SNARE

System iNtrusion Analysis & Reporting Environment

Guide to
Snare Epilog for UNIX

INTERSECT ALLIANCE

About this guide

This guide introduces you to the functionality of the Snare Enterprise Epilog for UNIX. Snare Epilog for UNIX is currently released for the Linux and Solaris operating systems and facilitates objective-based filtering, and remote audit event delivery of text-based log files for Linux and Solaris based systems. Snare Epilog for UNIX will also allow a security administrator to fully remote control the application through a standard web browser if so desired.

For more information on the Snare product suite, visit www.intersectalliance.com/our-product/other-documentation/.

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, OSX, SQL Server and many more, including Epilog. The agents are capable of sending data to a wide variety of target collection systems, including our very own **'Snare Server'** (see *Chapter 6* for further details). The Snare Server is beneficial to organisations that wish to collect from a wide variety of Snare agents and appliances such as firewalls or routers. 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. The Agent Management Console may be purchased separately from the Snare Server.

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

2 Overview of Snare Epilog for UNIX

Snare operates through the actions of one key application; the '***Epilog***' process. Snare will monitor the given log files and manage the generated events based on the objectives defined in the Snare configuration files. Log files are filtered using the Snare objectives, labeled according to the log type identified and then passed over the network, using the UDP or TCP protocol, to one or more remote servers for collection, analysis and archival.

The TCP protocol capability, and the ability to send events to multiple hosts is only available in the Enterprise versions of the agents made available to Snare Server customers.

Snare Epilog for UNIX is compatible with Redhat 5, 6, SLED 10,11, Ubuntu and Debian, Solaris 9, 10, 11.

3 Installing and running Epilog

3.1 Epilog installation

Epilog includes an installation script to allow for easy installation and configuration of all critical components. The Epilog installation file includes the following key components:

- **Epilog binary**
  The ***Epilog*** daemon is contained in the '***Epilog***' binary. This binary provides the capability to read event log records from text files, filter the events according to the 'objectives' defined by the user, provide a web based remote control interface, and specify the log files to monitor.

- **install.sh/uninstall.sh**
  These two scripts undertake the installation and uninstallation functions for Epilog for UNIX. The scripts may prompt the user for confirmation, or for specific configuration options during the installation and uninstallation processes.

- **Configuration File**
  A single configuration file is required to correctly run ***Epilog***. The installation script will ensure that a correctly formatted configuration file, named epilog.conf is generated and copied to the /etc/snare/epilog directory on your local filesystem during the installation process.

- **README File**
  The version control file for Epilog found in /usr/share/doc/EpilogUnix*.

How to... **Download the 'Epilog' file from the Secure Area at the Intersect Alliance website to the target server and perform the following:**

Install the Snare Epilog binary RPM package

1. Change directory to the folder containing the .RPM and, as the 'root' user, type:
   `>rpm -Uvh filename.rpm`

   `E.g. >rpm -Uvh epilog-SUPP-1.5.2.1.x86_64.rpm`
2. This will install Snare Epilog and the ***Epilog*** daemon will start automatically.

Install the Snare Epilog binary .TAR package

1. Change directory to the folder containing the .TAR.GZ file and, as the 'root' user, type:
   `>gzip -d filename.tar.gz`
   `>tar xvf filename.tar`

   `E.g. >tar xvf epilog-SUPP-1.5.2.tar`
2. A directory called *filename* will be created. Enter this directory, e.g.:
   `>cd epilog-SUPP-1.5.2`
3. In order to commence the installation, type:
   `>./install.sh`

   A prompt will only be displayed *if* an existing configuration file is found, otherwise a basic configuration file is used by default.
4. Once the installation process has completed, the ***Epilog*** daemon will start automatically (although no log monitors will be configured) and the daemon will also be integrated into your normal boot process.

Install the Snare Epilog binary .DEB package

1. Logon as root user and issue the command:
   `>dpkg -i filename.deb`
2. This will install Snare Epilog and the ***Epilog*** daemon will start automatically.

How to... Remove the Snare Epilog binary RPM package (if applicable)

1. Query the RPM database to ensure Snare Epilog is installed
   `>rpm -q epilog-supp`
2. Remove the Snare Epilog package

   `>rpm -e epilog-supp`

Remove the Snare Epilog binary .TAR package (if applicable)

Execute:
`>/etc/snare/epilog_uninstall.sh`

Remove the Snare Epilog binary DEB package (if applicable)

Remove the Snare Epilog package

`>dpkg -r epilog-supp`

The installation scripts may request the choice of two installation profiles. There is only one starting configuration for each agent, which will be automatically selected unless the agent is being reinstalled. Where the agent is being reinstalled, there is the second option to preserve the existing configuration file.

3.2 Running Epilog

Upon installation of Snare Epilog for UNIX, the ***Epilog*** binary will be installed in the /usr/bin directory. The ***Epilog*** process will be controlled by the /etc/init.d/epilogd daemon control script, so there is no need to start or stop ***Epilog*** directly.

The ***Epilog*** daemon must be running, if the events are to be passed to a remote host. The ***Epilog*** daemon may be stopped, started or restarted by issuing the following commands respectively:

How to... Run the ***Epilog*** Daemon:

1. Login as root.
2. Execute the command:

   ```
   >/etc/init.d/epilogd start
   ```

3. To check that there is one process (or two if the micro-web server is active) called '/usr/bin/epilog', execute the command:

   ```
   >ps -ef | grep epilog
   ```

The ***Epilog*** daemon may also be stopped or restarted by issuing the following commands respectively: `/etc/init.d/epilogd stop`, `/etc/init.d/epilogd restart`

To run Epilog via the Remote Control Interface, then remote audit control must be enabled as per following:

How to... Enable Remote Audit Control

If the ***Epilog*** daemon is run on a system that has remote control enabled in the epilog.conf file, then the audit subsystem may be remotely controlled using a standard web browser. Note that for this to work, the remote control facility should be set *(see specific instructions on remote control settings)*, and the `/etc/Snare/epilog/epilog.conf` MUST have AT LEAST the 'allow=1' line under the [Remote] configuration category specified (NB: Epilog must also have a different listen_port if it is operating on the same system as a Snare operating system audit daemon):

```
[Remote]
        allow=1
        listen_port=6162
        restrict_ip=10.0.0.1
        accesskey=SnYLb.gT4Gk2k
```

If the 'restrict_ip' line is in the epilog.conf file, then the only machine that can access the remote control feature, is the system that is listed on that line. If the 'accesskey' line is specified, then a password is required to access the remote control function (the username for remote control is always '***Snare***'). The password in the Snare configuration file, is 'encrypted' using the standard UNIX 'crypt' function. Using a web browser type in the following on the URL bar:

```
http://<ip address or DNS hostname>:6162
```

(NOTE that '6162' will be the port number specified in the '***listen_port***' of the ***/etc/Snare/epilog/epilog.conf*** file). More information on web browser in next section.

