. Snare for Windows group policy only updates the settings of all Snare for Windows.
For example, network domain administrators can use Microsoft ® Group Policy Editor to update all Snare for Windows agents on network to send the log to Snare Server running at 10.1.1.1 on TCP port 6161. Once this Snare for Windows group policy is applied, all Snare for Windows agents will now send logs to the Snare Server running at 10.1.1.1 on TCP port 6161.

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 AuditService 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\AuditService\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\AuditService\Config"

                                PART !!"Override detected DNS Name with:" EDITTEXT EXPANDABLETEXT
                                        VALUENAME "Clientname"
                                END PART
                        END POLICY
                END CATEGORY   ;CONFIG_CATEGORY
```

6. Audit event viewer functions

Events collected by the agent that meet the filtering requirements as per the **Audit Configuration**, will be displayed in the 'Latest Events' window illustrated in Figure 7. 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 ***SnareCore*** service. This list will be empty if the agent has not yet found any matching events or if there has been a network problem and the agent has temporarily suspended event processing.

A key feature of the ***SnareCore*** service is that events are not stored locally on the host (except for events stored natively in the Windows event log), but rather sent out over the network to one or more remote hosts.

A summary version of the events is displayed on the 'Latest Events' window. The 'Latest Events' window is restricted to a list of 20 entries and cannot be cleared, except by restarting the agent. The status of the current network connection(s) to the log server is also displayed on this screen. The window will automatically refresh every 30 seconds.

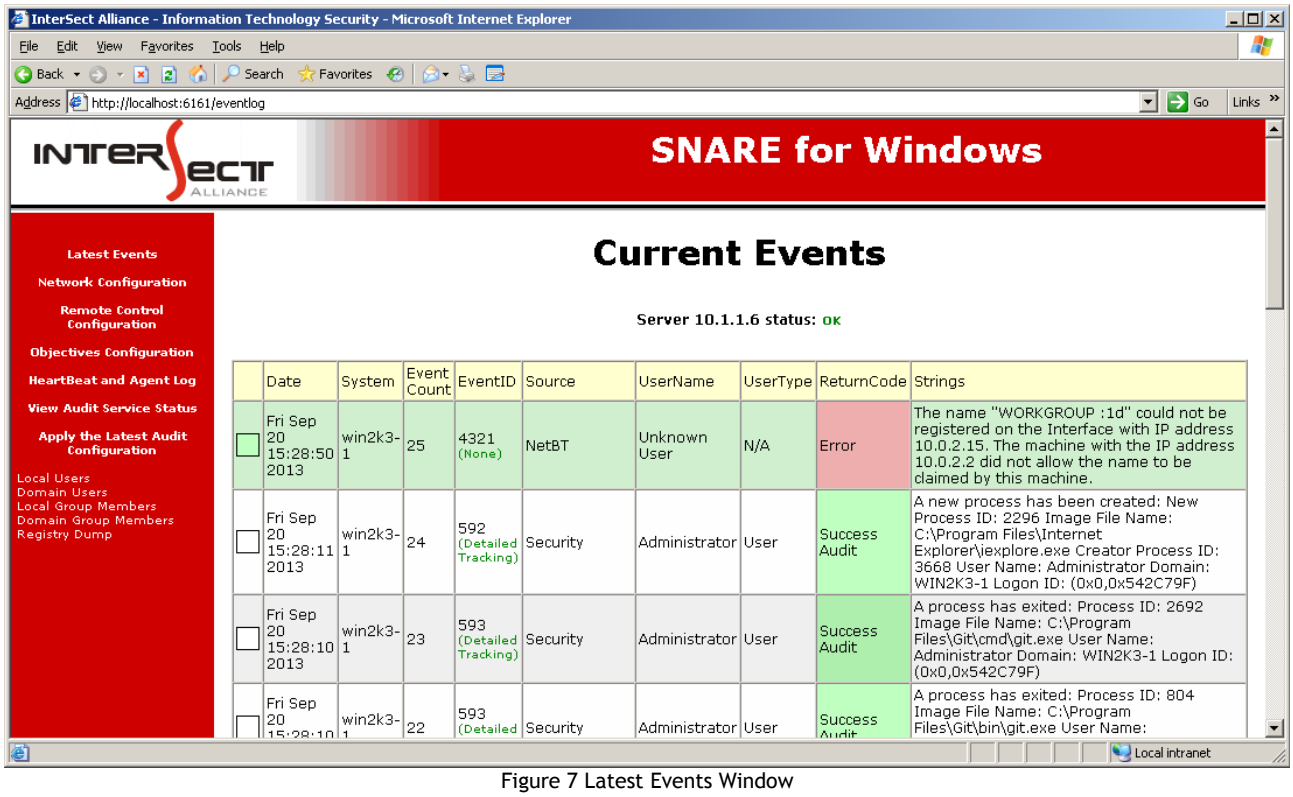


Figure 7 Latest Events Window

7. 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 8).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.

