

SNARE

System iNtrusion Analysis & Reporting Environment

Guide to Snare Epilog for Windows



01001100111010001110010 00000000
110100010101000101000 00000000
10101000101101001010 00000000
001111110100111010 00000000

INTERSECT
ALLIANCE

Documentation History

Version No.	Date	Edits	By whom
1.0	16 August 2006	First release for the Guide to Snare Epilog for Windows documentation.	David Mohr
1.1	16 June 2008	Updates for new supported features	David Mohr

© 1999-2008 Intersect Alliance Pty Ltd. All rights reserved worldwide.

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

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

About this guide

This guide introduces you to the functionality of 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.....	4
2 Overview of Snare Epilog for Windows.....	5
3 Installing and running Epilog.....	6
3.1 Epilog installation.....	6
3.2 Running Epilog.....	7
4 Setting the audit configuration.....	8
4.1 Logging control.....	8
4.2 Log configuration.....	11
5 Audit event viewer functions.....	13
6 Remote control and management functions.....	14
7 Snare Server.....	16
8 About Intersect Alliance.....	18
Appendix A - Event output format.....	19
Appendix B - Epilog Windows registry configuration description.....	20

1 INTRODUCTION



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

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

The development of 'Snare Epilog for Windows' allows for text-based event logs to be collected from the Windows NT/2000/2003/XP operating systems and then forwarded to a remote audit event collection facility. Epilog is designed to compliment the Snare for Windows agent by allowing programs and services that do not use the inbuilt event log system to have their log files collected and analyzed. Snare Epilog for Windows will also allow a security administrator to fully remote control the application through a standard web browser if so desired. Epilog has been designed in such a way as to allow the remote control functions to be easily effected manually, or by an automated process.

The overall project is called 'Snare' - **System iNtrusion Analysis & Reporting Environment**. The '**Snare Server**' is a commercial release of software beneficial to organizations that wish to collect from a wide variety of Snare agents and appliances such as firewalls or routers.

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

2 OVERVIEW OF SNARE 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. *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.* 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 Event output format on page 19.* 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
```

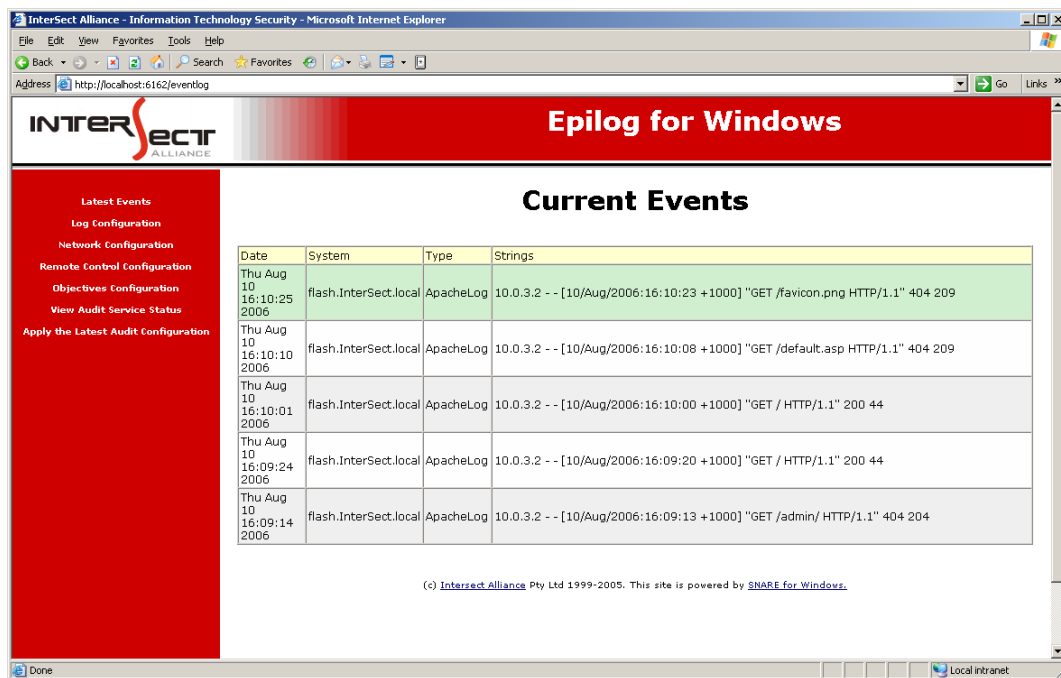


Figure 1 Main Event Window

3 INSTALLING AND RUNNING EPILOG

3.1 EPILOG INSTALLATION

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 NT/2000/2003 or XP.

Installation of the main component (*Epilog*) is undertaken as follows:

1. Download the **EpilogSetup-{Version}.exe** file from the Intersect Alliance website.
2. To use the installation wizard: Ensure you have administrator rights, double-click the **EpilogSetup-{Version}.exe** file. This is a self extracting archive, and will not require WinZip or other programs.

OR

To use a silent install: Ensure you have administrator rights, open a command prompt and browse to the directory where the set up program is stored. Using the "/verysilent" option, run the file:

```
EpilogSetup-{Version}.exe /verysilent
```

This will install the Epilog component with the default options and will not display any pop-up windows. This option is suitable for packaging and non-interactive installations. All existing settings will be maintained using this install method.

3. 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 in Figure 2.
4. Once the installation process has completed the system should be rebooted so that all configurations are applied correctly.

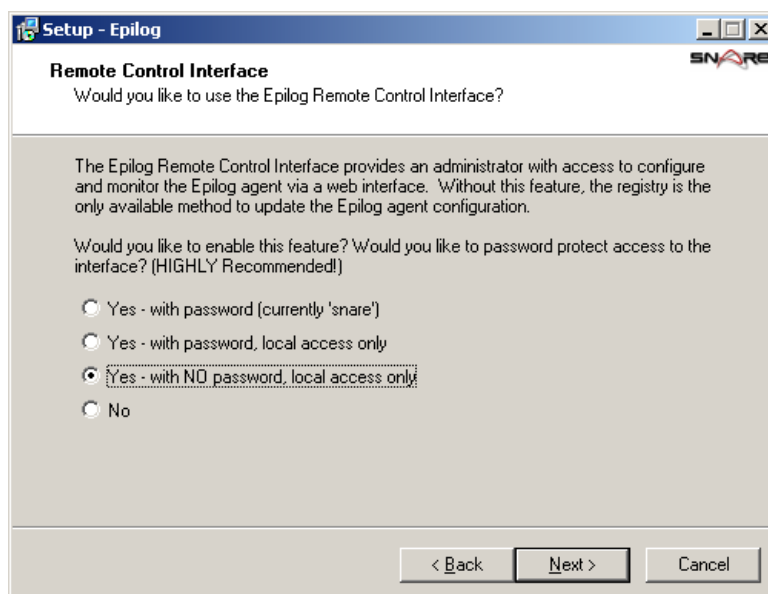


Figure 2 Epilog password dialog box

3.2 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 **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 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 *Appendix B - Windows registry configuration description on page 20*.