4 Setting the audit configuration

4.1 Configuration

The configuration files are stored in ***/etc/Snare/epilog*.** This directory contains necessary configuration files with all the details required by the audit daemons to successfully execute. Failure to have a correct configuration file available in this location will not 'crash' the daemons, but will result in logs not being processed, or forwarded to your central log server.

> Tip: Manual editing of the configuration files is possible, but care should be taken to ensure that it conforms to the required format for the audit daemon. Also, any use of the Remote Control Snare capability to modify security objectives or selected events, will result in any manual configuration file changes being overwritten. Details on the configuration file format can be viewed in Appendix B – Snare Configuration File.

The most effective and simplest way to configure the Epilog audit daemons is to use the Remote Control Interface capability (remote control web browser). The ***Epilog*** daemon can be restarted remotely from the menu item ***Apply the Latest Audit Configuration***. This will instruct the audit daemon to re-read the configuration file, clear the buffers and restart. This function is useful when changes to the audit configuration have simply been saved to the configuration file, without being 'applied'.

5 The Remote Control Interface

The Remote Control Interface is accessible by entering http://localhost:6162 in a web browser. The Remote Control Interface is turned on by default, and also password protected for security reasons. The default username and password are as follows and it is strongly recommended to change the password to a complex password.

Username: snare

Password: snare

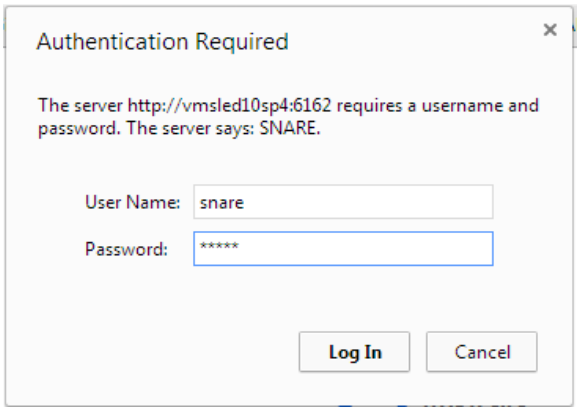


Figure 1: Access the Remote Control Interface

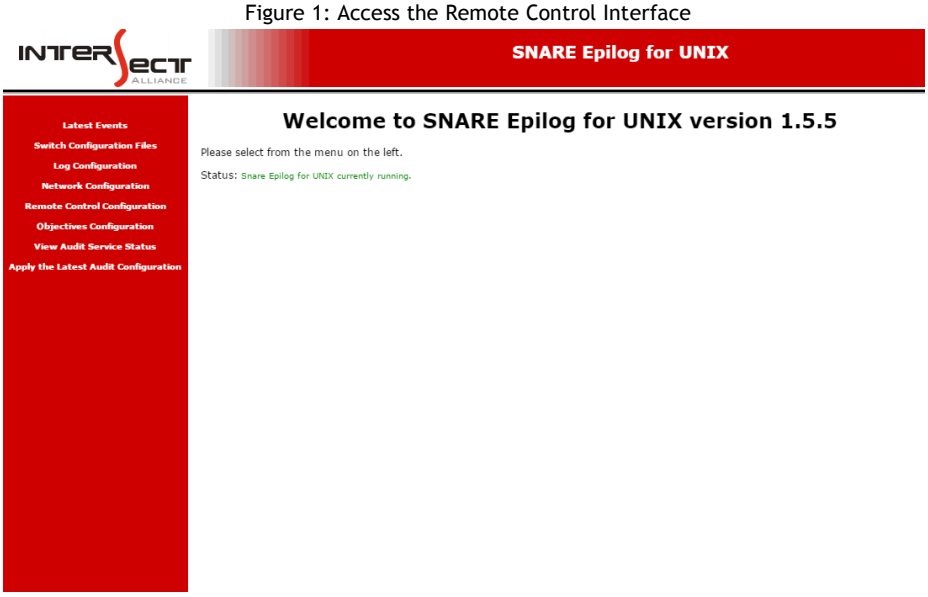


Figure 2: Welcome to the Remote Control Interface

The Remote Control Interface provides a number of capabilities including:

- Network Configuration
- Remote Control Configuration
- Objectives Configuration
- Log Configuration
- Switch Configuration Files
- Viewing Latest Events

Note: There are some options on these pages that *are not* available to users of Snare OpenSource Epilog.

5.1 Configuration Control

The Remote Control Interface is available to access and modify all of the available configuration files, and is accessed from the menu item *Switch Configuration Files*, as displayed in Figure 3: Configuration File Selection.

Once the chosen configuration file is selected, for example apache.conf, epilog.conf (indicated by the **bold** name), all of the functions discussed below will operate on the selected configuration file. By default, all functions will operate on the **epilog.conf** file.