Figure 8 HeartBeat and Agent Log

8. Remote control and management functions

The ***SnareCore*** service is a separate, standalone component of the Snare system. The Snare Remote Control Interface can be used to interact with a number of aspects of its operation. Primarily, the interface is used to develop and set the audit, network and objectives configuration, as described in the previous sections, however, options are available to manage the ***SnareCore*** service.

The ***SnareCore*** service can be reloaded directly from the menu item **Apply the Latest Audit Configuration**. This will instruct the ***SnareCore*** service to re-read all the configuration settings, clear the buffers and essentially restart the service. This function is useful to apply any saved changes that have been made to the audit configuration. The user can therefore select when to activate a new configuration by selecting this menu item. Please note, this option does not restart the Windows service, but instead performs all the operations as if the service had been restarted.

The ***SnareCore*** service status can be viewed by selecting the **View Audit Service Status** menu item. This will display whether the ***SnareCore*** service is active as well as information relating to the architecture of the machine and the running binary file as shown in Figure 9 .

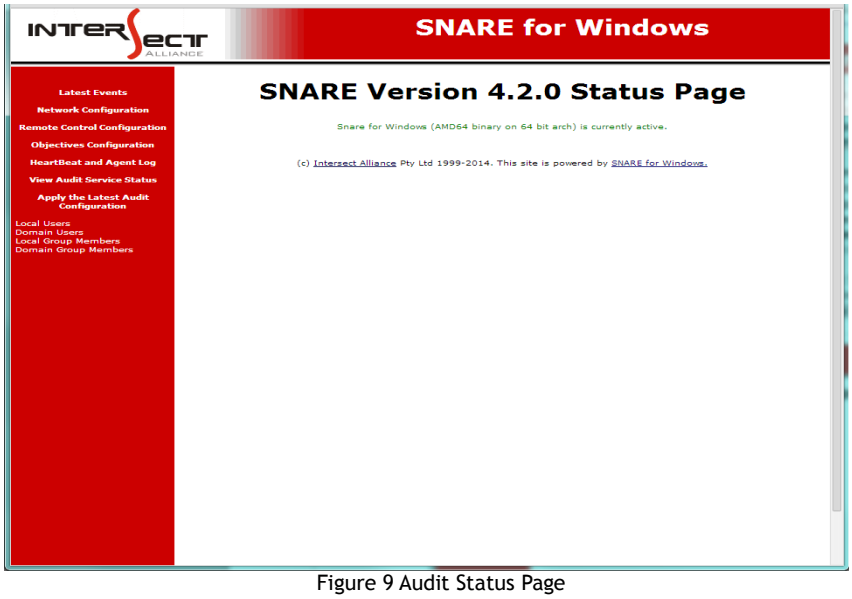


Figure 9 Audit Status Page

A significant function of the ***SnareCore*** service is its ability to be remote controlled. This facility has been incorporated to allow all the functions previously available through the front end Snare tool, to be available through a standard web browser. The ***SnareCore*** service employs a custom designed web server to allow configuration through a browser, or via an automated custom designed tool. The parameters which may be set for remote control operation are shown in Figure 10 and discussed in detail below:

- **Restrict remote control of SNARE agent to certain hosts**. This feature indicates whether to allow remote control of the Snare Agent. This option is also configurable at the time of installation. Enabling this option will allow the Snare Agent to be remote controlled from another machine via a web browser or the Snare Server's Agent Management Console. If the remote control feature is unselected, it may only be turned on by enabling the correct registry key on the hosted PC in which the Snare Agent has been installed.
- **IP Address allowed to remote control SNARE**. Remote control actions may be limited to a given host. This host, entered as an IP address in this field, will only allow remote connections to be effected from the stated IP address. Note that access control based on source IP address is prone to spoofing, and should be considered as a security measure used in conjunction with other countermeasures.
- **Require a password for remote control?** Indicate whether a password will be set so that only authorised individuals may access the remote control functions.
- **Password to allow remote control of SNARE**. If above checkbox is set, set the password. If accessing the remote control functions through a browser or custom designed tool, note that the userid is 'snare', and the password is whatever has been set through this setting. This password is stored in an encrypted form in the registry, using the MD5 hashing algorithm.
- **Change Web Server default (6161) port**. The default ***SnareCore*** web server port (6161) may be changed using this setting, if it conflicts with an established web server.
- **Web Server 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) 6161, then the user needs to type **http://mysite.com:6161** to reach the web server. Note the new server port, as it will need to be placed in the URL needed to access the Snare agent.

