SNARE

System iNtrusion Analysis & Reporting Environment

Guide to Snare for OSX v1.1

INTERSECT ALLIANCE

About this guide

This guide introduces you to the functionality of the Snare Agent for the OSX operating system. Snare for OSX provides an event, auditing subsystem for the OSX systems, and facilitates objective-based filtering, and remote audit event delivery. Snare for OSX will also allow a security administrator to fully remote control the application through a standard web browser if so desired. Snare has been designed in such a way as to allow the remote control functions to be easily effected manually, or by an automated process.

Other guides that may be useful to read include:

- Snare Server User's Guide.
- The Snare Toolset - A White Paper.

Table of contents:

1 Introduction

The team at InterSect Alliance have experience with auditing and intrusion detection on a wide range of platforms - Solaris, Windows, Android, AIX, 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.

'Snare for OSX' allows event logs from the OSX subsystem to be collected from the operating system, and forwarded to a remote audit event collection facility after appropriate filtering. Snare for OSX will also allow a security administrator to fully remote control the application through a standard web browser if so desired. Snare 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 Snare for OSX agent is released as an Enterprise version only. Other Snare agents are also available including Snare for Solaris, Linux, AIX, IRIX, IIS, Apache, MSSQL, Epilog and Windows. The agents are capable of sending data to a wide variety of target collection systems, including our very own **'Snare Server'**. See *Chapter 5 Snare Server* for further details.

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

2 Overview of Snare for OSX

Snare operates through the actions of three complementary components:

- The native OSX audit subsystem
- The user-space audit daemon (auditd)
- The Snare 'dispatcher' applications.

The audit daemon, and kernel component act in concert to configure the underlying audit subsystem, and extract events of interest from the operating system.

Snare for OSX operates as an 'audit dispatcher' application that receives the audit log data, with Snare directing auditd what events to selectively filter out that you are not interested in, formats the resulting data into something that is more suited to follow-on processing, and delivers it to one or more remote systems over the network.

Snare formats the audit log data into a series of 'tokens'. Two different field separators are used in order to facilitate follow-on processing - TABS separate 'tokens', and COMMAS separate data within each token. This format is further discussed in the section on the Snare output format. The result is that a raw event, as processed by Snare, may appear as follows:

```
snares-MacBook-Air.local AppleBSM 1 header,283,11,open(2) - write,0,Wed Mar 19
10:44:32 2014, + 857 msec  argument,2,0x1,flags    path,/Users/snare/Library/Saved
Application State/com.apple.Safari.savedState/data.data
path,/Users/snare/Library/Saved Application
State/com.apple.Safari.savedState/data.data
attribute,100600,snare,staff,16777218,713775,0  subject,
nnare,snare,staff,snare,staff,231,100003,50331650,0.0.0.0 return,success,25
trailer,283 snareseq,11076
```

Snare also incorporates a tiny embedded web server, the Remote Control Interface, which allows administrators to remotely control which events are collected and reported. The Remote Control Interface also provides information on users, groups, and group membership on the local machine, which can be used to satisfy various regulatory security requirements.

Snare for OSX is known to work on OSX 5.7 (Lion), OSX 5.8 (Snow Lion), OSX 5.9 (Mavericks).

3 Installing and running Snare

3.1 Snare installation

Snare is available as an Self installing package that enables it to be installed and removed with relative ease on OSX Systems.

WHAT YOU NEED...

- An appropriate OSX Distribution.
- The SnareOSX package in binary format downloaded from the InterSect Alliance website. Snare for OSX provides the infrastructure required to filter, format and distribute audit log data to one or more central log collection systems.

HOW TO... Install Snare for OSX binary package.

There are two methods to install the Snare OSX Binary package. The first method uses the graphical OSX environment, the second method uses the command line installer.