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 (see Figure 3).

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 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.*
- 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.
- Note that the following options are only available to users who purchase a Snare Server. These are not part of the Open Source toolset. 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 guarantee message delivery.
 - 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 - Encrypt messages between the agent and the Snare Server. This option requires matching Remote Access Passwords on both the agent and the Snare Server.

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

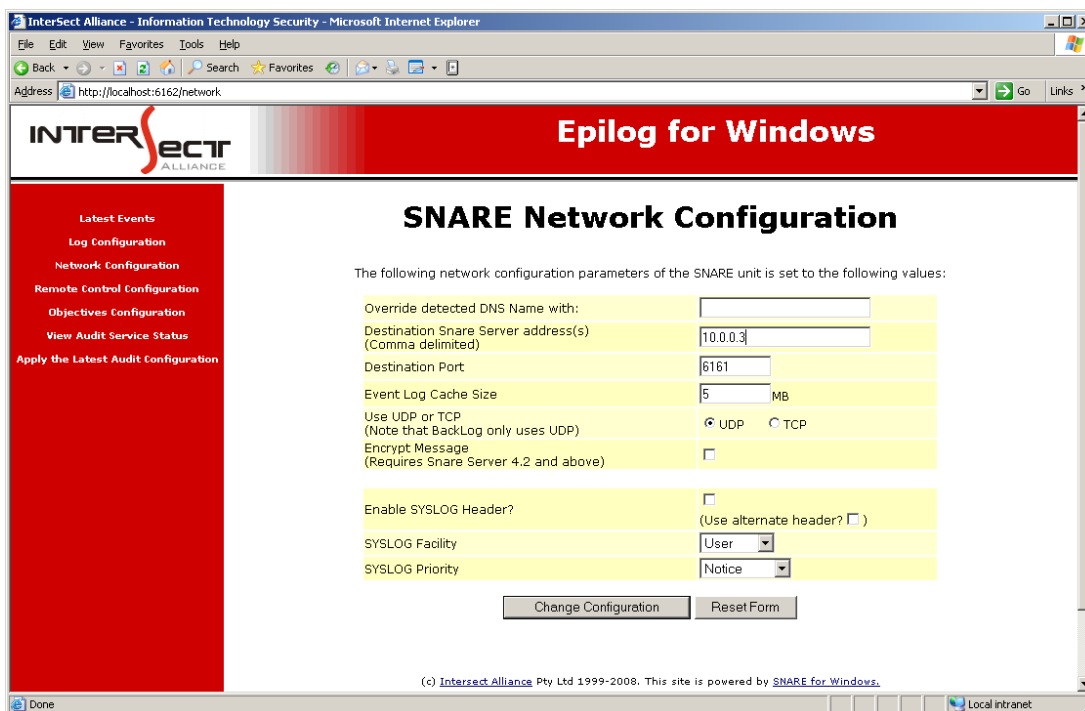


Figure 3 Network Configuration Window

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.

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.

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

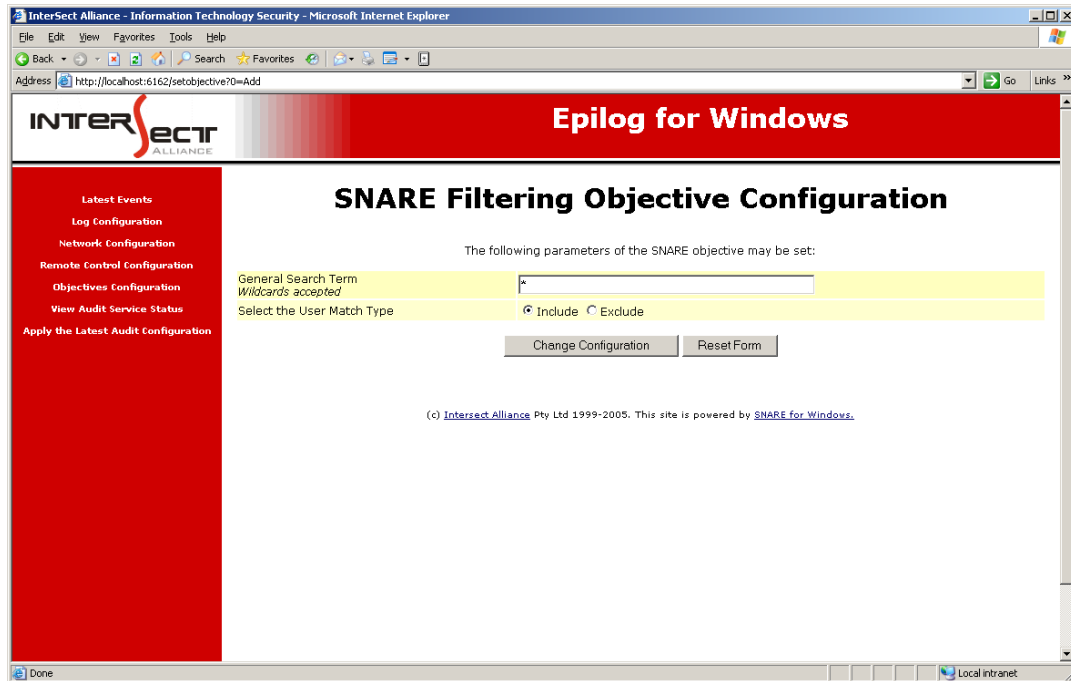


Figure 5 Create or Modify an Objective Window

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 Figure 6 below.

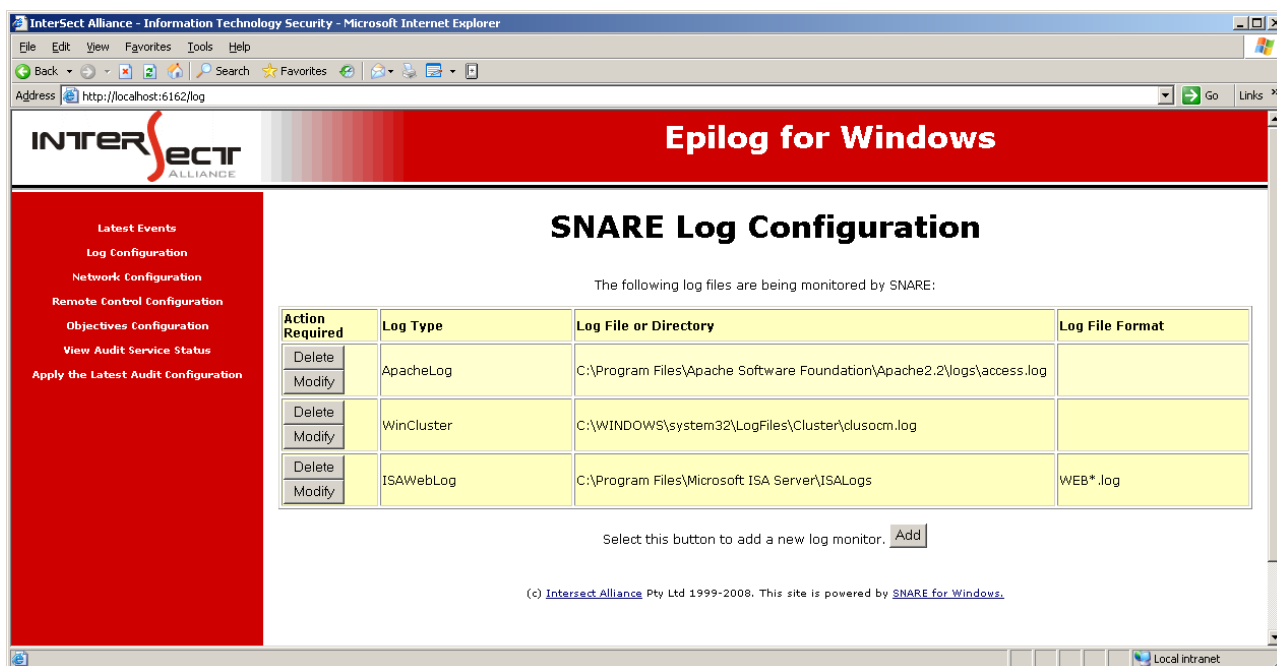


Figure 6 Log Configuration Window

From this page, log monitors can be added, deleted and modified. The 'Log File or Directory' field 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. Spaces are valid characters. The 'Log File Format' field allows you to specify the file name or pattern you are targeting. Wildcards are accepted ('*' and '?') and 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.