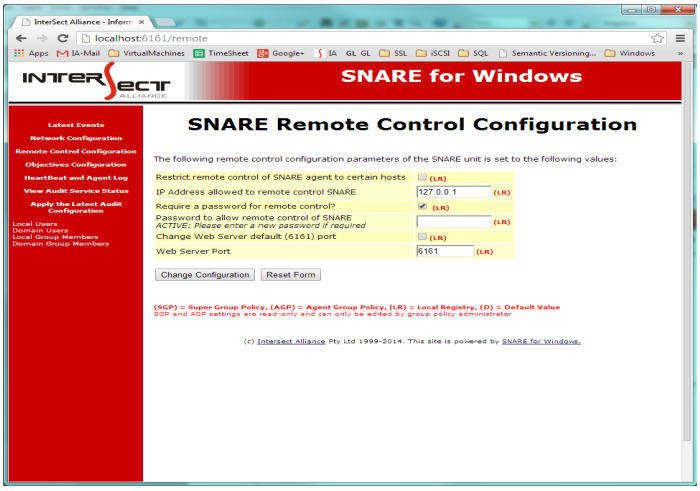


Figure 10 Remote Control Configuration

9. Retrieving user and group information

The ***SnareCore*** service also has the ability to retrieve local and domain users, groups and group membership from accounts local to the host that is running the agent and from the domain for which it is a member (if any). The host that is running the Snare agent must be a member of the domain, and have the ability to read user and group information, for the 'domain users/group' feature to work. This feature is available through the remote control web page and can be accessed through any standard web browser. The menu structure on the remote web pages (Figure 11) shows the selections:

- 'Local Users'
- 'Local Groups'
- 'Local Group Members'
- 'Domain Group Members'

*Note for advanced users only: There is a fifth option called “Registry Dump” which is disabled by default. This option will only be displayed if the DWORD registry key HKEY_LOCAL_MACHINE\SOFTWARE\InterSect Alliance\AuditService\Config\EnableRegDump exists and is set to 1.

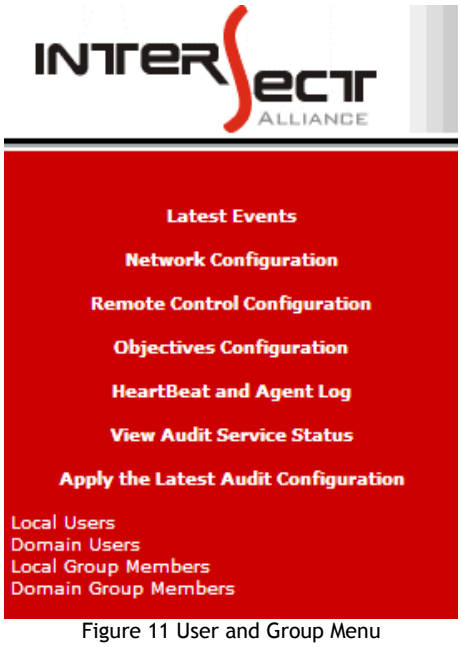


Figure 11 User and Group Menu

Selecting any of these items will then display the relevant details. For example, Figure 12 shows the output of selecting 'Local Users'. The output from these commands has been designed with no HTML markup to assist automated services, such as the Snare Server, to interrogate the users, groups and group membership.

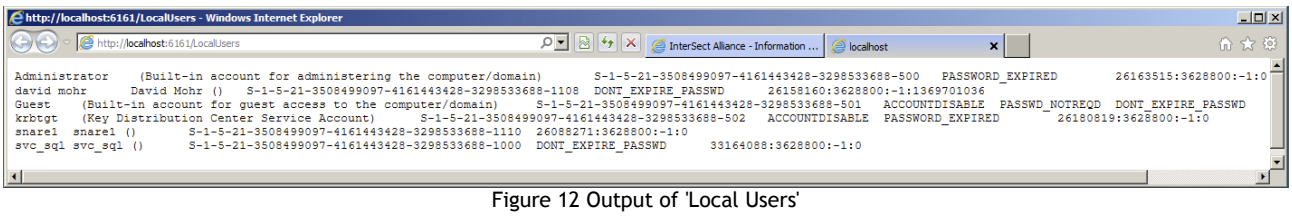


Figure 12 Output of 'Local Users'

In the case of 'Local Users' or 'Domain Users', the output shows a number of tab delimited entries, per line. These entries should be interpreted as follows:

Username; ***Description***; ***SID***; ***Attributes***; ***Settings***; These attributes include items such as Don't expire the password (token will be: DONT_EXPIRE_PASSWD); Account Disabled (token will be: ACCOUNTDISABLE); No Password (token will be: PASSWD_NOTREQD). The settings are "Password age in seconds since last reset : Maximum password age in seconds : Account Expiry as seconds elapsed since 00:00:00 1 January, 1970 (-1 means the account will not expire) : Last Logon". For DomainUsers, the Last Logon field will be the latest of LastLogon and LastLogonTimestamp across all Domain Controllers on the network.