To use the graphical environment:

1. Double click the package `SnareOSX-1.1.0.pkg` in the GUI
2. Follow the on screen instructions. This will install Snare for OSX and start/restart the audit daemon(auditd).
3. Restart the machine

To use the command line

1. Logon as root user, i.e. at the command prompt enter the command `sudo -s` and enter the root password when prompted. Issue the command, as root:
   `installer -pkg SnareOSX-1.1.0.pkg -target /`
   This will install Snare for OSX and start/restart the audit daemon (auditd).
2. Restart the machine

HOW TO... Remove Snare for OSX binary package (if required).

OSX does not provide facilities for uninstallers for pkg based applications. Hence Intersect Alliance has provided an uninstall script to completely uninstall Snare for OSX if required.
The uninstall script requires no confirmation. Hence once run it will uninstall Snare for OSX without any prompts. To uninstall Snare for OSX:

1. Logon as root user, ie at the command prompt enter the command:

   `sudo -s` and enter the root password.
2. Run the command:
   `/Applications/Utilities/SnareAgent\ WebConsole.app/\ Contents/Resources/uninstall.sh`

3.2 Running Snare

Once the Snare agent is installed, it will begin to operate using a very simple configuration. The Remote Control Interface is accessible by entering http://localhost:6161 in the web browser as shown in Figure 1: Remote Control Configuration, or by running the SnareAgent WebConsole application which is installed as part of the installation (It can be found in the Application/Utilities Folder) By default the Remote Control Interface is password protected for security reasons. The default username and password are:

Username: snare
Password: snare

Figure 1: Remote Control Configuration

4 Setting the audit configuration

4.1 Audit configuration

The Snare configuration is stored as */etc/security/snare.conf*. This file contains all the details required by Snare to configure the audit subsystem to successfully execute. Failure to specify a correct configuration file will prevent Snare from running.

The configuration of */etc/security/snare.conf* can either be changed directly, or by modifying the objectives via the web server embedded within Snare, i.e. Remote Control Interface. The most effective and simplest way to configure */etc/security/snare.conf* is to use the Remote Control Interface. It operates completely in memory, and does not rely on any external files, other than the */etc/audit/snare.conf* file. The Remote Control Interface component ***IS*** turned on by default.

The Remote Control Interface provides a number of capabilities including:

- Network Configuration
- Remote Control Configuration
- Objectives Configuration
- Viewing Recent Events
- User and Group meta-data

Tip: Manual editing of the snare.conf configuration file 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 Interface to modify security objectives or selected events, may result in manual configuration file changes being overwritten. Details on the configuration file format can be viewed in Appendix A – Configuration File Description.

HOW TO... Remote Audit Monitoring

The Remote Control Interface can be turned off by tweaking the default */etc/security/snare.conf* file. You can either edit the */etc/security/snare.conf* file directly, commenting the 'allow=1' line under the '[Remote]' section, or by setting this value to 0. Be sure to restart the agent, for the change to take effect. The agent can be restarted by sending a HUP signal,i.e.,

```
>killall -HUP snarecore
```

4.2 Network Configuration

The audit configuration parameters to use are found in the 'Network Configuration' link in the Remote Control Interface of the Snare for OSX agent, displayed below in Figure 2.

