SNARE

System iNtrusion Analysis & Reporting Environment

Guide to
Snare Epilog for Windows
from v1.7

INTERSECT ALLIANCE

About this guide

This guide introduces you to the functionality of Snare Epilog with a Windows operating environment. The development of 'Snare Epilog for Windows' will now allow events found in text-based log files to be collected and forwarded to a remote audit event collection facility. Snare Epilog 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.
- Snare Server Installation Guide.
- 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* 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 *Agent Management Console* on page 23.

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

2 Overview of Snare Epilog for Windows

Epilog operates through the actions of a single component; the ***Epilog*** service based application (epilog.*exe*). The ***Epilog*** service interfaces with the Windows text-based log files to read, filter and send event logs to a remote host. The logs are filtered according to a set of objectives chosen by the administrator, and passed over a network, using the UDP or TCP protocol or optionally SSL/TLS encryption protocol to a remote server. *The TCP and SSL/TLS protocol capability, and the ability to send events to multiple hosts is only available to those users that have purchased the enterprise agent. See Chapter 8 of this document for further details.* The ***Epilog*** service is able to be remotely controlled and monitored using a standard web browser (see Figure 1 for an example screen), or via a custom designed tool.

The ***Epilog*** service reads event log data from the identified text files. ***Epilog*** appends a TAB delimited header to the string of the event log record, suitable for sending to a SYSLOG or Snare Server. This format, is further discussed in *Appendix A*. The net result is that a raw event, as processed by the Epilog service may appear as follows:

Example:

```
flash ApacheLog 0 10.0.3.2 - -[10/Aug/2006:16:10:00 +1000] "GET / HTTP/1.1" 200 44
```

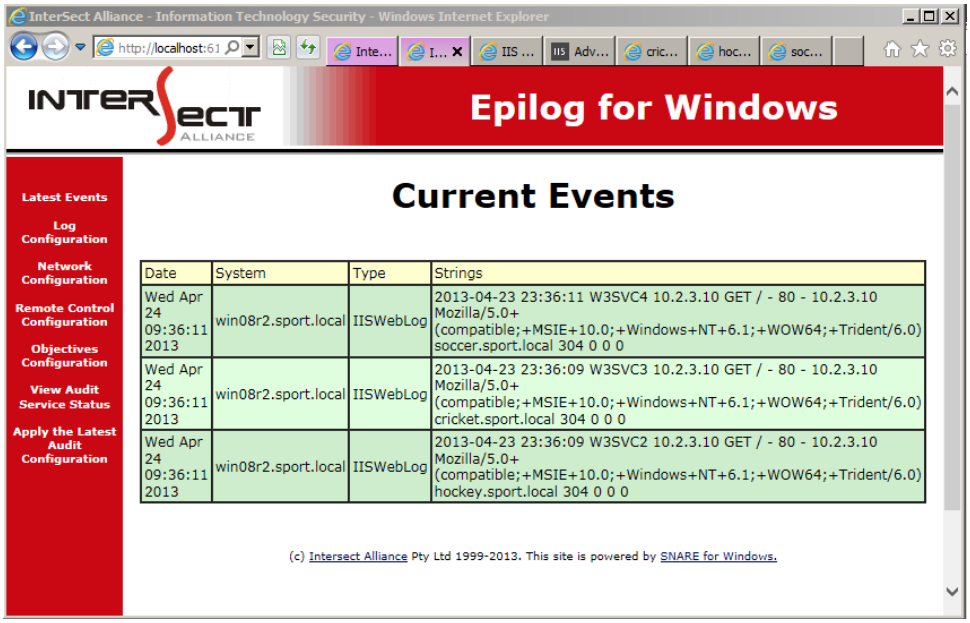


Figure 1 Main Event Window

3 Installing and running Epilog

Epilog is available in compressed format, and has been designed with an installation wizard to allow for easy installation and configuration of all critical components. The compressed file includes the major component of the agent, namely ***epilog*.exe.** The ***Epilog*** service is contained in the 'epilog.exe' binary. This binary contains all the programs to read the log records, filter the events according to the objectives, provide a web based remote control and monitoring interface, and provide all the necessary logic to allow the binary to act as a service defined in Windows.

3.1 Wizard Install

Download the **SnareEnterpriseEpilog-Windows-v*{Version}*-SUPP-MultiArch.exe** file from the Secure Site on the Intersect Alliance website where *{Version}* is the most recent version of the file available.

Ensure you have administrator rights, double-click the SnareEnterpriseEpilog-Windows-v*{Version}*-SUPP-MultiArch.exe file. This is a self extracting archive, and will not require WinZip or other programs. A series of screens will then be displayed, requesting that various parameters be set. Read these settings carefully, using this manual as reference. Most of the references are discussed later in this guide, so it pays to read this guide first, before installing the software.

The installation wizard will prompt the user to set a password for accessing the Remote Control Interface. It is strongly recommended that this setting is accepted and configured. The initial password dialog is shown inFigure 2. For further information on these fields:

- **"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.

    From version 1.8.0 the following settings are available:

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

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

  - **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.

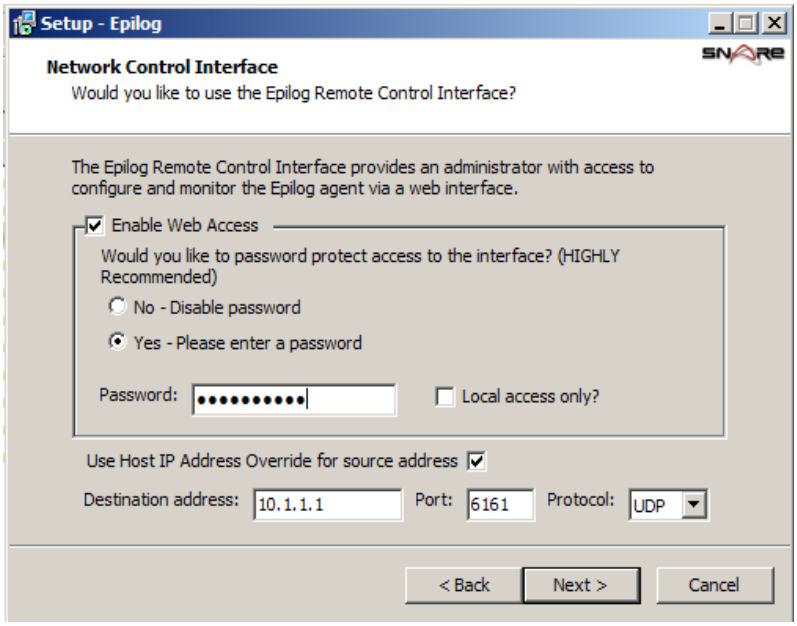


Figure 2 Epilog password dialog box

3.2 Silent Install

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

  From version 1.8.0 the following options are available:

- **/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 and execute the following commands:

   epilog -x
   Export the information and error messages, along with the INF file contents to the screen.

   epilog -x *INFfile*
   Export the information and error messages to the screen and write the INF file contents to a file e.g INFfile for use with the /LoadInf command line option.
5. Follow the prompts carefully and where required, enter the necessary password information for either the Service Account and/or the Sensitive Information encryption.
6. 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:

SnareEnterpriseEpilog-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 (e.g the INFfile) 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:

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

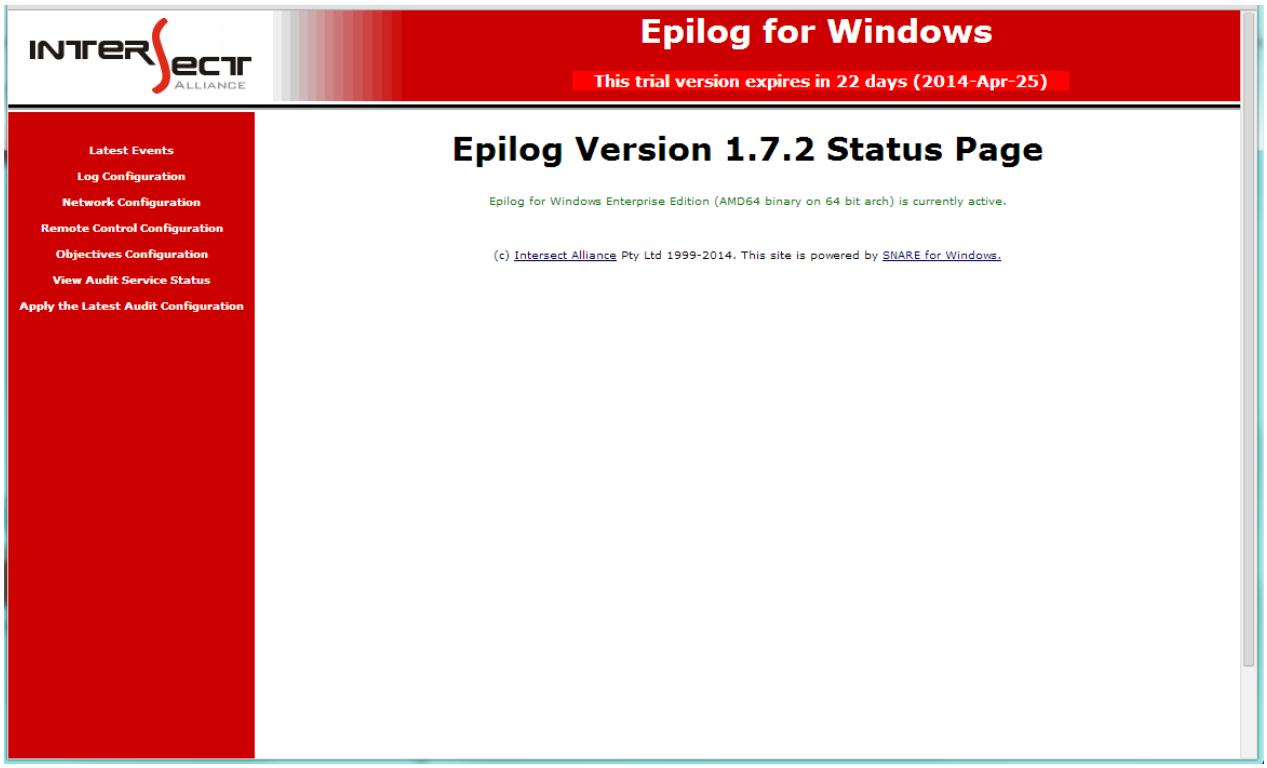
3.3 Running Epilog

Upon installation of the Epilog agent, an 'Intersect Alliance' menu item is installed off the **Program** main Windows menu. The Epilog remote control launch menu is then available from **Programs->Intersect Alliance->Epilog for Windows**. If the menu launcher is not available, the Epilog control interface may be accessed via a web browser from the local machine by visiting the URL **http://localhost:6162/**. If you previously configured a password, you will need this to log in, along with the username '*snare*'.

For events to be passed to a remote host, the ***Epilog*** service must be running. The ***Epilog*** service may be checked that it is active by selecting the Services item in Control Panel on older Windows NT hosts, or by selecting Services from the **Administrative Tools** or **Computer Management** menus. If Epilog is not running, double click on the service name, then select A**utomatic** 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.

3.4 Evaluation Version

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



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

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

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

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

4 Setting the audit configuration

The configurations for Epilog are 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 Epilog to successfully execute. Failure to specify a correct configuration will not 'crash' the ***Epilog*** service, but may result in selected events not being able to be read, and the system 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 Epilog 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 ***Windows registry configuration description***.

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

4.1 Logging control

The initial audit configuration parameters to consider are:

- The hostname, IP address and UDP port of the remote collection server. *Please note: The TCP and SSL/TLS protocol capability, and the ability to send events to multiple hosts is only available to those users that have purchased the Enterprise Agent. See Chapter 8 of this document for further details.*
- The requirement to incorporate a SYSLOG header. There are two header types available; the standard SYSLOG header used by Snare agents and an alternate header to assist message processing on some SYSLOG servers. Snare Server users should only send events to UDP or TCP port 6161. SSL/TLS configurations will sent to port 6163 on the destination server.
- Note that the following options are only available to users who purchase Enterprise Agents. These are not part of the Open Source tool set. See Chapter 8 below for more details on the supported versions of the Snare agents.
    - Use UDP or TCP – Select the protocol you would like Epilog to use when sending events. Using TCP will reliable message delivery.
    - Use SSL/TLS(ENTERPRISE AGENT ONLY) to encrypt or to protect the message contents over insecure networks.
    - Cache size – Allow Epilog to store messages that could not be sent. Combined with the TCP, this option will allow the agent to cache messages if there is a network failure or the Snare Server is otherwise unavailable. Any cached message is kept (even if the agent is restarted) until it is sent or the size of the cache exceeds the specified allotment, in which case the oldest message is removed.
    - Encrypt Message – This is for legacy support to encrypt messages between the agent and the Snare Server. This option requires matching Remote Access Passwords on both the agent and the Snare Server. This feature has been deprecated in favor of TLS/SSL support which provides stronger encryption.