The first three entries of username, description and SID will be displayed as a tab delimited list. The remaining tokens will only be shown if they exist in relation to a particular account. The settings will always appear at the end of each line.

In the case of Group Memberships, the attributes displayed are ***Groupname***; ***GID***; ***Group Members***. The group member list will be shown when selecting the 'Local Group Members' or 'Domain Group Members' menu item from the remote control web page. Additionally, the group members will be displayed as a comma separated list of usernames. As stated previously, the 'Domain Group Members' and associated membership displayed via the web browser will only be displayed if the host that is running the Snare agent is a member of a Windows domain.

10. 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 13 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.

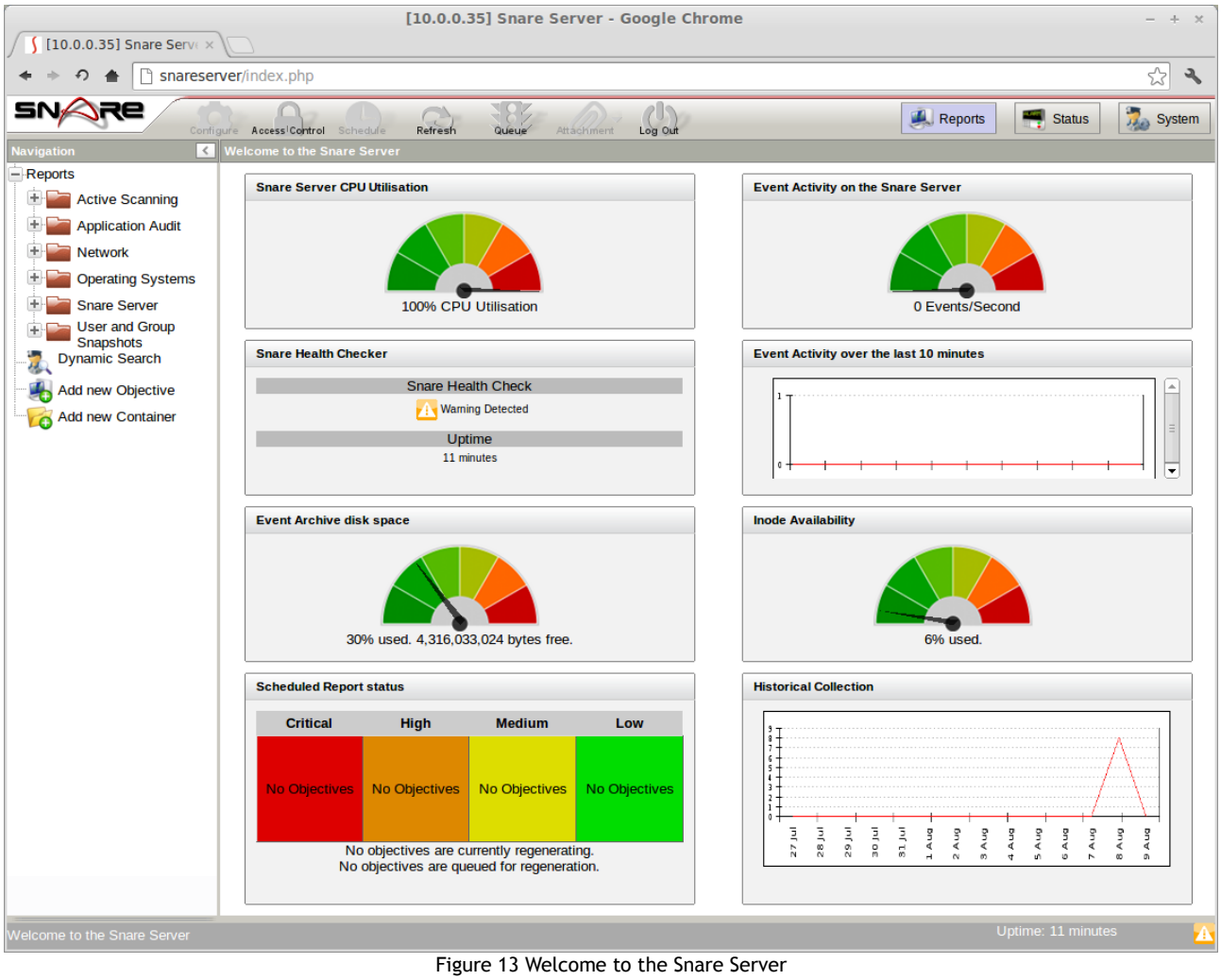


Figure 13 Welcome to the Snare Server

Some of the key features of the Snare Server include:

- Ability to collect any arbitrary log data, either via UDP or TCP
- Secure, encrypted channel for log data using TLS/SSL or 3DES
- 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 organisational 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.