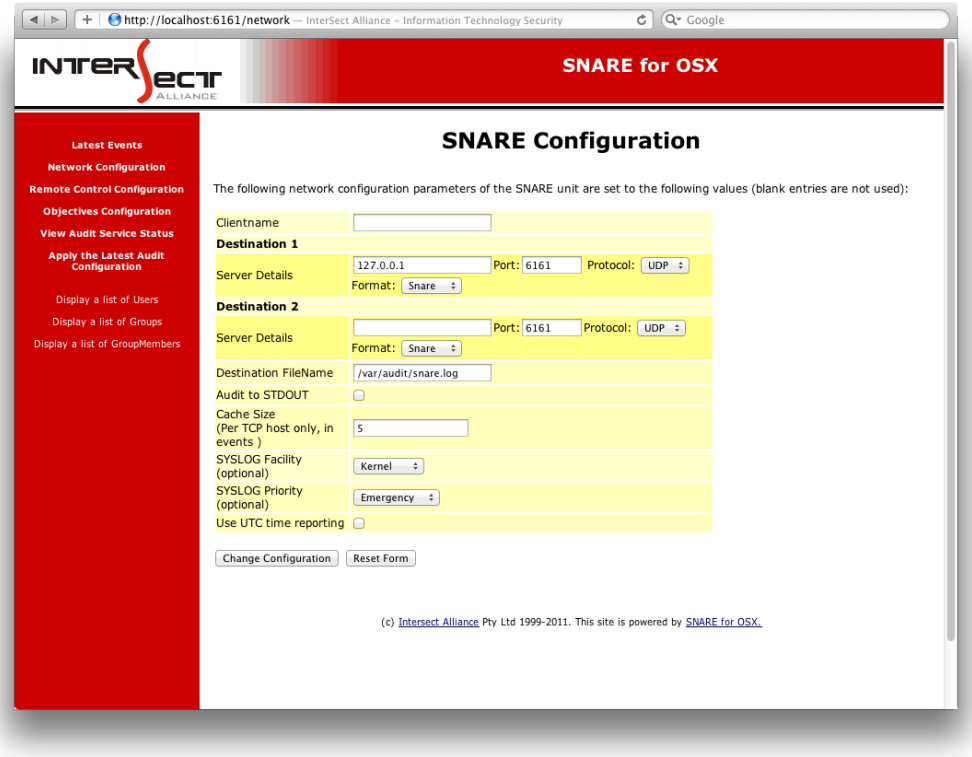


Figure 2: The Network Configuration page

The network configuration parameters available are as follows:

- ***Clientname:*** Can be used to override the name that is given to the host. Unless a different name is required to be sent in the processed event log record, leave this field blank. The default is to use the fully qualified name for the machine.
- ***Destination:*** Snare for OSX can send audit events to one or more network destinations. Enter a DNS name, or IP address for each planned destination. Snare can send data either to a Snare-compatible server, or a SYSLOG compatible destination. Please be aware that most SYSLOG servers are incompatible with the extremely high volumes of data Snare is capable of generating.

  Protocol: Select the protocol you would like Snare to use when sending events. Using TCP or SSL will guarantee message delivery. Using SSL will use an encrypted connection to the server.

  Format: Select this option if the requirement is that the event records need to be in a specific format. This feature will allow the event log record to be formatted so it is accepted by a SYSLOG or a Snare server.

Note: The agent will override the specified format in some cases. Specifying port 6161 will force the use of Snare format. Specifying a port of 514 will force the use of the Syslog format.

- ***Destination FileName (optional):*** Output logging to disk as well as the network.
- ***Allow SNARE to automatically set audit configuration:*** By default, Snare will take control and manage your audit event settings for you. Normally on a Unix system, you will need to modify the file */etc/audit/audit.rules* in order to establish a new monitored event. Snare has the capability to 'turn on' event auditing in response to the objectives you set within the Remote Control Interface. We recommend that this parameter is enabled.
- ***Audit to STDOUT:*** This option is useful for debugging and allows audit events to be sent to STDOUT, useful if you run the snarecore binary manually from the console.
- ***Cache size:*** Allow Snare 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 until it is sent or the size of the cache exceeds the specified allotment, in which case the oldest message is removed. If the agent is restarted, any cached messages are lost.
- ***SYSLOG Facility (optional):*** If you are sending your data to a SYSLOG server, specifies the subsystem that produced the message. The list displays default facility levels.
- ***SYSLOG Priority (optional):*** If you are sending your data to a SYSLOG server, the agent can be configured to use a static or dynamic priority level.
- ***Use UTC time reporting:*** Enables UTC (Coordinated Universal Time) timestamp format for events instead of local machine time zone format.