- Use Coordinated Universal Time (UTC)?: (ENTERPRISE AGENT ONLY) Enables UTC timestamp format for events instead of local machine time zone format.

All of the aforementioned parameters are found in the **Network Configuration** window.

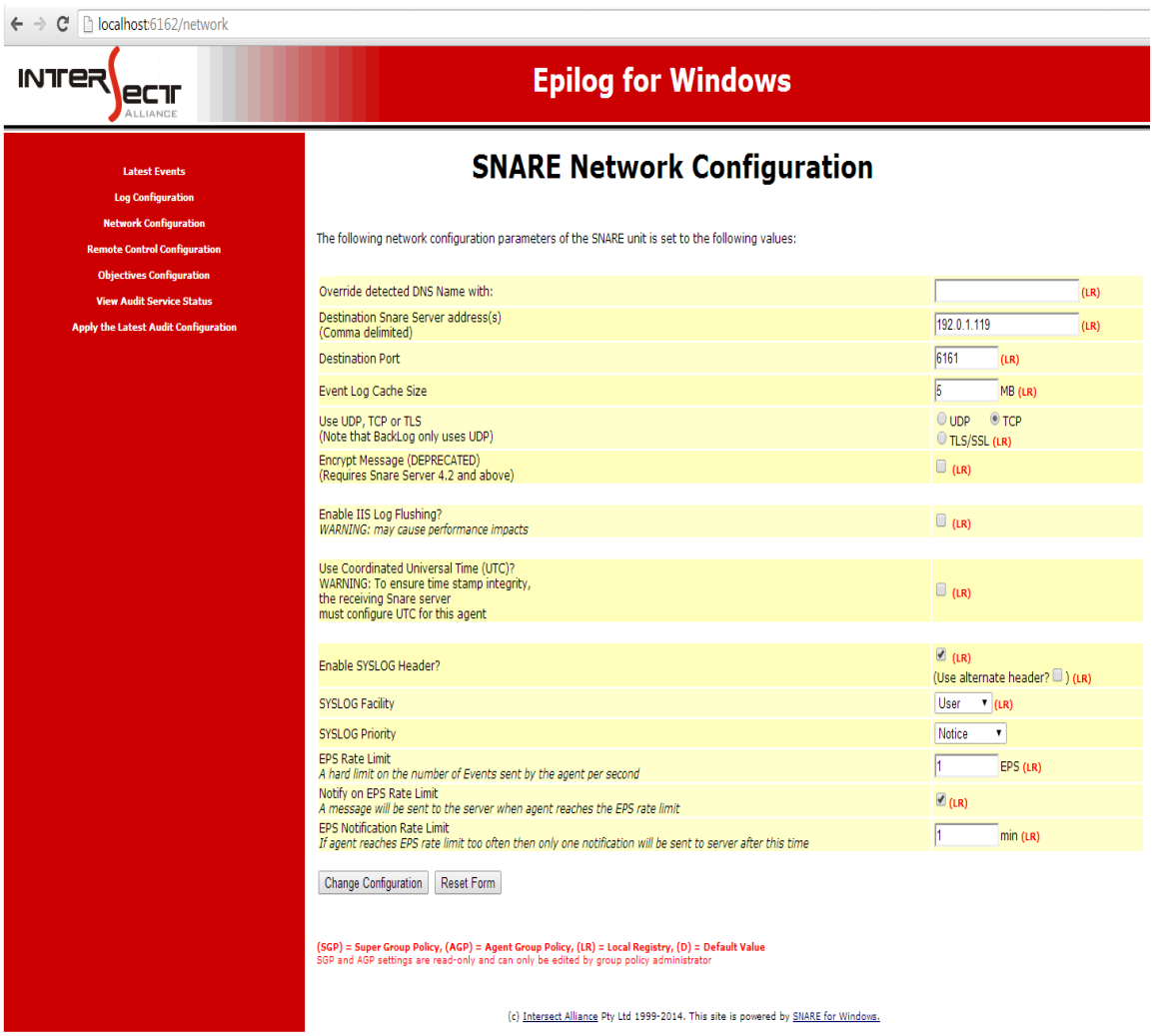


Figure 3 Network Configuration Window

The ***Override detected DNS Name*** field can be used to override the name that is given to the host when Windows is first installed. Unless a different name is required to be sent in the processed event log record, leave this field blank, and the ***Epilog*** 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.

From version 1.8.0, the following setting is available, ***Use Host IP Address Override for source address***. Enabling this setting will use the first network adapator as listed in the network configuration as the source of the IP address. The agent will periodically (about ten minutes) check this setting and pick up any changes that occur via a manual change of IP or DHCP reassignment. The value of the IP address will be displayed in "***Override detected DNS Name with***" once selected. If the host does not have a valid IP address, i.e. DHCP has not been responded to, then the syslog message will default to the system's hostname which is the default setting for the agent.

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. If this format is not processed correctly by your SYSLOG server, please try the alternate header.

The EPS Rate Limit 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. If 'Notify on EPS Rate Limit' option is selected then a message will be sent to the server whenever agent reaches the EPS rate limit. The message also include the EPS rate limit value. EPS Notification Rate Limit 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. The EPS rate limit settings are 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.

A major function of the Epilog system is to filter events. This is accomplished via the auditing 'objectives' capability. Any number of objectives may be specified, and are displayed within the **Objective Configuration** window (Figure 4). A listed objective may be viewed or modified within the **Create or Modify an Objective** window, as shown in Figure 5.