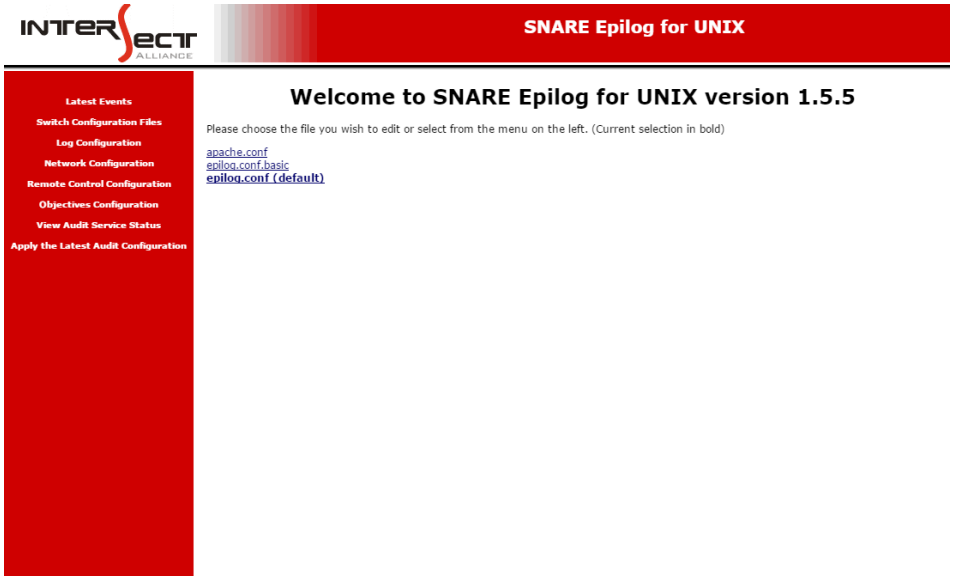


Figure 3: Configuration File Selection

5.2 Network Configuration

The configuration parameters available are as follows and shown in Figure 4:

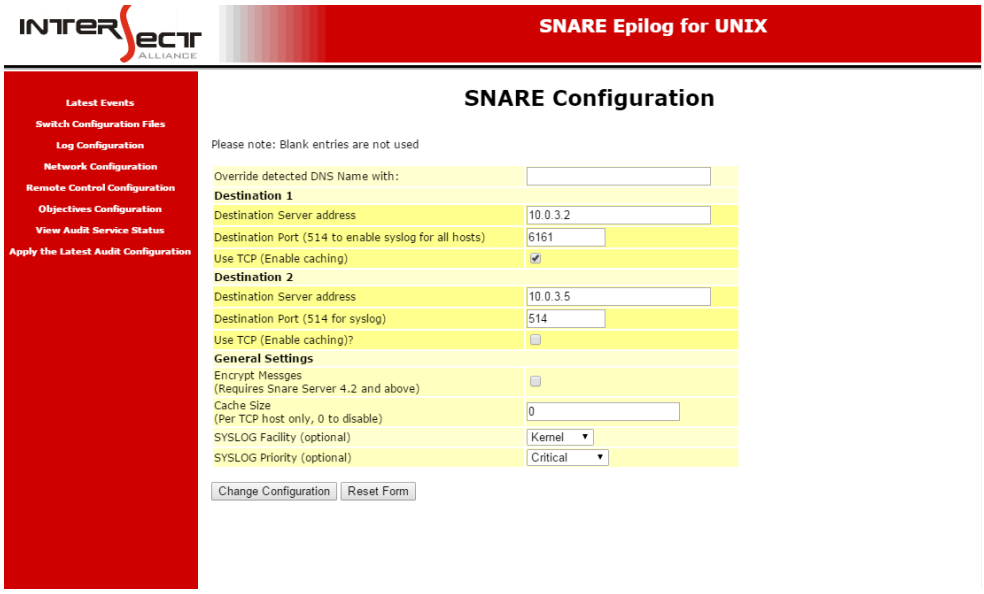


Figure 4: Network Configuration

The ***Override detected DNS Name with*** field can be used to override the fully qualified domain name of the host system, which will be used by Epilog if this field is blank. Note that executing the command 'hostname' on a command prompt will display the current host name allocated to the host.

Snare can send audit events to one or more network ***destinations***. Enter a DNS name or IP address, and a ***destination port*** for Snare to use when sending events. If, for example, the Intersect Alliance Snare Server is used, then this should be the default port of 6161 and 514 for syslog. Supported agents will have an additional options to enable TCP, ***Use TCP***, (and optional caching for one server) and configure multiple hosts.. Additional hosts can be added one at a time by clicking “Change Configuration” after each addition. To remove a host, delete the “Destination server address” and click “Change Configuration”.

Encrypt message 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 server.

The caching feature, ***Cache Size***, will store unsent messages in memory until the destination server is once again contactable. The cache is limited to 320000 messages or the available memory of the host system (whichever comes first). Restarting the agent will purge this cache, freeing all the memory used by the cache.

If there is a requirement to incorporate a ***Syslog header***, there are two types available, 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.

Once the above settings have been finalised, clicking 'Change Configuration' on the remote control page will save the configuration to the designated configuration file (as defined by the 'Switch Configuration' page).

5.3 Remote Control Configuration

Epilog is able to be remote controlled. This facility has been incorporated to allow all the functions normally available through the configuration file, to also be available through a standard web browser as displayed in Figure 5.