4.3 Remote Control Configuration

The Snare for OSX agent can be controlled remotely by administrators, if required. Remote control is enabled by default, but can be disabled by modifying the file */etc/security/snare.conf* as per instructions in section 4.1 of this guide.

The remote control page is shown in Figure 3 below.

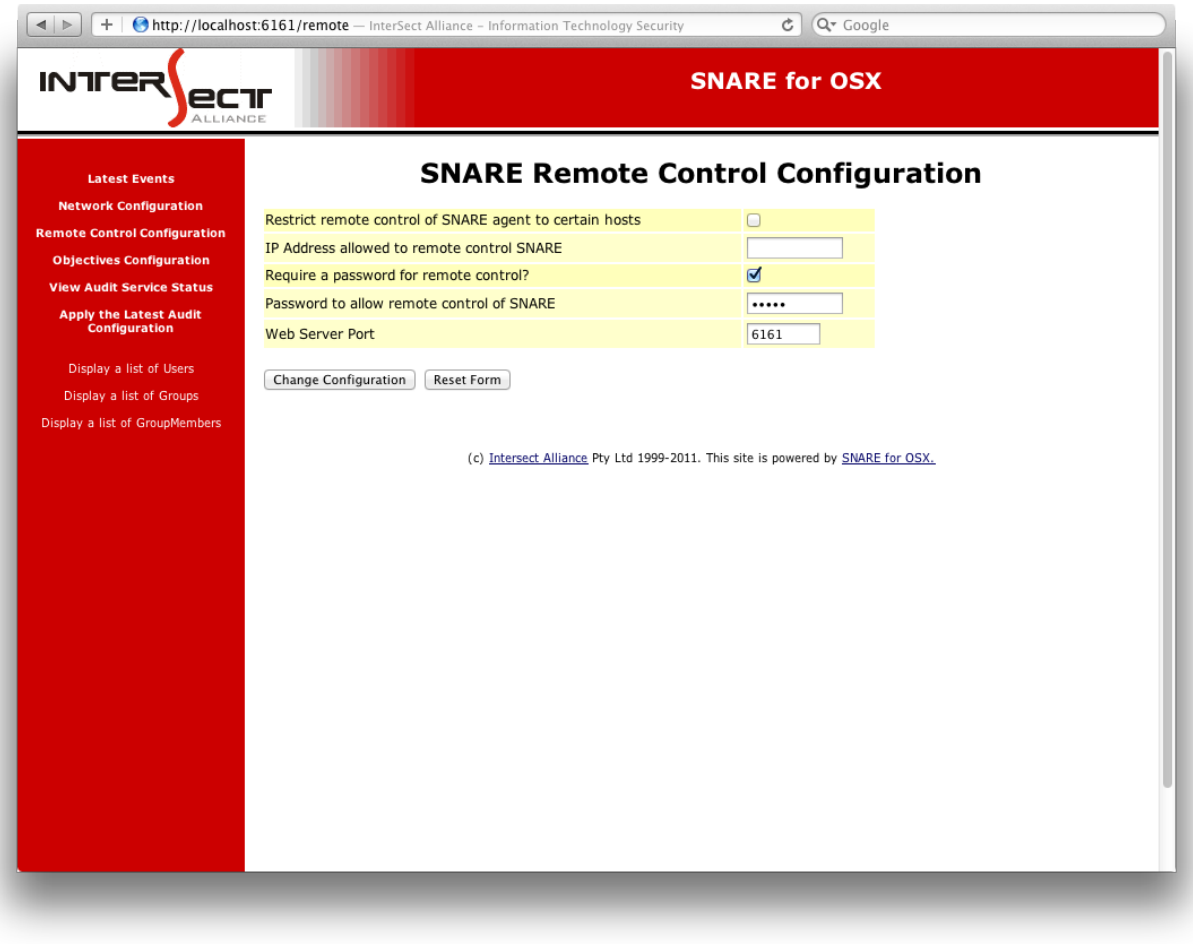


Figure 3: Remote Control

The parameters which may be set for remote control operation include:

- ***Restrict remote control of SNARE agent to certain hosts:*** By default SNARE allows any IP address to connect to the remote control interface. Enabling this option restricts connections to the remote control interface to the ip given in the following option.
- ***IP Address allowed to remote control SNARE:*** Remote control actions may be limited to a given host. This host, entered as an IP address will only allow remote connections to be effected from the stated IP address. Application-level firewall capabilities are also available, which block users from accessing the Remote Control Interface from any IP address other than the one specified.
- ***Require a password for remote control?:*** Indicate whether a password will be set so that

only authorised individuals may access the remote control functions. Highly recommended.

- ***Password to allow remote control of SNARE:*** If above checkbox is checked, password must be set. A password of appropriate strength should be set for the remote control facility.
- ***Web Server Port:*** An optional port that the Remote Control Interface listens on, can be specified. Users of the Snare Server should generally leave this as 6161, in order to take advantage of the Snare Server's user and group audit capabilities.

4.4 Objectives configuration

A major function of the Snare system is to filter events. This is accomplished via the auditing 'objectives' capability. The term 'objective' is used within Snare Agents to describe an 'auditing goal'. It is generally made up of events that Snare should watch for, a filter term containing a 'token' and a criticality level.

Event Objectives

The following parameters may be set on the Filtering Objective Configuration page as show in Figure 4:

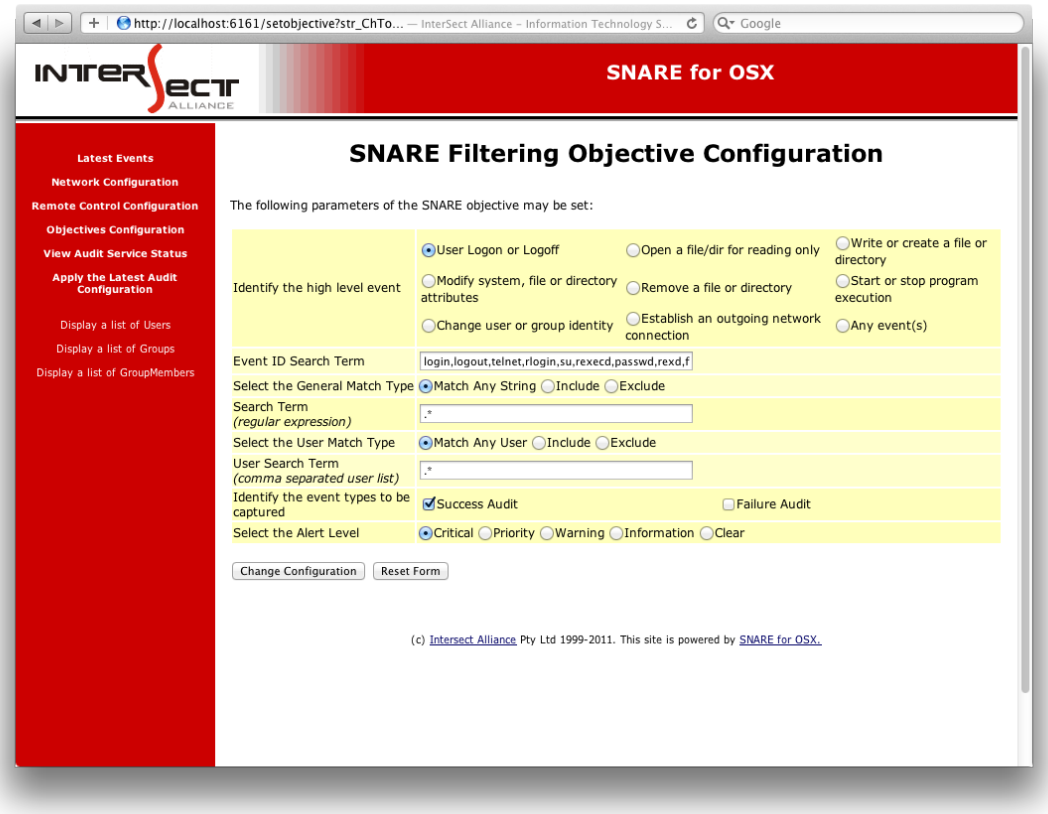


Figure 4: Creating an event objective

- ***Identify the high level event:*** Each of the objectives provides a high level of control over which events are selected and reported. Events are selected from a group of high level requirements, and further refined using selected filters. Events are generally grouped into the following:
    - User Logon or logoff:
      login, logout, telnet, rlogin, su, rexecd, passwd, rexd, ftpd, admin_authenticate, ssh
    - Modify system, file or directory attributes:
      chmod, fchmod, chown, fchown, mctl, fcntl, lchown, aclset, faclset
    - Change user or group identity:
      setgroups, setpgrp, setuid, setgid, setauid, setreuid, setregid, setuid, osetpgrp
    - Open a file/dir for reading only:
      open_r, readlink
    - Remove a file or directory:
      rmdir, unlink
    - Establish an outgoing network connection:
      connect, shutdown, setsockopt
    - Write or create a file or directory:
      open_rc, open_rt, open_w, open_wc, open_wtc, open_rw, open_rwt, create, mkdir,mknod,xmknod,link,symlink,rmdir,unlink,rename,truncate,ftruncate
    - Start or stop program execution:
      exec,execve

  In addition, any event that can be generated by the OSX audit subsystem can be specified (comma separated) by using the 'Any Event(s)' high level group.

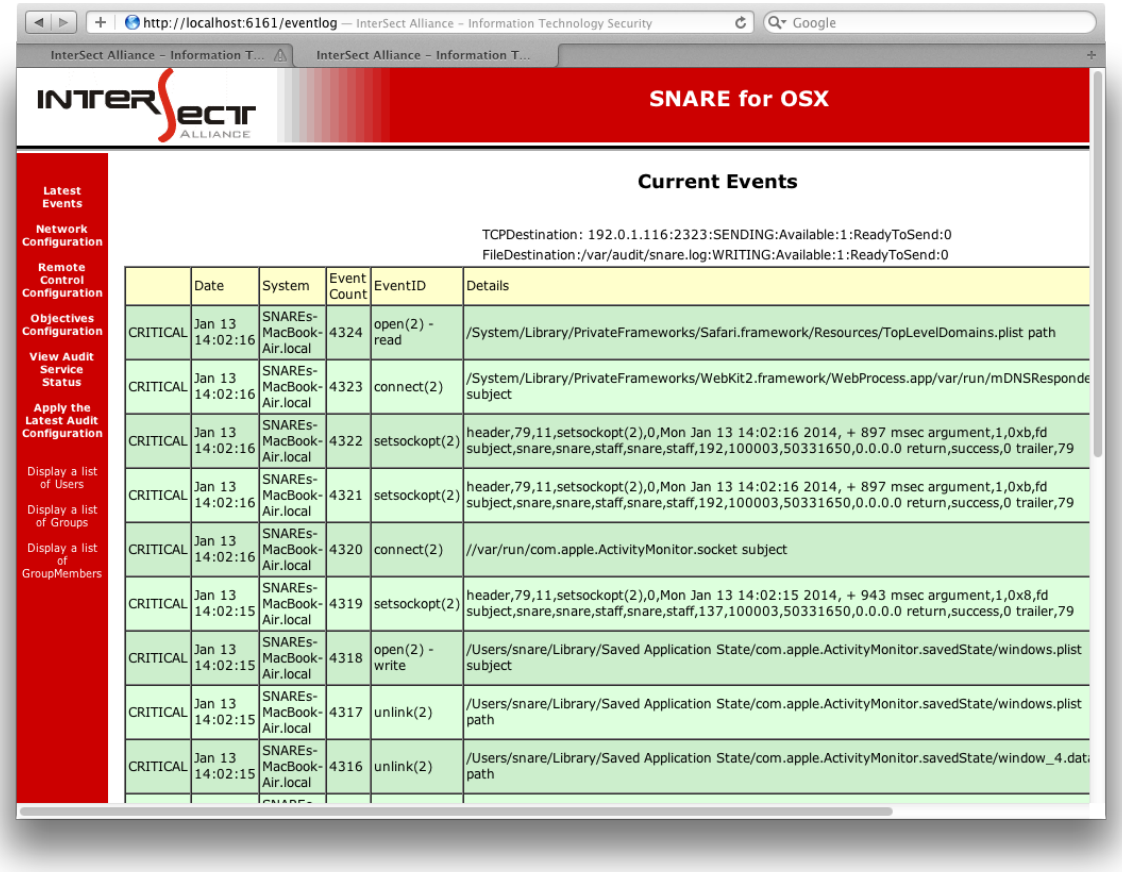
  Tip: Turning on file-related events can produce a very high volume of audit events on some systems, and therefore result in a considerable amount of CPU time being used by Snare and the audit subsystem.
- ***Event ID Search Term:*** If 'Any Event(s)' is selected as the high level event, then add a comma separated list of OSX audit events to search for.
- ***Search Term:*** A filter term containing a 'token' which appears within the events of interest, and the search criteria that Snare should use to include or exclude the event. For example, a search term of: `/etc/.*` Would match any event which mentions any file in `/etc`
- ***User Search Term:*** A filter term containing a users the objective should match. For example using: `root,snare` would cause the objective to match if users root or snare caused the event. Additionally the value .* may be used to match any user.