Figure 4 Objectives Configuration Window

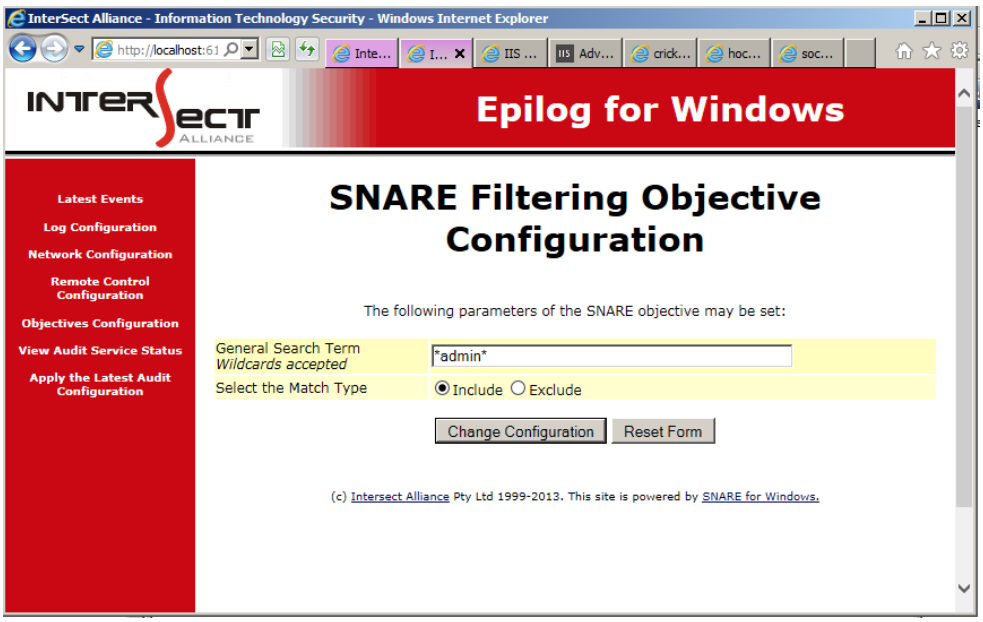


Figure 5 Create or Modify an Objective Window

Each of the objectives provides a high level of control over which events are selected and reported. Events are selected using specific filters called 'Objectives'. Due to the generic nature of Epilog for Windows, no default objectives are defined and subsequently, all events will be passed directly to the configured network destination. The 'General Search Term' field is used to perform a case insensitive search against each log entry collected (including wildcards such as '*' and '?'). Any matching entries are then included or excluded depending on the option selected (NB: all entries are included by default).

Once the above settings have been finalized, clicking **OK** will save the configuration to the registry. However, to ensure the ***Epilog*** service has received the new configuration, the ***Epilog*** service MUST be restarted via the **Windows' Services control panel** or via the **Apply the latest audit configuration** menu item.

4.2 Log configuration

The Epilog service's main focus is the ability to monitor any text-based log file. The initial log configuration parameters to consider are:

- The location of the log files to be monitored, and
- The type of log files being monitored.

These parameters are shown in the 'Log Configuration' menu, shown in 15 below.

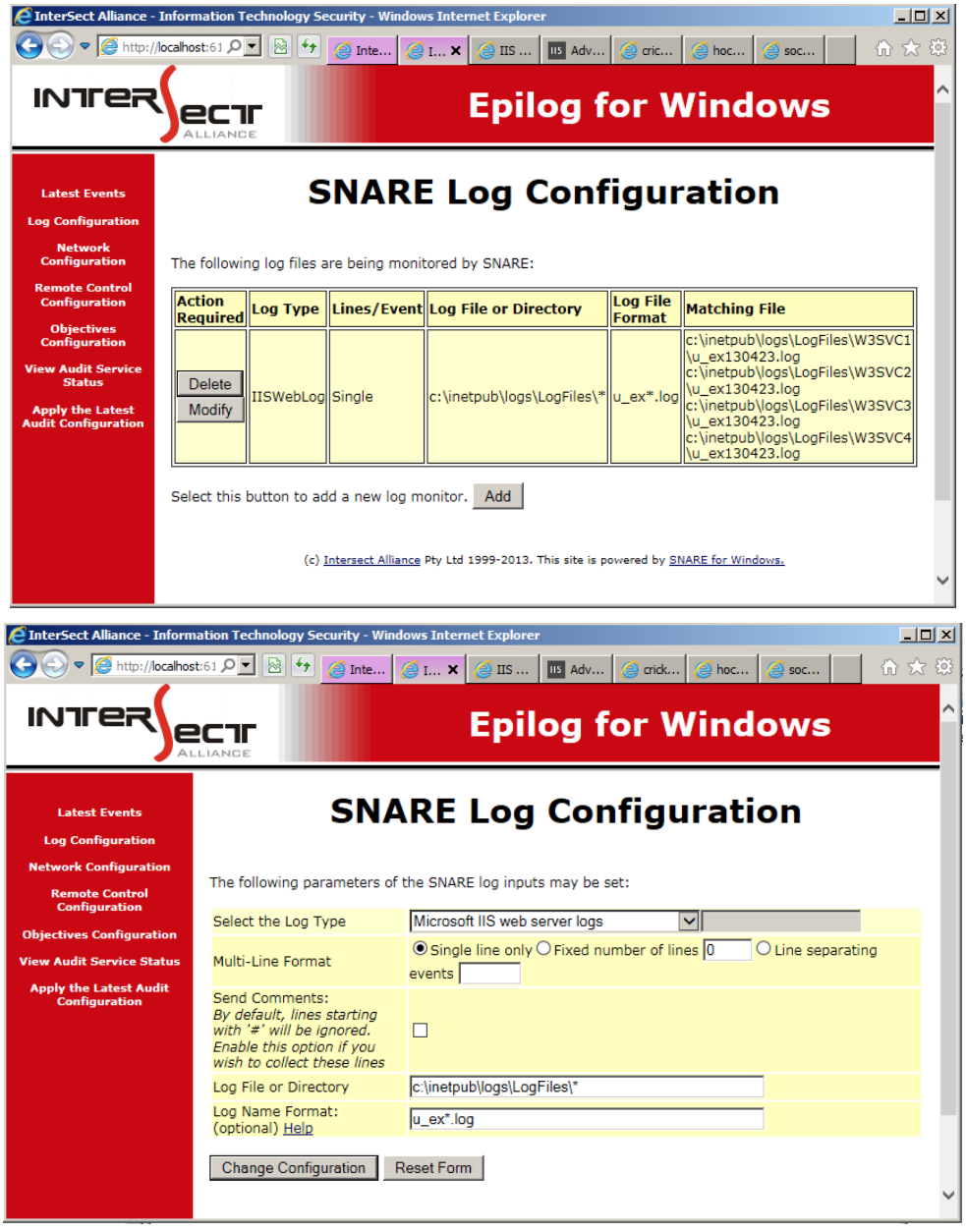


Figure 6 Log Configuration Window

From this page, log monitors can be added, deleted and modified. The following parameters of the SNARE log inputs may be set:

- **Select the Log Type** - The log type of a file will tell the Snare server how to handle the incoming data stream and in which table the processed information should be stored. The currently available log types are:

  GenericLog – Generic log format (default)

  ApacheLog – Apache web logs

  ExchMTLog – Exchange message tracking logs

  IISWebLog – Microsoft IIS web logs

  ISAFWSLog – Microsoft ISA firewall logs

  ISAWebLog – Microsoft ISA web logs

  MSProxySvr – Microsoft proxy server logs

  SMTPSvcLog – Microsoft SMTP logs

  SquidProxyLog – Squid proxy logs

  Custom Event Log – User configurable log type. When this is selected the desired format can be added in the text field.

- **Multi-Line Format** – How you would like Epilog to send events to the server e.g. Snare Server.

  Single line only - If this option is selected then Epilog will read from file line-by-line i.e. Epilog will keep reading from file until it finds a new line, '\n' in the file. Each of these lines will be sent to server as separate events.

  Fixed number of lines - If this option is selected then Epilog will read fixed number of lines from the file. For example, under this option if value is set to 4 then Epilog will keep reading the file until it finds '\n' 4 times. Each occurrence of '\n' represents a new line and Epilog will read 4 lines. These fixed number of lines will be sent to server as a single event

  Line separating events - If this option is selected then Epilog will keep reading from file until it finds a specific pattern in file. The input for this option is treated as a string. For example, if the line separating event is defined as `<end>` then Epilog will keep reading from the file until it finds the pattern `<end>` in the file however it must be on a newline by itself. After that the whole data read up to `<end>` will be sent to the server as a single event

  From v1.8.2 having a caret (^) as the pattern match for example ^ABCD will split the event into each line. The caret acts as a multi-line separator to match on text at the beginning of a log entry.

- **Send Comments** – Enable this option if you wish to collect the lines with a comment in them. A comment is represented by `#` and by default all lines starting with the hash will be ignored.

- **Log File or Directory** - must be defined as the fully qualified path to the desired log file OR the fully qualified path to the directory containing the target log files e.g `C:\mylogfiles\`. Spaces are valid characters. To indicate one or more sub-directories that should be searched for matching files wildcards are to be added to the Log Name Format .

- **Log Name Format** - allows you to specify the file name or pattern you are targeting. Wildcards are accepted (e.g. Myfile*.log, using '*' and '?' expressions). A percent sign (%) can be used to represent the current date of the form YYMMDD.

For example, ISA is configured to log both web logs (e.g. ISALOG_20080612_WEB_000.w3c) and firewall logs (e.g. ISALOG_20080611_FWS_000.w3c) to the same directory. To watch each log type, you will need two log watches, both with the same Log Directory but the Log File Format set to "ISALOG_20%_WEB_*" and "ISALOG_20%_FWS_*" for web and firewalls logs respectively.

If *no* log name format is defined then it uses a default log format of YYMMDD and matches files within the specified directory set in Log File or Directory field, for example `c:\mylogfiles` and for date such as for 30 October 2014 it will match files using filter **`141030.*`** and will match files for example **`C:\mylogfiles\141030.*`**

Last matching file – Users may monitor the last file within a directory (default behaviour pre v1.7.5).

First matching file – Users may monitor the first file within a directory.

All matching files - Users may create a single log monitor for all files within a directory

Once each log watch is configured, Epilog for Windows will display a list of the matching files and after the agent has been restarted, it will continuously monitor each file for any changes, immediately reporting them to the identified Snare servers. For specific file names, Epilog for Windows will follow the exact name of the file even if it is rotated, truncated, replaced or deleted. In the event that the file is removed, the Epilog service will wait until the file is recreated and then resume normal monitoring. If a Log Name Format is used, Epilog will also watch for new filenames, dynamically updating the file watch each time a new file becomes available.

Once the above settings have been finalized, clicking 'Change Configuration' on the Remote Control Interface will save the configuration to the registry.

If the Log File or Directory does not exist, or if no files are found in that directory to be watched the *Matching File* column will be displayed in red as below. If this is the case, check your paths and log file formats.

To ensure Epilog has received the new configuration, the service MUST be restarted via the **Apply the Latest Audit Configuration** menu item, or alternatively, by issuing the restart command via the **Windows' Services control panel**.

5 Audit event viewer functions

The main Epilog window also contains the events that have been filtered. Events collected, which meet the filtering requirements as per the **Audit Configuration**, will be displayed in the 'Latest Events' window. This display is NOT a display from the text-based log file, but rather a temporary display from a **shared memory** connection between the Epilog remote control interface and the ***Epilog*** service. The Epilog remote control interface will begin with a clear event log, since filtered events are not written to a local disk during normal operations. A key feature of the ***Epilog*** service is that events are not stored locally on the host (except for the log files being monitored by Epilog), but rather sent out over the network to one or more remote hosts. *Please note: If caching is enabled, messages will be written to disk when the agent is stopped to prevent lost messages. This file is read into memory and removed as soon as the agent is restarted. Caching, the TCP protocol capability, and the ability to send events to multiple hosts is only available to those users that have purchased a Snare Server, through the supported agents. See Chapter 8 of this document for further details.*

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 window will automatically refresh every 30 seconds.