11. 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 ***SnareCore*** service reads data from the Windows operating system via the Event 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 ***SnareCore*** service has SYSLOG header functionality active.

Example:

Test_Host MSWinEventLog 0 Security 3027 Fri May 24 20:30:43 2010 593 Security Administrator User Success Audit LE5678WSP Detailed Tracking A process has exited: Process ID: 656 User Name: Administrator Domain: LE5678WSP Logon ID: (0x0,0x6C52)

The format of the event log record is as follows:

1. **Hostname** (the assigned hostname of the machine or the override value entered using the Snare front).
2. **Event Log Type**. Fixed value of 'MSWinEventLog'.
3. **Criticality**. This is determined by the Alert level given to the objective by the user and is a number between 0 and 4, as detailed in the registry settings in Appendix B.
4. **SourceName**. This is the Windows Event Log from which the event record was derived. In the above example, the event record was derived from the 'security' event log.
5. **Snare Event Counter.** Based on the internal Snare event counter. Rotates at '*MAXDWORD*'.
6. **DateTime**. This is the date time stamp of the event record.
7. **EventID**. This is the Windows Event ID.
8. **SourceName**. This is the Windows Event Log from which the event record was derived. In the above example, the event record was derived from the 'security' event log.
9. **UserName**. This is the Window's user name.
10. **SIDType**. This is the type of SID used. In the above example, it is a 'User' SID, but it may also be a 'computer' or other type of SID.
11. **EventLogType**. This can be anyone of 'Success Audit', 'Failure Audit', 'Error', 'Information', or 'Warning'.
12. **ComputerName**. This is the Windows computer name.
13. **CategoryString**. This is the category of audit event, as detailed by the Windows event logging system.
14. **DataString**. This contains the data strings.
15. **ExpandedString**. This contains the expanded data strings.
16. **MD5 Checksum** (optional). An md5 checksum of the event can optionally be included with each event sent over the network by the Snare for Windows agent. Note that the application that evaluates each record will need to strip the final delimiter, plus the checksum, prior to evaluating the event.

Appendix B - Snare Windows 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\AuditService** and this location may not be changed. If the configuration key does not exist, the ***SnareCore*** service will create it during installation, but will not actively audit events until a correctly formatted objective(s) is present. These settings can be overridden using Group Policy settings located at **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Intersect Alliance\AuditService** using exactly the same settings and structure described below.
Snare can be configured in several different ways, namely:

- Via the remote control interface (Recommended).
- By manually editing the configuration items in the registry (NOT Recommended).
- Using the Snare Server's Agent Management Console.
- Via Group Policy Objects to target the aforementioned Policies key location.

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

`[Config]`	This subkey stores the delimiter and clientname values.
`Audit`	This value is of type REG_DWORD, and determines whether Snare is to automatically set the system audit configuration. Set this value to 0 for no, or 1 for Yes. Will default to TRUE (1) if not set. The audit configuration includes selecting the audit categories and the retention policy on ALL event log files.
`Checksum`	This value is of type REG_DWORD, and determines whether Snare is includes an MD5 Checksum of the contents of each audit record, with the record in question. Set this value to 0 for no, or 1 for Yes. Will default to FALSE (0) if not set. Note that the checking application will need to strip the final delimiter, plus the MD5 Checkum, from the record before evaluating the record against the checksum.
`Clientname`	This is the Hostname of the client and is of type REG_SZ. If no value has been set, "hostname" command output will be displayed. Must be no more than 100 chars, otherwise will truncate.
`CritAudit`	This value is of type REG_DWORD, and determines whether Snare will only send an event for the highest criticality match

Delimiter	This is of type REG_SZ and 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.
EnableRegDump	This value is of type REG_DWORD and determines whether a link to 'Registry Dump' appears on the main GUI display. Set this value to 1 to allow access to the link. If this is set to any other value, or if the key itself is removed, the link will be obscured.
EnableUSB	This value is of type REG_DWORD, and determines whether Snare should actively capture USB auditing events (XP/2003/2008/2012 only). Set this value to 0 for no, or 1 for Yes. Will default to FALSE (0) if not set.
FileAudit	This value is of type REG_DWORD, and determines whether Snare is to automatically set the file system audit configuration. Set this value to 0 for no, or 1 for Yes. Will default to TRUE (1) if not set.
FileExport	This value is of type REG_DWORD, and determines whether Snare will write a log file to the system32 path. USE WITH CARE!!
LeaveRetention	This value is of type REG_DWORD and determines whether Snare should leave the existing Log Retention settings as they are on each event log. Set this value to 0 for no, or 1 for Yes. Will default to FALSE (0) if not set.