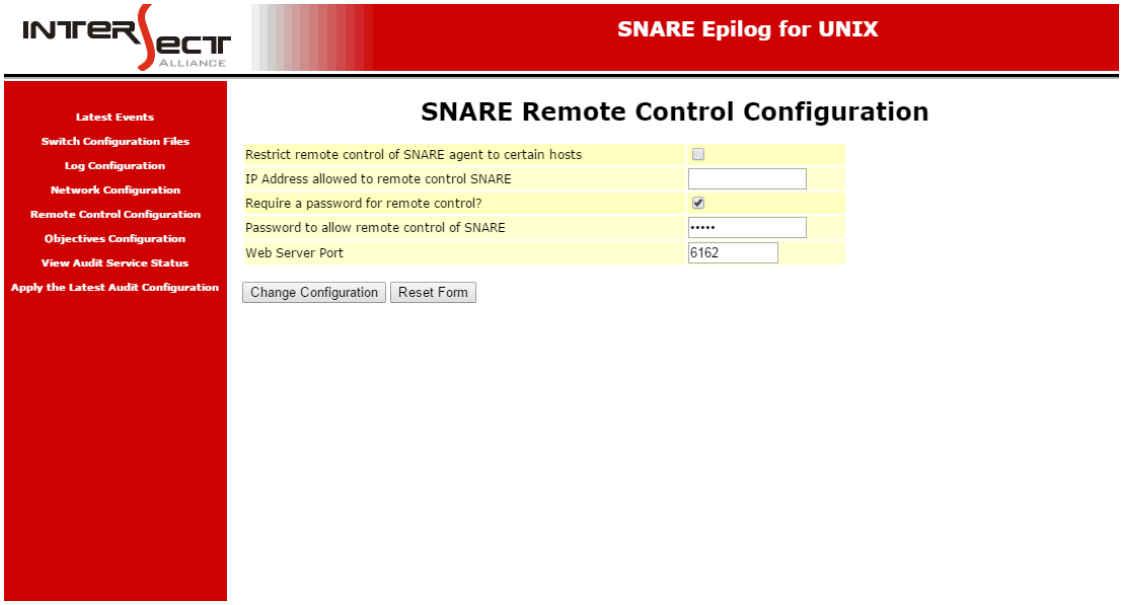


Figure 5: Remote Control Configuration

The functions available through the web browser are identical to those available on the Snare configuration file. The parameters which may be set for remote control operation are discussed below:

- **Allow remote control of Snare agent**. Selecting this checkbox will allow the Snare agent to be remotely controlled from a web browser. This host may be independent from the central audit collection server. If the remote control function is disabled, and you wish to enable the facility, follow the instructions detailed in 'Enable Remote Audit Control' in Section 3.2 of this document.
- **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 to be used in conjunction with other countermeasures (such as ensuring your organisational firewall does not allow external connections to the Snare micro-web server port).
- **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 batch-mode tool (such as 'curl' or 'wget'), note that the UserID is always '***Snare'***, and the password is whatever has been defined by the user. This password is not encrypted when being transmitted via the http session, but is encrypted when stored in the respective configuration files.

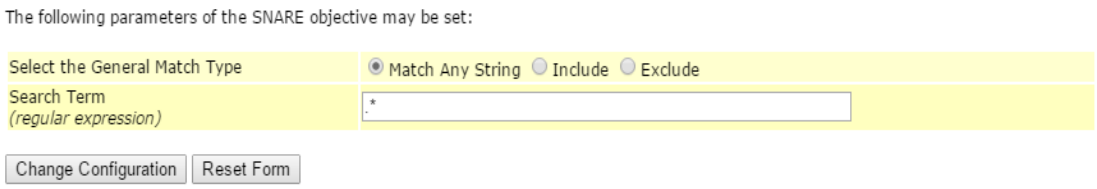
- **Web Server Port**. Normally, a traditional web server operates on port 80. If this is the case, then a user need only type the address into the browser to access the site. If however, a web server is operating on a port other than 80 (eg. 6162), then the user needs to type **http://mysite.gov:6162** to reach the web server. The default ***Epilog*** web server port may be changed using this setting, if it conflicts with an established web server or Snare agent. 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 Snare agent.

5.4 Objectives Configuration

A major function of Snare Epilog for UNIX is the capability to filter events, accomplished via the advanced auditing 'Objectives' function. Each of the objectives provides a high level of control over which events are selected and reported. Any number of objectives may be specified, and are displayed within the 'Objectives Configuration' menu on the remote control browser page, as shown in Figure 6 and Figure 7 below. Due to the generic nature of Snare Epilog for UNIX, no default objectives are defined and subsequently, all events will be passed directly to the configured network destination.

To ensure you get events, you must define at least one objective to capture, I.e '.*' To do this:

1. Select Objectives Configuration from the menu
2. Click Add
3. The objective will be displayed as below:



4. Click Change Configuration.
5. Click Apply the Latest Audit Configuration from the menu.

When adding an objective, the following parameters may be set:

Select the General Match Type – To include or exclude a search term, or match any string may be selected.

Search Term - allows a 'regular expression' match term to check against the event-specific matchable item. Regular expressions are an advanced form search filter. For example, the term '.*[Pp]ass(word|wd).*' would match the following:

- /etc/passwd
- /tmp/PasswordFile

but would not match

- /etc/PASSWD/
- /home/red/PaSsWoRd .txt

The search term will be used to search the entire string for any matches against the given expression. For example, this means that an included search term of '.*pwd.*' would apply to any single line with the term 'pwd' contained in it. If the objective is set to exclude, then lines matching the search term will be discarded. All events are included by default.

Tip: Order any 'Exclude' Objectives at the top of the list for the objectives.

The following shows an exclude objective, filtering out any events with *SnareDispatch* or *kernel* in its event.