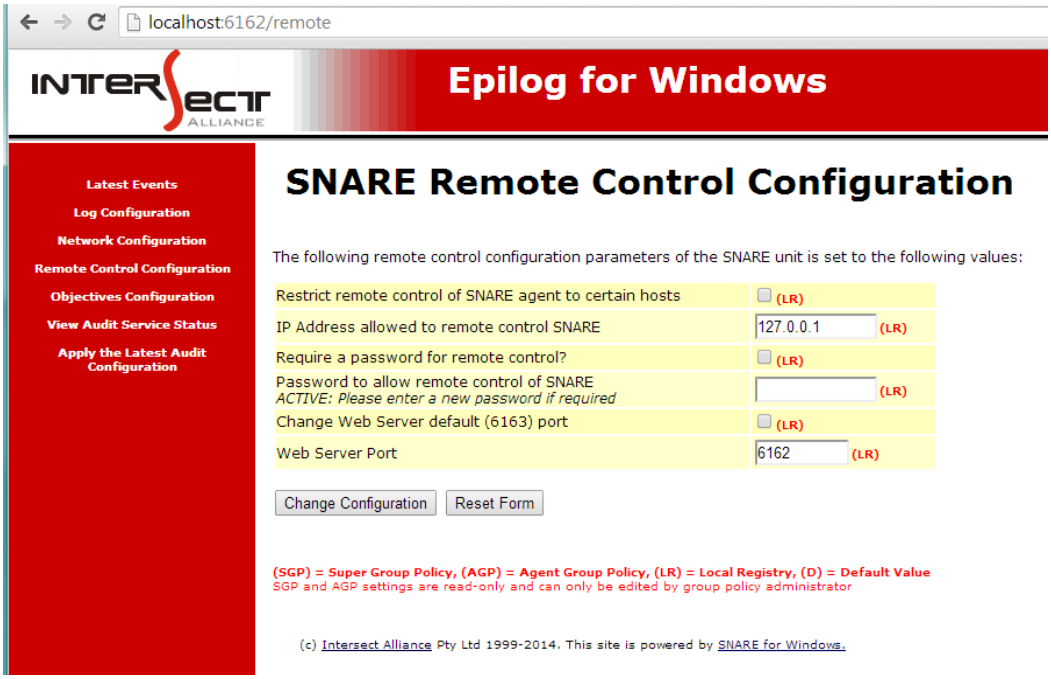


Figure 10 Remote Control Window

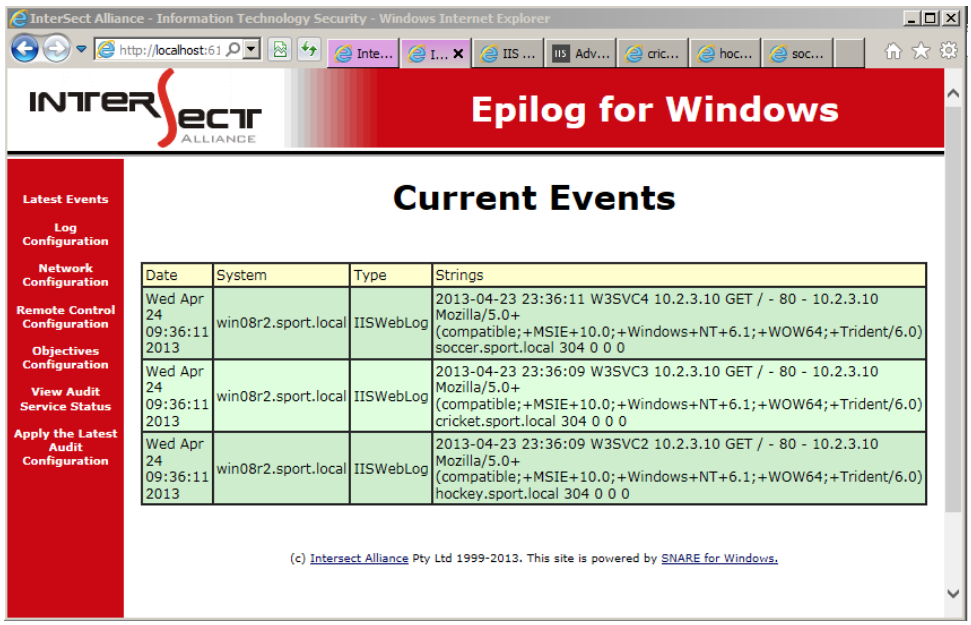


Figure 7 Latest Events Window

6 Remote control and management functions

The ***Epilog*** service is a separate standalone component of the Epilog system, however the Epilog remote control interface can be used to control a number of aspects of its operation. Primarily, the log configuration can be developed and set, as described in the previous sections. Furthermore, two other functions are available to manage the ***Epilog*** service.

The ***Epilog*** service can be restarted directly from the menu item **Apply the latest audit configuration**. This will instruct the ***Epilog*** service to re-read all the configuration settings, clear the buffers and restart the service. This function is useful when changes to the audit configuration have been saved, without being applied. The user can therefore select when to activate a new configuration by selecting this menu item.

The ***Epilog*** service status can be viewed by selecting the **View Audit Service Status** menu item as shown in Figure 9. This will display whether the ***Epilog*** service is active