UseUTC	This value is of type REG_DWORD and determines whether Snare should use UTC timestamps instead of the local system time when sending events. Set this value to 0 for no, or 1 for Yes. Will default to FALSE (0) if not set.
[Objective]	This subkey stores all the filtering objectives.
Objective# (where # is a serial number)	This section describes the format of the objectives. Objectives are of type REG_SZ, of no greater than 1060 chars, and is composed of the following string (the figures in the brackets represent the maximum size of the strings that can be entered): Criticality(DWORD);Event Type (DWORD);Event Log Type(DWORD);EventID Match [256];General Match[512];UserMatchType(DWORD);User Match[256];EventIDMatchType(DWORD);GeneralMatchType(DWORD);SourceName Match [256];SourceNameMatchType(DWORD);TruncateList [2048]; Criticality - an integer between 0 and 4 that indicates

	the severity of the event. Critical = 4, Priority = 3, Warning = 2, Information = 1, Clear = 0 User Match Type: =0 (Include users that match user search term type; =1 for Exclude) EventID Match Type: =0 (Include events that match the entire objective; =1 for Exclude) Event Type: Success = 16, Failure = 8, Error = 4, Information = 2, Warning = 1. (These values are checkboxes, hence the sum of the selected values is recorded). Event Log Type: Custom = 64, Security = 32, System = 16, Application = 8, Directory Service = 4, DNS Server = 2, File Replication = 1. (These values are checkboxes, hence the sum of the selected values is recorded). The match terms (EventID Match, General Match and User Match) are the filter expressions and are defined to be any value (except TAB) which includes DOS wildcard characters. Note that these are NOT regular expressions with the exception of the General Match term. This has the option of interpreting the search string as a Perl Compatible Regular Expression by selecting the checkbox next to it. If it is not selected, the default simple search is used. NOTE: Semicolons are actually "TAB" characters.
`[Network]`	This subkey stores the general network configurations.
`CacheSizeM`	This value is of type REG_DWORD, and determines the size of the Windows Event Log (if CacheSizeSet is 1). The value must be between 1 and 1024. This feature only appears in supported agents.
`CacheSizeSet`	This value is of type REG_DWORD, and determines if the agent should set the Windows Event Log size (0 for No, 1 for Yes). This feature only appears in supported agents.
`Destination`	This sub key is of type REG_SZ and is 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	This value is of type REG_DWORD, and determines the Destination Port number. This value must be in 1-65535 range. Will default to 514 if a SYSLOG header has been specified.
EncryptMsg	This value is of type REG_DWORD, and determines if encryption should be used (0 for No, 1 for Yes). 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.
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.
Syslog	This value is of type REG_DWORD, and 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	This value is of type REG_DWORD, and determines the SYSLOG Class and Criticality. This value will default to 13 if not set, or out of bounds.
SocketType	This value is of type REG_DWORD, and determines the protocol used (0 for UDP, 1 for TCP, 2 for TLS/SSL). This feature only appears in supported agents.
TruncateList	This is a CRLF separated list of strings which result in event truncation if matched in the event text.
[Remote]	This subkey stores all the remote control parameters.
AccessKey	This value is of type REG_DWORD and is used to determine whether a password is required to access the remote control functions. It is set to either 0 or 1, with 0 signifying no password is required.
AccessKeySet	This is of type REG_SZ, and stores the actual password to be used, in encrypted format.

AccessKeySetSnare1	This is of type REG_SZ, and stores the DIGEST password to be used (username “snare”), in encrypted format.
AccessKeySetSnare2	This is of type REG_SZ, and stores the DIGEST password to be used (username “Snare”), in encrypted format.
AccessKeySetSnare3	This is of type REG_SZ, and stores the DIGEST password to be used (username “SNARE”), in encrypted format.
Allow	"Allow" is of type REG_DWORD, and set to either 0 or 1 to allow remote control If not set or out of bounds, will default to 0/NO (ie; not able to be remote controlled).
Restrict	This value is of type REG_DWORD, and set to either 0 or 1 to signal whether the remote users should be restricted via IP address or not. 0 = no restrictions.
RestrictIP	This is of type REG_SZ and is the IP address set from above.
WebPort	This value is 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	This value is of type REG_DWORD, and set to either 0 or 1 to signal whether the web port should be changed or not. 0 = no change.

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 Security Log event IDs and enable the user to create some of the more common objectives without having to know which event IDs they require. For each high level event, the Windows XP/2003 event IDs will be listed in blue and the Vista/2008/Windows7 and above event IDs will be listed in green. As a rule of thumb, to find the equivalent Windows XP/2003 event ID on a newer Windows operating system, just add 4096.