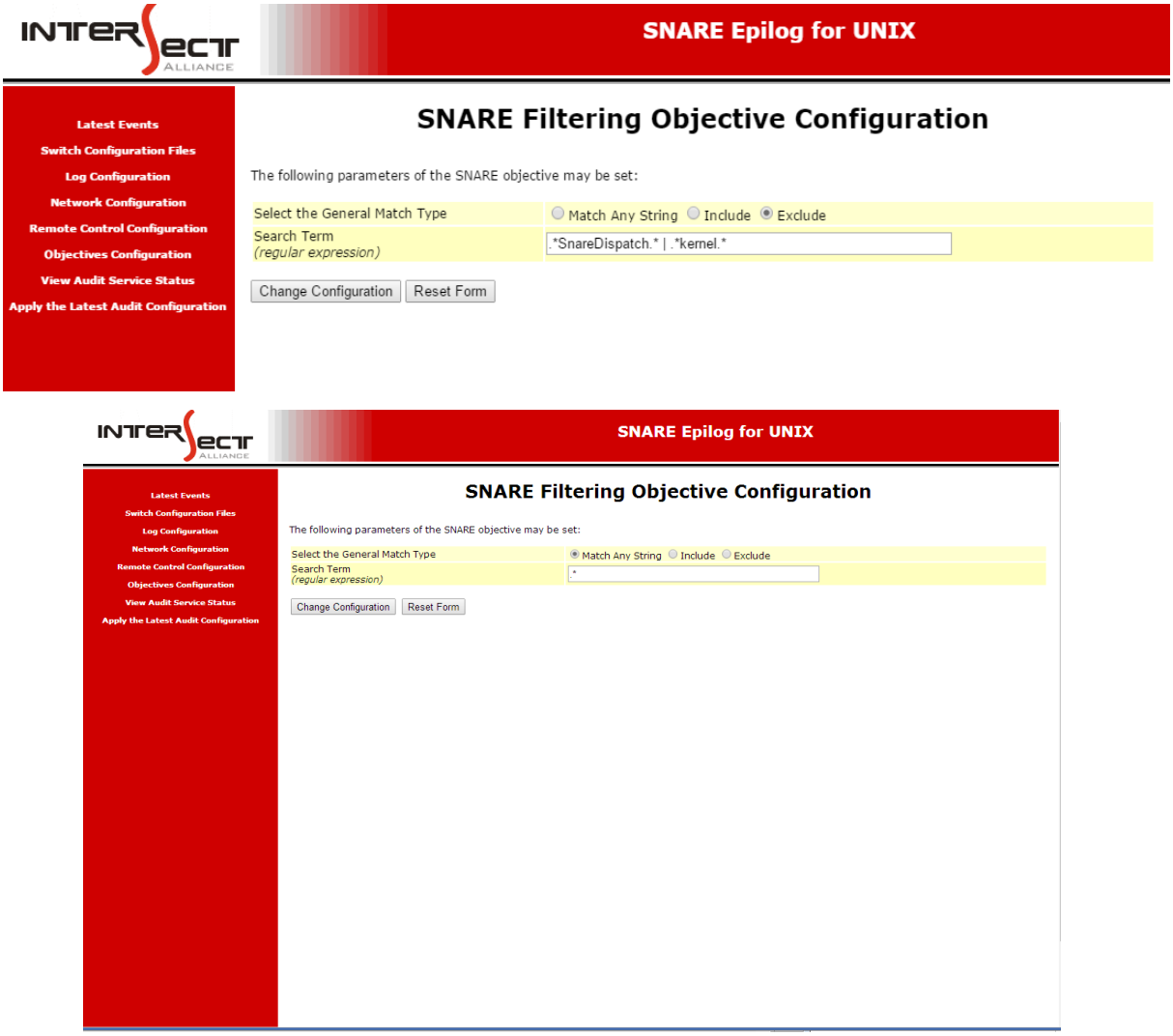


Figure 6: Adding an Objective

5.5 Log configuration

The ***Epilog*** daemon'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.

From the '***Log Configuration***' page, log monitors can be added, deleted and modified as shown in Figure 8 below.

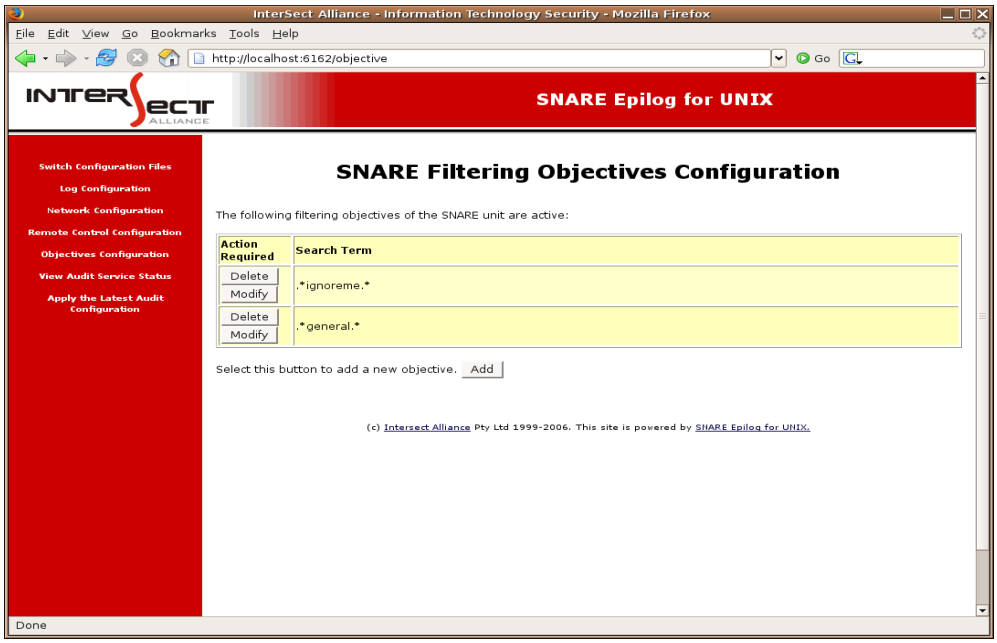


Figure 7: List of Objectives

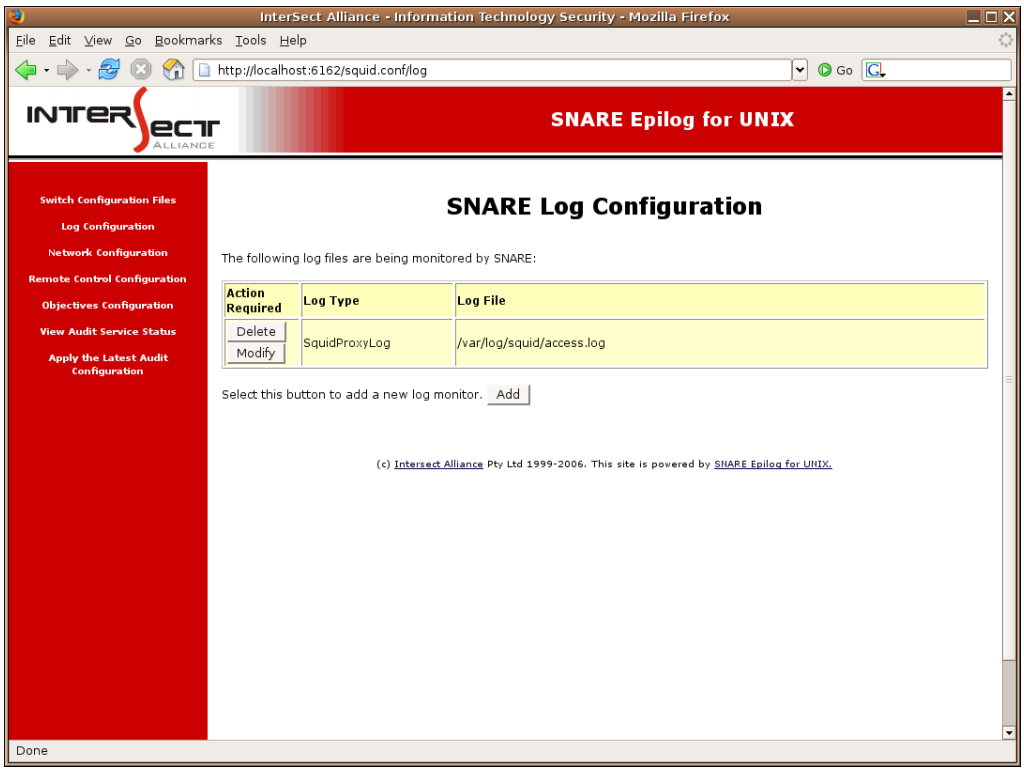


Figure 8: SnareSquid Log Configuration

The parameters to configure are displayed in Figure 9:

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 database table the processed information should be stored. The log types available are:

- GenericLog - Generic log format (default)
- ApacheLog - Apache web logs
- ISAWebLog - Microsoft ISA web logs
- MSProxySvr - Microsoft proxy server logs
- SMTPSvcLog - Microsoft SMTP logs
- SquidProxyLog - Squid proxy logs
- Custom Event Log

If Custom Event Log is selected then the details are to be entered in the adjacent dialog box.

Log File - must be defined as the fully qualified path to the desired log file (and may include spaces). Snare Epilog for UNIX will then continuously monitor this file for any changes, immediately reporting them to the identified Snare Servers. Snare Epilog for UNIX 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 daemon will wait until the file is recreated and then resume normal monitoring.

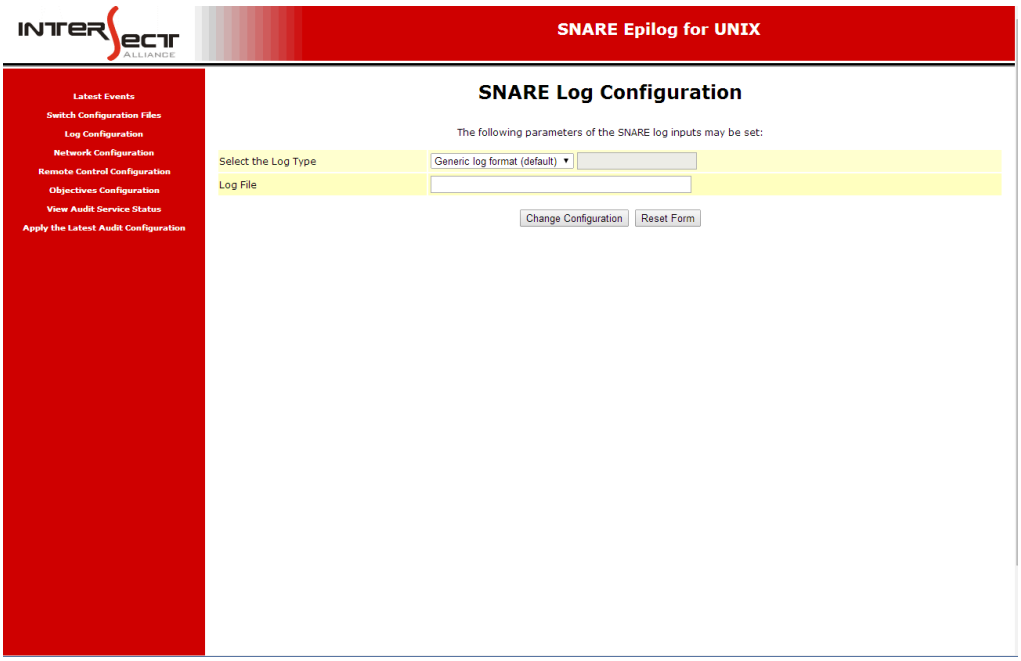
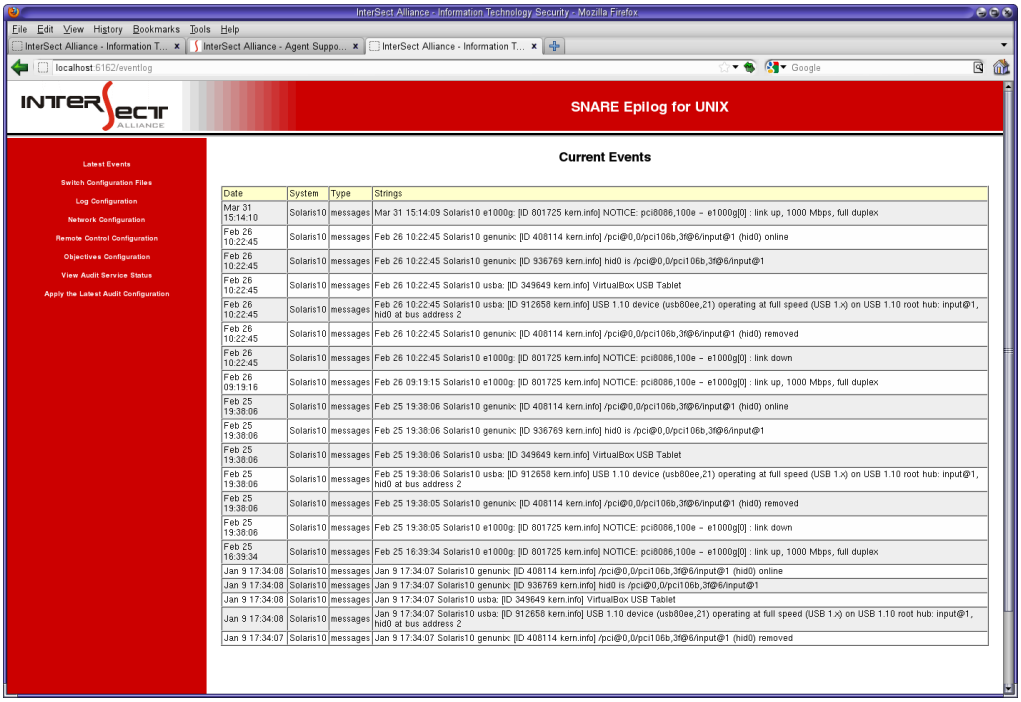


Figure 9: Defining the Log Configuration

Once the above settings have been finalised, clicking 'Change Configuration' to save the configuration. However, to ensure the designated daemon has received the new configuration, the daemon MUST be restarted via the 'Apply the Latest Audit Configuration' menu item, or alternatively, by issuing the restart command to the associated daemon control script.