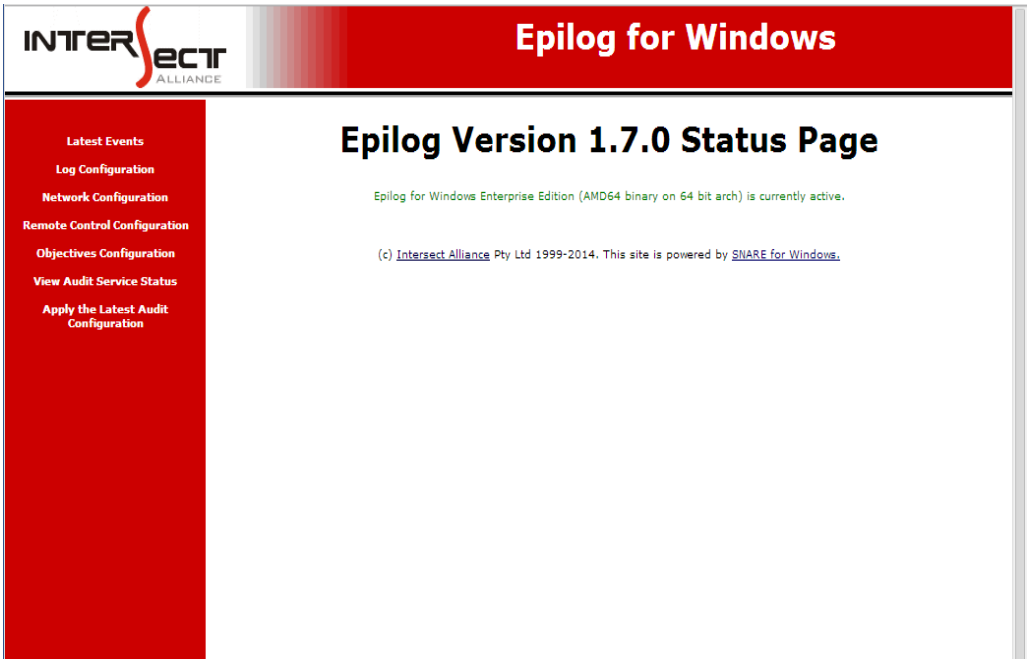


Figure 9 Audit Status Window

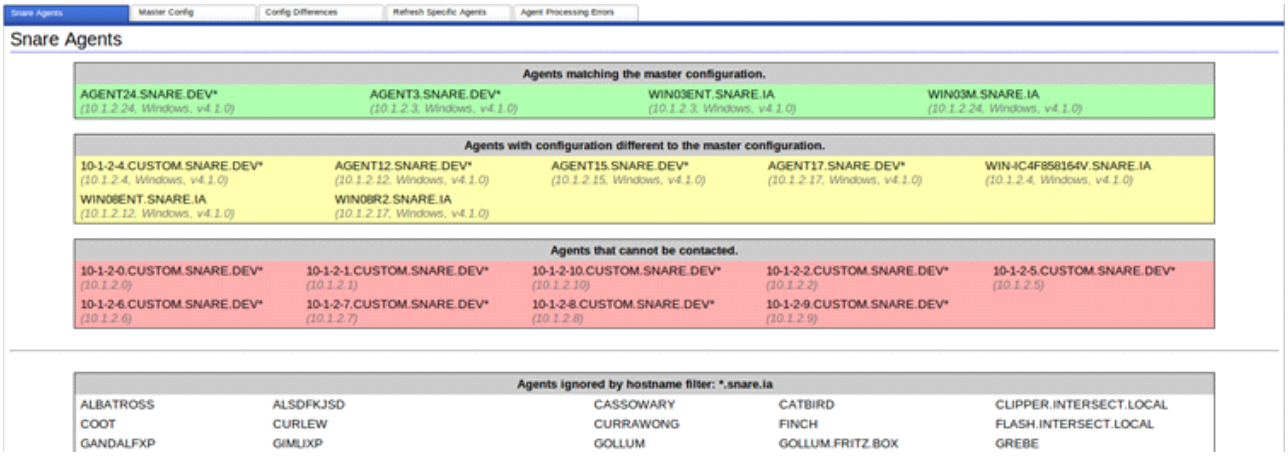
A significant function of the ***Epilog*** service is its ability to be remote controlled. This facility has been incorporated to allow all the functions available in Epilog, to be accessible through a standard web browser. The ***Epilog*** service employs a custom designed web server to allow configuration 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:

- **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.
- **Password to allow remote control of Snare**. A password may be set so that only authorised individuals may access the remote control functions. 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. Note that this password is stored in an encrypted form in the registry, using the MD5 hashing algorithm.
- **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) 6162, then the user needs to type **http://mysite.com:6162** to reach the web server. The default ***Epilog*** web server port (6162) may be changed using this setting, if it conflicts with an established web server. However, care should be taken to note the new server port, as it will need to be placed in the URL needed to access the Epilog agent.
- **Allow remote control of Snare agent**. Although previously available through the remote control interface, this option is now configurable at the time of installation. Enabling this option will allow the Epilog agent to be remote controlled by a remote host. If the remote control feature is unselected, it may only be turned on by enabling the correct registry key on the hosted PC which the Epilog agent has been installed.

7 Managing the Agent Configuration

7.1 Agent Management Console

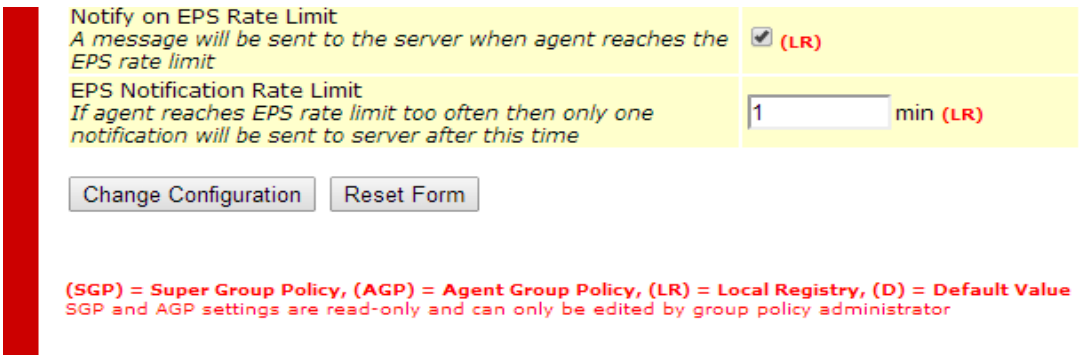
The most effective and simplest way to configure the SnareCore service is to use the Snare web based Remote Control Interface. If remote control is enabled, the process of configuring large numbers of agents can be further simplified by taking advantage of the Snare Server **Agent Management Console**.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



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

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

```
CLASS MACHINE

        CATEGORY !!"InterSect Alliance Snare Epilog 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\Epilog\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\Epilog\Config"

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

                                VALUENAME "Clientname"

                        END PART

               END POLICY

        END CATEGORY   ;CONFIG_CATEGORY
```

8 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.

TheFigure 10 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, OSX 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.