Once each log watch is configured, Epilog for Windows will then 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 File Format is used, Epilog will also watch for new filenames, dynamically updating the file watch each time a new file becomes available. 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

Once the above settings have been finalized, clicking 'Change Configuration' on the Remote Control Interface will save the configuration to the registry. However, 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 (as shown in Figure 7). 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.

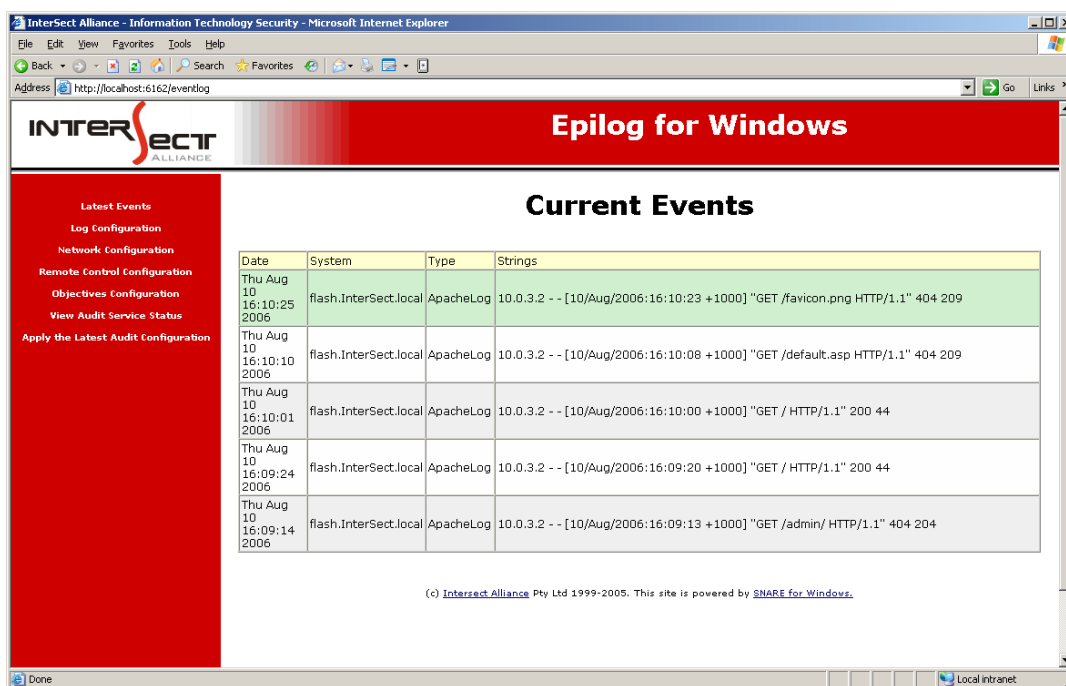


Figure 7 Latest Events Window