5.6 Latest Events

A small rotating cache of audit events is displayed on the Latest Events window and is restricted to a list of twenty entries and cannot be cleared, except by restarting the agent.



Date	System	Type	Strings
Mar 31 15:14:10	Solaris10	messages	Mar 31 15:14:09 Solaris10 e1000g: [ID 801725 kern.info] NOTICE: pci8086,100e – e1000g[0] : link up, 1000 Mbps, full duplex
Feb 26 10:22:45	Solaris10	messages	Feb 26 10:22:45 Solaris10 genunix: [ID 408114 kern.info] /pci@0,0/pci106b,3f@6/input@1 (hid0) online
Feb 26 10:22:45	Solaris10	messages	Feb 26 10:22:45 Solaris10 genunix: [ID 936769 kern.info] hid0 is /pci@0,0/pci106b,3f@6/input@1
Feb 26 10:22:45	Solaris10	messages	Feb 26 10:22:45 Solaris10 usba: [ID 349649 kern.info] VirtualBox USB Tablet
Feb 26 10:22:45	Solaris10	messages	Feb 26 10:22:45 Solaris10 usba: [ID 912658 kern.info] USB 1.10 device (usb80ee,21) operating at full speed (USB 1.x) on USB 1.10 root hub: input@1, hid0 at bus address 2
Feb 26 10:22:45	Solaris10	messages	Feb 26 10:22:45 Solaris10 genunix: [ID 408114 kern.info] /pci@0,0/pci106b,3f@6/input@1 (hid0) removed
Feb 26 10:22:45	Solaris10	messages	Feb 26 10:22:45 Solaris10 e1000g: [ID 801725 kern.info] NOTICE: pci8086,100e – e1000g[0] : link down
Feb 26 09:19:16	Solaris10	messages	Feb 26 09:19:15 Solaris10 e1000g: [ID 801725 kern.info] NOTICE: pci8086,100e – e1000g[0] : link up, 1000 Mbps, full duplex
Feb 25 19:38:06	Solaris10	messages	Feb 25 19:38:06 Solaris10 genunix: [ID 408114 kern.info] /pci@0,0/pci106b,3f@6/input@1 (hid0) online
Feb 25 19:38:06	Solaris10	messages	Feb 25 19:38:06 Solaris10 genunix: [ID 936769 kern.info] hid0 is /pci@0,0/pci106b,3f@6/input@1
Feb 25 19:38:06	Solaris10	messages	Feb 25 19:38:06 Solaris10 usba: [ID 349649 kern.info] VirtualBox USB Tablet
Feb 25 19:38:06	Solaris10	messages	Feb 25 19:38:06 Solaris10 usba: [ID 912658 kern.info] USB 1.10 device (usb80ee,21) operating at full speed (USB 1.x) on USB 1.10 root hub: input@1, hid0 at bus address 2
Feb 25 19:38:06	Solaris10	messages	Feb 25 19:38:05 Solaris10 genunix: [ID 408114 kern.info] /pci@0,0/pci106b,3f@6/input@1 (hid0) removed
Feb 25 19:38:06	Solaris10	messages	Feb 25 19:38:05 Solaris10 e1000g: [ID 801725 kern.info] NOTICE: pci8086,100e – e1000g[0] : link down
Feb 25 16:39:34	Solaris10	messages	Feb 25 16:39:34 Solaris10 e1000g: [ID 801725 kern.info] NOTICE: pci8086,100e – e1000g[0] : link up, 1000 Mbps, full duplex
Jan 9 17:34:08	Solaris10	messages	Jan 9 17:34:07 Solaris10 genunix: [ID 408114 kern.info] /pci@0,0/pci106b,3f@6/input@1 (hid0) online
Jan 9 17:34:08	Solaris10	messages	Jan 9 17:34:07 Solaris10 genunix: [ID 936769 kern.info] hid0 is /pci@0,0/pci106b,3f@6/input@1
Jan 9 17:34:08	Solaris10	messages	Jan 9 17:34:07 Solaris10 usba: [ID 349649 kern.info] VirtualBox USB Tablet
Jan 9 17:34:08	Solaris10	messages	Jan 9 17:34:07 Solaris10 usba: [ID 912658 kern.info] USB 1.10 device (usb80ee,21) operating at full speed (USB 1.x) on USB 1.10 root hub: input@1, hid0 at bus address 2
Jan 9 17:34:07	Solaris10	messages	Jan 9 17:34:07 Solaris10 genunix: [ID 408114 kern.info] /pci@0,0/pci106b,3f@6/input@1 (hid0) removed

Figure 10: Latest Events

6 Snare Server

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

The Snare Server, as shown in Figure 11 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.