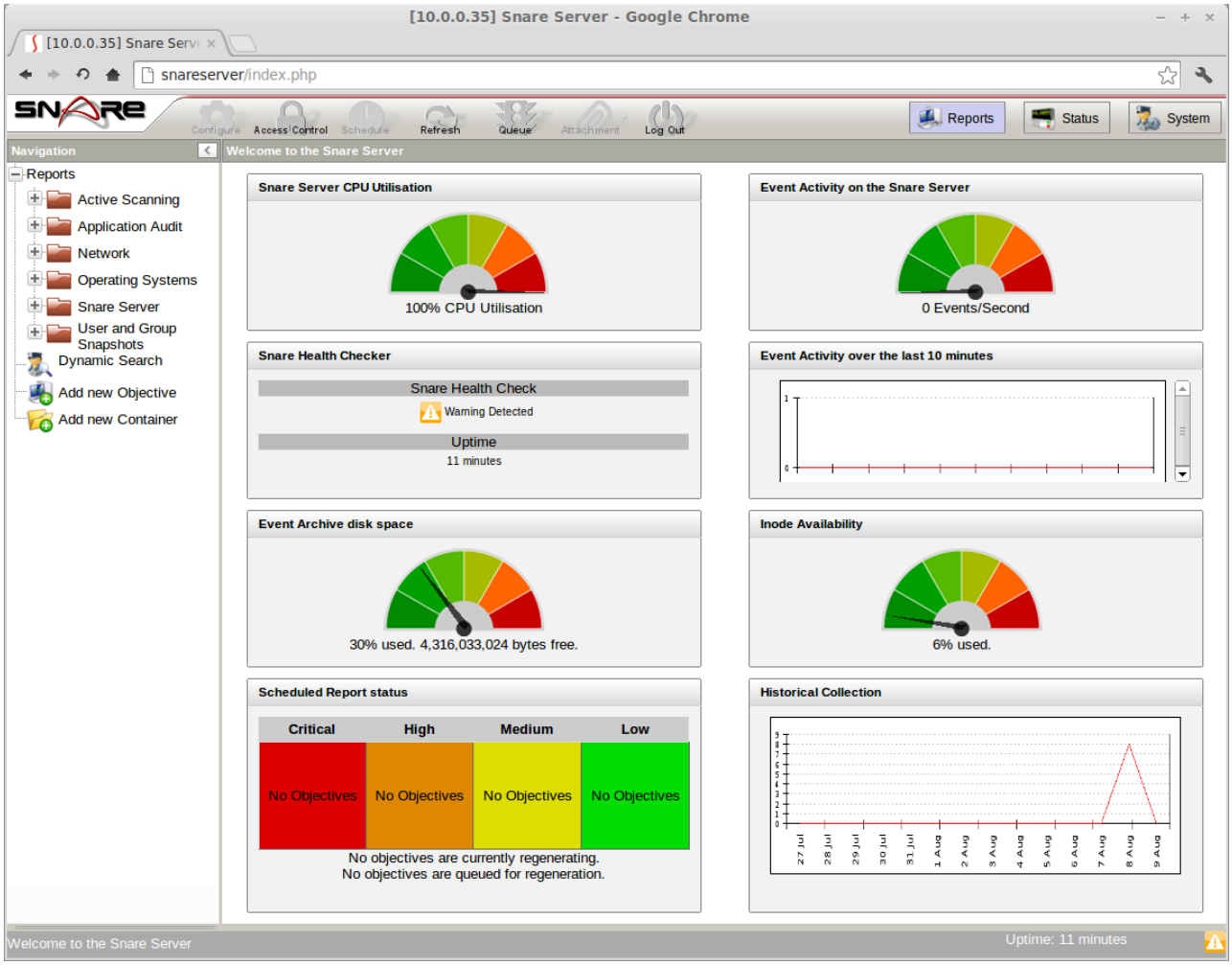


Figure 10: Welcome to the Snare Server

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.

9 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 ***Epilog*** service collects data from the identified log files and passes it unaltered to the identified network destination. Whitespace is the primary element used separate elements within the data. An audit event may look something like this:

Example:

```
flash     ApacheLog      0       10.0.3.2 - - [16/Jun/2008:10:10:00
                  +1000] "GET / HTTP/1.1" 200 44
```

The information in blue, as shown in the above record, is information added by the ***Epilog*** service. The format of this information is as follows:

<hostname> ***<log_type>*** ***<unused>*** ***<log_event>***

Appendix B - Epilog 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 Epilog configuration registry key is located at **HKEY_LOCAL_MACHINE\SOFTWARE\Intersect Alliance\Epilog**, and this location may not be changed. If the configuration key does not exist, the ***Epilog*** service will create it during installation, but will not actively audit events until a correctly formatted at least one log monitor is present.

Epilog can be configured in several different ways, namely:

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

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

`[Config]`	This subkey stores the delimiter and clientname values.
`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 Remote Control Interface.
`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.
`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): General Match[512];GeneralMatchType(DWORD) General Match Type: =0 (Include entries that match general search term type; =1 for Exclude) The General match term is the filter expression, and is defined to be any value which includes DOS wildcard characters. Note that these are NOT regular expressions. NOTE: Semicolons are actually "TAB" characters.

[Network]	This subkey stores the general network configurations.
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.
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.
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.
CacheSizeM	This value is of type REG_DWORD, and determines the size of the event cache. The value must be between 1 and 1024. 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.
NotifyMsgLimit	This value is of type REG_DWORD having value 0 or 1, and determines whether to send or not the EPS notification to server (1 means send and 0 means not to send) whenever agent reaches EPS RateLimit. This feature only appears in supported agents.
NotifyMsgLimitFrequency	This value is of type REG_DWORD, and determines the frequency of events per second notification. The value is treated in minutes and only one EPS notification message is sent to server regardless of how many times agent reaches EPS limit during these minutes. This feature only appears in supported agents.
[Remote]	This subkey stores all the remote control parameters.
Allow	"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).
WebPort	This value is the web server port, if it has been set to something other than port 6162. It is of type REG_DWORD. If not set or out of bounds, it will default to port 6162.

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.
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.
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.
[Log]	This subkey stores all the log monitors.
Log# (where # is a serial number)	This section describes the format of the log monitors. Log monitors are of type REG_SZ, of no greater than 512 chars, and is composed of the following string: Logtype|LogPath LogType is optional and is used to inform the Snare server how to process the data stream. A list of valid log types can be found in Section 4.2. The LogPath is the fully qualified path to the log file that needs to be monitored OR the fully qualified path to the directory containing date stamped log files of the form "*YYMMDD*" (in this case a trailing backslash ('\') is required). Spaces are vaild, except at the start of the term.