- **Logon of Logoff.**
  - 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 551, 552, 672, 673, 674, 675, 676, 677, 678, 680, 681, 682, 683
  - 4624, 4625, 4626, 4627, 4628, 4629, 4630, 4631, 4632, 4633, 4634, 4647, 4648, 4768, 4769, 4770, 4771, 4772, 4773, 4774, 4776, 4777, 4778, 4779, 4800, 4801, 4802, 4803
- **Access a file or directory.**
  - 560, 561, 562, 563, 564, 565, 566, 567, 594, 595
  - 4656, 4657, 4658, 4659, 4660, 4661, 4662, 4663, 4690, 4691
- **Start or stop a process.**
  - 592, 593, 594, 595
  - 4688, 4689, 4690, 4691
- **Use of user rights.**
  - 576, 577, 578, 608, 609
  - 4672, 4673, 4674, 4704, 4705
- **Account administration.**
  - 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671
  - 4720, 4721, 4722, 4723, 4724, 4725, 4726, 4727, 4728, 4729, 4730, 4731, 4732, 4733, 4734, 4735, 4736, 4737, 4738, 4739, 4740, 4741, 4742, 4743, 4744, 4745, 4746, 4747, 4748, 4749, 4750, 4751, 4752, 4753, 4754, 4755, 4756, 4757, 4758, 4759, 4760, 4761, 4762, 4763, 4764, 4765, 4766, 4767
- **Change the security policy.**
  - 516, 517, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 620, 643
  - 104, 1102, 4612, 4613, 4704, 4705, 4706, 4707, 4708, 4709, 4710, 4711, 4712, 4713, 4714, 4716, 4719, 4739
- **Restart, shutdown and system.**
  - 512, 513
  - 4608, 4609
- **USB Events.**
  - 1003,1004,1006,1008,2000,2001,2003,2004,2005,2006,2010,2100,2101,2102,2105,2106,2900,2901,4230,4231,7036

  Note: Events 4230 (Device ARRIVED) and 4231 (Device REMOVAL) are Snare specfic IDs. They are not part of the Windows event system.

- **Filtering Events.**
  - 5152, 5153, 5154, 5155, 5156, 5157, 5158, 5159, 5447

The above events will be generated by turning on selected audit categories, on the Windows audit sub-system. The following paragraphs detail the Snare for Windows event IDs and the categories to which they belong.

Audit Privilege Use (Success and Failure) will generate:
576;Special privileges assigned to new logon
577;Privileged Service Called
578;Privileged object operation
Audit Process Tracking (Success and Failure) will generate:
592;A new process has been created
593;A process has exited
594;A handle to an object has been duplicated
595;Indirect access to an object has been obtained
Audit System Events (Success and Failure) will generate:
514;An authentication package has been loaded
515;A trusted logon process has registered
516;Loss of some audits;
517;The audit log was cleared
518;A notification package has been loaded
Audit Logon Events (Success and Failure) will generate:
528;A user successfully logged on to a computer
529;The logon attempt was made with an unknown user name or bad password
530;The user account tried to log on outside of the allowed time
531;A logon attempt was made using a disabled account
532;A logon attempt was made using an expired account
533;The user is not allowed to log on at this computer
534;The user attempted to log on with a logon type that is not allowed
535;The password for the specified account has expired
536;The Net Logon service is not active
537;The logon attempt failed for other reasons
538;A user logged off
539;The account was locked out at the time the logon attempt was made
540;Successful Network Logon
541;IPSec security association established
542;IPSec security association ended
543;IPSec security association ended
544;IPSec security association establishment failed
545;IPSec peer authentication failed
546;IPSec security association establishment failed
547;IPSec security association negotiation failed
682;A user has reconnected to a disconnected Terminal Services session
683;A user disconnected a Terminal Services session without logging off
Audit Account Logon Events (Success and Failure) will generate:
672;An authentication service (AS) ticket was successfully issued and validated
673;A ticket granting service (TGS) ticket was granted
674;A security principal renewed an AS ticket or TGS ticket
675;Pre-authentication failed
676;Authentication Ticket Request Failed
677;A TGS ticket was not granted
678;An account was successfully mapped to a domain account

680;Identifies the account used for the successful logon attempt
681;A domain account log on was attempted
682;A user has reconnected to a disconnected Terminal Services session
683;A user disconnected a Terminal Services session without logging off