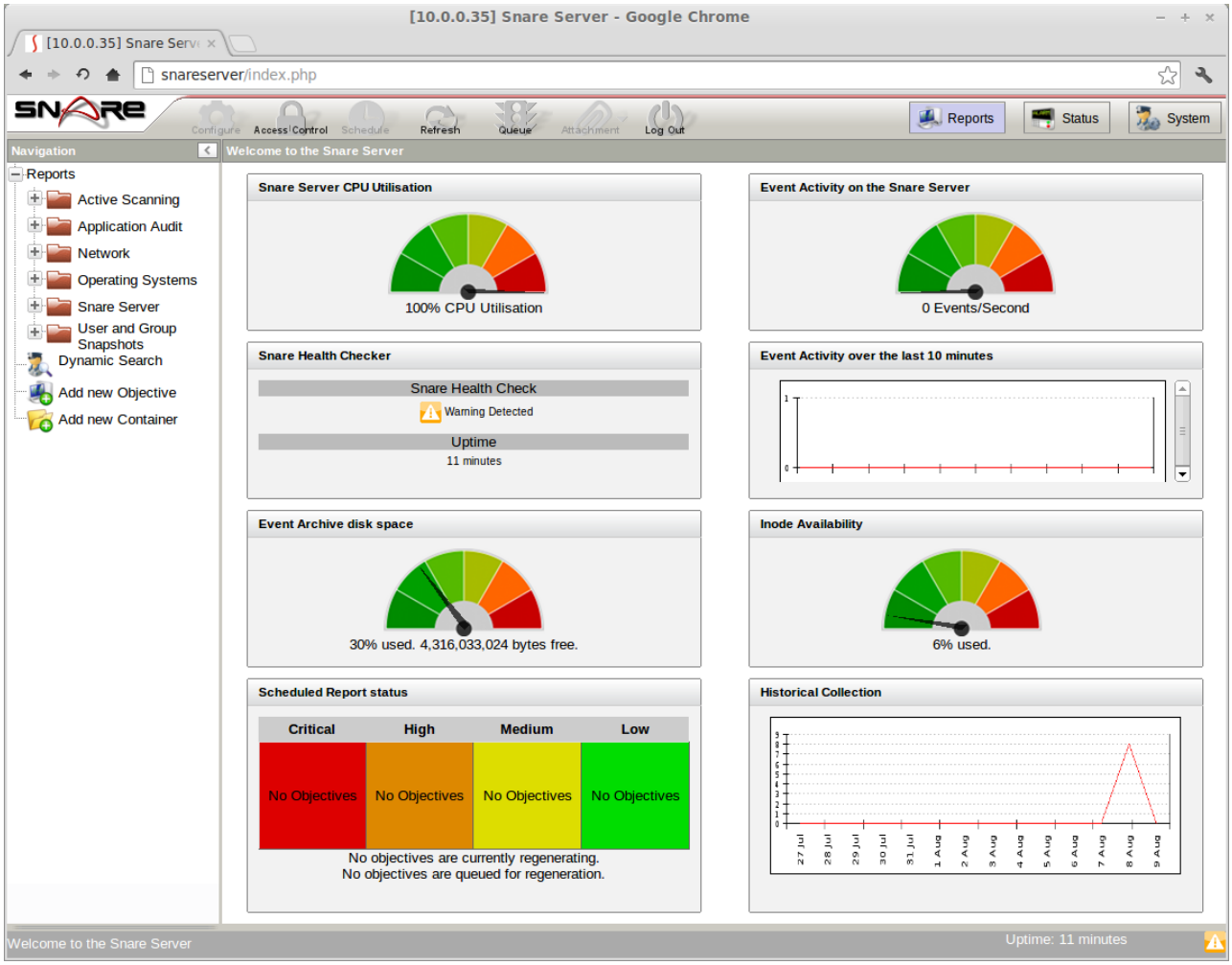


Figure 11: Welcome to the Snare Server

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 visit the Intersect Alliance website at https://www.intersectalliance.com/our-product/snare-server.

7 About InterSect Alliance

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

Intersect Alliance intend to continue releasing tools that enable users, administrators and clients worldwide to achieve a greater level of productivity and effectiveness in the area of IT Security, by simplifying, abstracting and/or solving complex security problems.

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

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

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

Asia Pacific +61 8 8213 1200 Adelaide Australia

Europe and the UK +44 (797) 090 5011

Email intersect@intersectalliance.com

Visit www.intersectalliance.com

Appendix A - Event Output Format

The ***Epilog*** daemon collects data from the identified logs 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:

```
sol10dev      SquidProxyLog       0         1152134522.688     857 127.0.0.1 TCP_MISS/200 12149 GET
http://www.intersectalliance.com/ - DIRECT/150.101.115.22 text/html
```

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

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

Appendix B - Snare Configuration File

Details on the audit configuration were discussed previously. The purpose of this section is to discuss the makeup of the configuration file. The Epilog configuration file is located in ***/etc/Snare/epilog***, and its location may not be changed. If the configuration file does not exist, the audit daemon will execute, but will not actively audit events until a correctly formatted configuration file is present, or unless specific instructions are passed to the audit module at load time. The format of the audit configuration file is discussed below.

Snare can be configured in several different ways, namely:

- Via the installation script (*Recommended*), or
- Via the web server (*Recommended*), or
- By manually editing the configuration file.

`[HostID]`	This item stores the hostname, if different from the assigned hostname.
`name=<hostname>`	This is the name of the host.
`[Output]`	By default, if no output section exists within the configuration file, the audit daemon will **NOT** send any audit data out. Note that audit events will be sent to all valid network destinations specified in the Output section.
`network=hostname:port:tcp` `network=hostname:port`	Audit data can be sent to a remote system using the UDP (default) or TCP protocol. Data will be sent to the remote host, and network port specified here. Each additional host must be specified on a new line. Caching will be enabled for the first host only if TCP is enabled.
`[Input]`	This section identifies the log files to be monitored.
`log=LogType:/fully/qualified/file/name` `log=/fully/qualified/file/name`	The audit daemon will continuously monitor the identified files by name and send data to the network destinations specified within the [Output] section. Spaces are valid characters. Note that if the audit daemon is not running as root, the file must be readable by the user under which the audit daemon is running. The 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 4.3.
`[Objectives]`	This section describes the format of the objectives. Objectives are composed of *the match term* : a filter expression, and is defined in extended regular expression format. Note that whitespace will be trimmed from the start and end of items, but will be assumed to be valid when bracketed by other characters.
`match=.*more.*`	Include any lines that contains the word “more”
`match!=.*less.*`	Exclude any lines that contains the word “less”
`[Remote]`	This subkey stores all the remote control parameters.
`allow=1`	"Allow" is an integer, and set to either 0 or 1 to allow remote control user interface. 1= allow remote, 0=do not allow.
`listen_port=6162`	This value is the web server port. A missing "listen_port" will default the web server to port 80.
`restrict_ip=10.0.0.1`	This is an IP address, that will be used so that this address will be the only host that is allowed to connect to the web server. If this item does not exist, then the web server will not restrict by IP address.
`accesskey=Snare`	This value is the password that is used to log into the Snare web server. If this item does not exist, then a password will not be requested when connecting to the web server. The password is encrypted when stored in the Snare.conf, using the standard UNIX “crypt” facility, with salt