6 REMOTE CONTROL AND MANAGEMENT FUNCTIONS

The *Epilog* service is a separate standalone component of the Epilog system, as described in *Overview of Snare Epilog for Windows* on page 5. 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 8. This will display whether the *Epilog* service is active

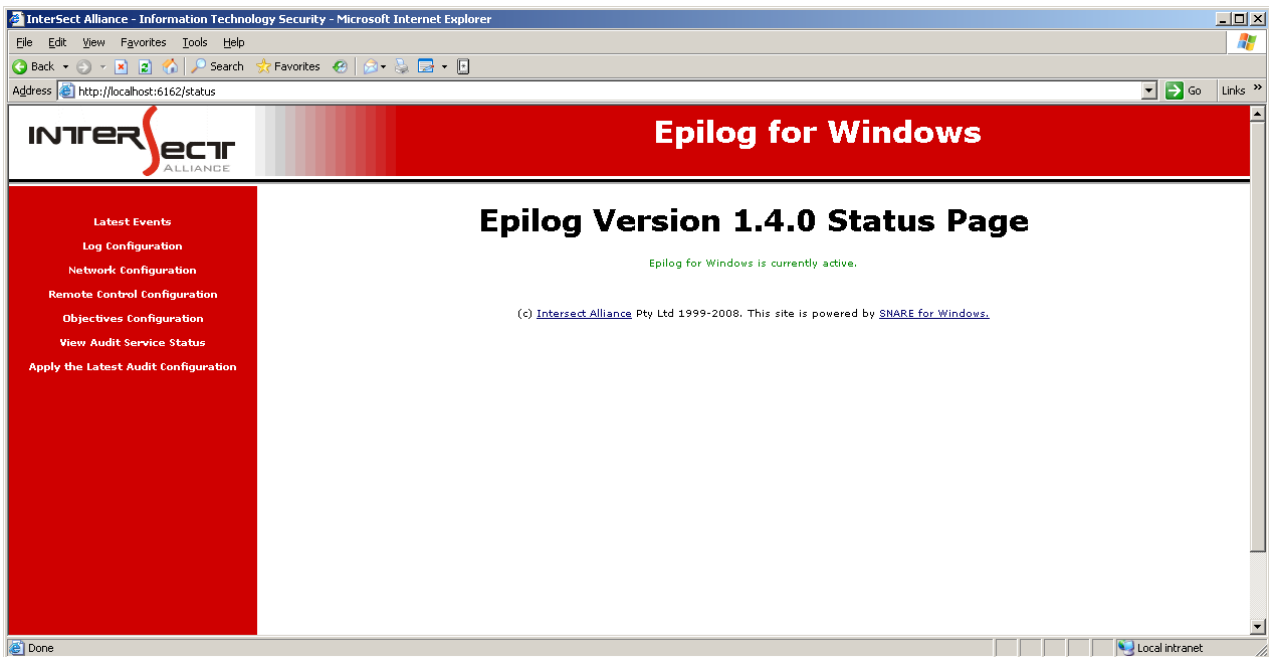


Figure 8 Audit Status Window

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 9 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.

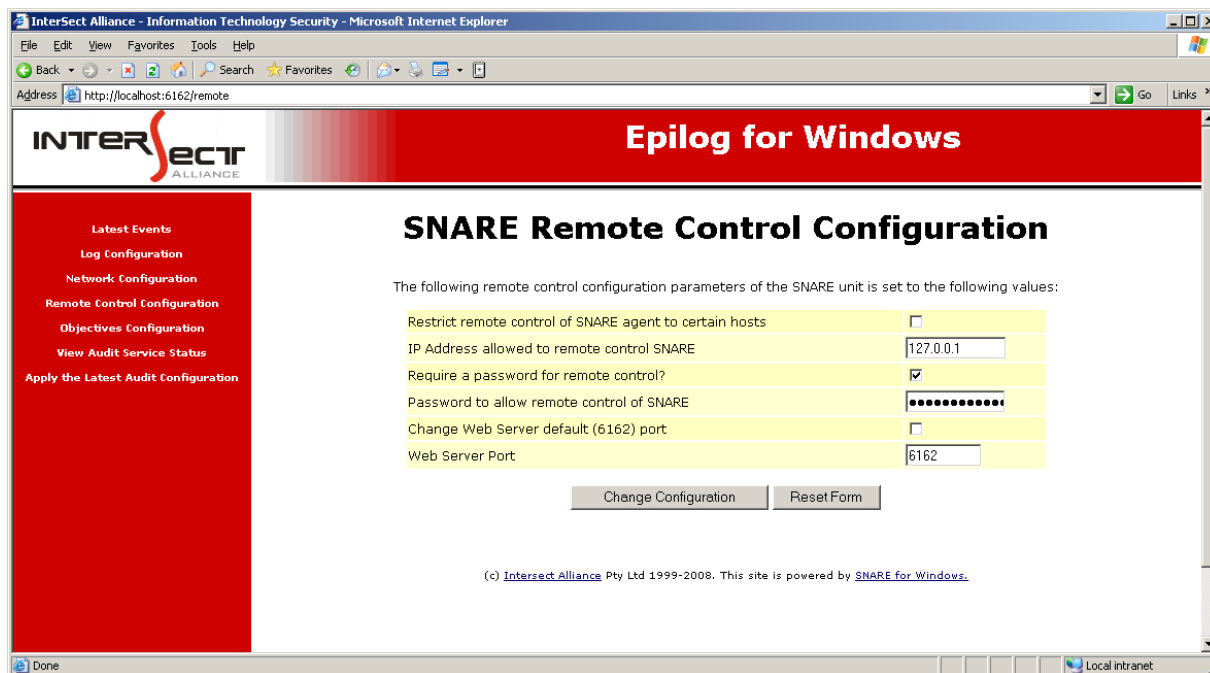


Figure 9 Remote Control Window

7 SNARE SERVER



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

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

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

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