Audit Object Access (Success and Failure) will generate:
560;Access was granted to an already existing object
561;A handle to an object was allocated
562;A handle to an object was closed
563;An attempt was made to open an object with the intent to delete it
564;A protected object was deleted
565;Access was granted to an already existing object type
566;Object Operation
608;A user right was assigned
Audit Policy Change (Success and Failure) will generate:
609;A user right was removed
610;A trust relationship with another domain was created
611;A trust relationship with another domain was removed
612;An audit policy was changed
613;IPSec policy agent started
614;IPSec policy agent disabled
615;IPSec policy changed
616;IPSec policy agent encountered a potentially serious failure
617;Kerberos policy changed
618;Encrypted data recovery policy changed
620;Trusted domain information modified
768;A collision was detected between a namespace element in two forests
Audit Directory Service Access (Success and Failure) will generate:
565;Information about accessed objects in AD

Audit Account Management Events (Success and Failure) will generate:
624;User Account Created
625;User Account Type Change
626;User Account Enabled
627;Password Change Attempted
628;User Account Password Set
629;User Account Disabled
630;User Account Deleted
631;Security Enabled Global Group Created
632;Security Enabled Global Group Member Added
633;Security Enabled Global Group Member Removed
634;Security Enabled Global Group Deleted
635;Security Disabled Local Group Created
636;Security Enabled Local Group Member Added
637;Security Enabled Local Group Member Removed
638;Security Enabled Local Group Deleted
639;Security Enabled Local Group Changed
640;General Account Database Change
641;Security Enabled Global Group Changed
642;User Account Changed
643;Domain Policy Changed
644;User Account Locked Out

645;Computer object added
646;Computer object changed
647;Computer object deleted
648;Security Disabled Local Group Created
649;Security Disabled Local Group Changed
650;Security Disabled Local Group Member Added
651;Security Disabled Local Group Member Removed
652;Security Disabled Local Group Deleted
653;Security Disabled Global Group Created
654;Security Disabled Global Group Changed
655;Security Disabled Global Group Member Added
656;Security Disabled Global Group Member Removed
657;Security Disabled Global Group Deleted
658;Security Enabled Universal Group Created
659;Security Enabled Universal Group Changed
660;Security Enabled Universal Group Member Added
661;Security Enabled Universal Group Member Removed
662;Security Enabled Universal Group Deleted
663;Security Disabled Universal Group Created
664;Security Disabled Universal Group Changed
665;Security Disabled Universal Group Member Added
666;Security Disabled Universal Group Member Removed
667;Security Disabled Universal Group Deleted
668;Group Type Changed
669;Add SID History (Success)
670;Add SID History (Failure)

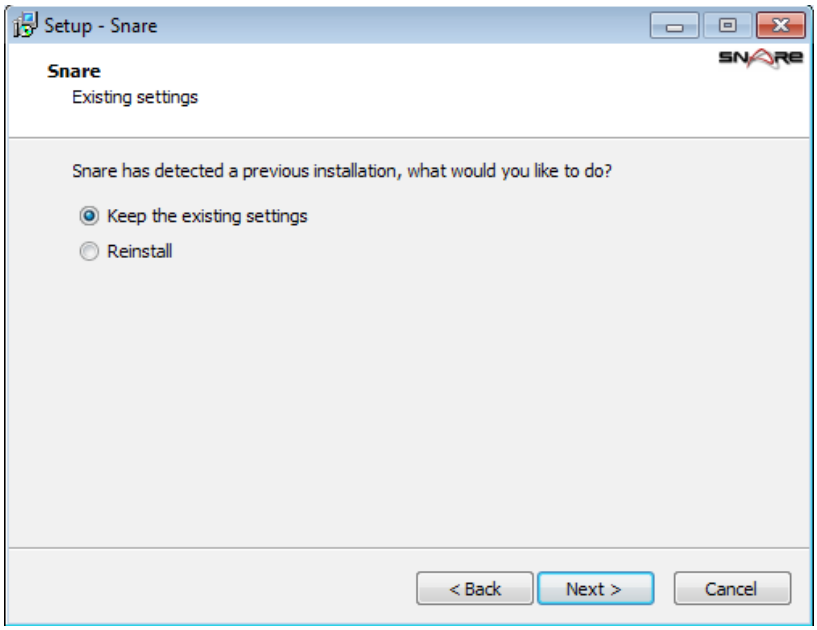
Appendix D - Upgrading an Evaluation Agent to the Enterprise Agent

This path is aimed at customers with the Snare Evaluation Agent for Windows installed, and after their purchase of the Enterprise version, would like to update their agents without losing their customised settings configured during their trial.

Download the SnareEnterpriseAgent-Windows-v*{Version}*-SUPP-MultiArch.exe file from the Intersect Alliance Secure Area website (where *{Version}* is the most recent version of the file available).

Ensure you have administrator rights, double-click the SnareEnterpriseAgent-Windows-v*{Version}*-SUPP-MultiArch.exe file. You will be prompted with the following screens:

1. Welcome to the Snare Setup Wizard screen- Select "Next" to continue the installation.
2. License Page - Select I ***accept the Agreement*** and click "Next".
3. Existing Install screen



4. The Wizard will detect the previous install of the Snare agent. Select ***Keep the existing settings*** to leave the agent configuration intact, and only update the Snare executable files.
5. Ready to Install screen – set the destination directory if required, and click "Install".
6. Information screen – click "Next.
7. Completing the Snare Setup Wizard page – click "Finish".