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

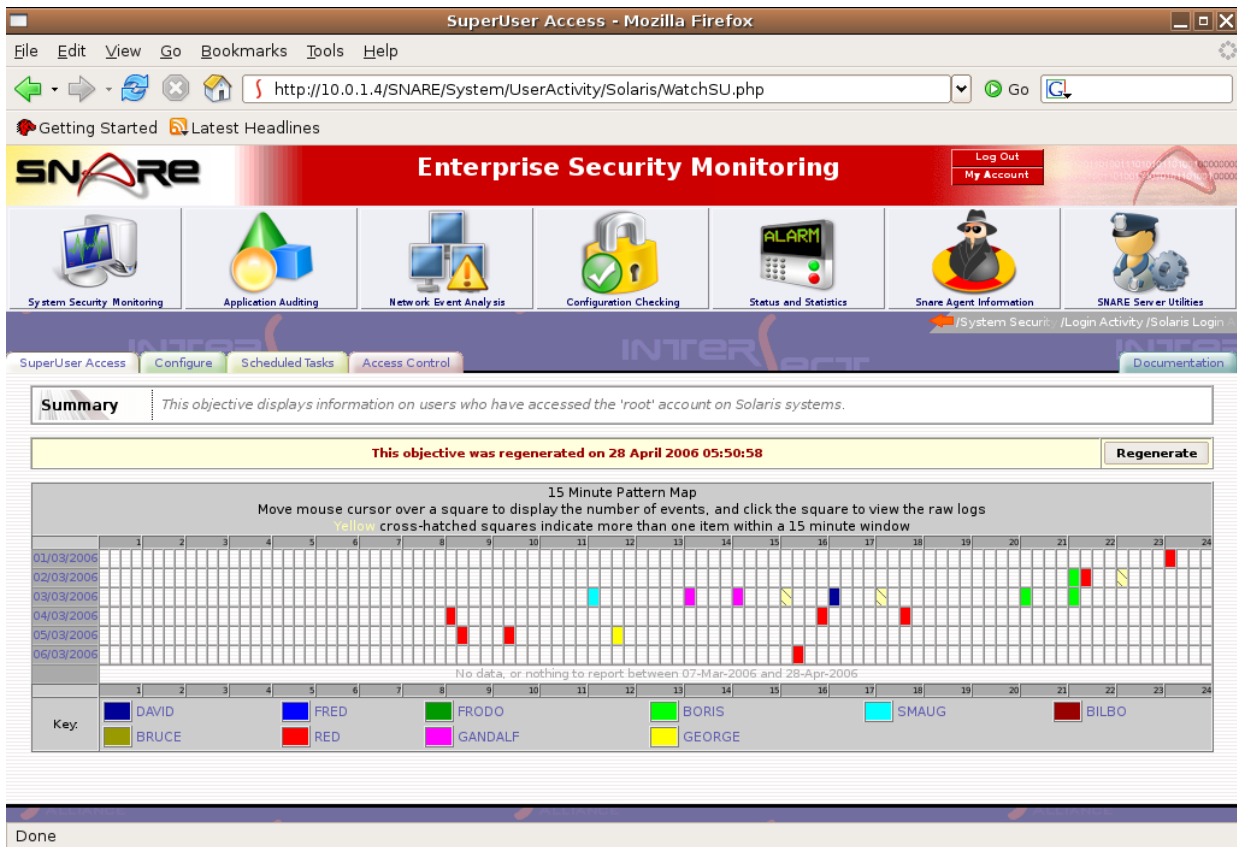


Figure 10 Screen shot from the Snare Server

8 ABOUT INTERSECT ALLIANCE



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

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

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

APPENDIX A - EVENT OUTPUT FORMAT

The *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.
[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). 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.
[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]

Log#
(where # is a serial number)

This subkey stores all the log monitors.

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 valid, except at the start of the term.