The order of the objectives is not important. Once the above settings have been finalized, the configuration may be saved to the configuration file, via the **Change Configuration** button. However, to ensure the audit daemon has received the new configuration, the **Apply the Latest Audit Configuration** menu item should be selected.

The objective configuration page supplied as part of the web based remote control is intended as a way to enable users to commence audit functions reasonably quickly. It is not intended for power users. A far more powerful and functional way is to manually control the */etc/security/snare.conf* file. This is described in more detail in Appendix A, and is intended for users who have a very detailed knowledge of OSX administration and security. It is NOT recommended for novice users.

4.5 Display of Latest Events / Destination Status

A small rotating cache of audit events is kept by the Snare for OSX web server. Clicking on the **Latest Events** menu item on the left hand side of the Remote Control Interface, as shown in Figure 7, will display twenty of the most recent events.



	Date	System	Event Count	EventID	Details
CRITICAL	Jan 13 14:02:16	SNAREs-MacBook-Air.local	4324	open(2) - read	/System/Library/PrivateFrameworks/Safari.framework/Resources/TopLevelDomains.plist path
CRITICAL	Jan 13 14:02:16	SNAREs-MacBook-Air.local	4323	connect(2)	/System/Library/PrivateFrameworks/WebKit2.framework/WebProcess.app/var/run/mDNSResponde subject
CRITICAL	Jan 13 14:02:16	SNAREs-MacBook-Air.local	4322	setsockopt(2)	header,79,11,setsockopt(2),0,Mon Jan 13 14:02:16 2014, + 897 msec argument,1,0xb,fd subject,snare,snare,staff,snare,staff,192,100003,50331650,0.0.0.0 return,success,0 trailer,79
CRITICAL	Jan 13 14:02:16	SNAREs-MacBook-Air.local	4321	setsockopt(2)	header,79,11,setsockopt(2),0,Mon Jan 13 14:02:16 2014, + 897 msec argument,1,0xb,fd subject,snare,snare,staff,snare,staff,192,100003,50331650,0.0.0.0 return,success,0 trailer,79
CRITICAL	Jan 13 14:02:16	SNAREs-MacBook-Air.local	4320	connect(2)	//var/run/com.apple.ActivityMonitor.socket subject
CRITICAL	Jan 13 14:02:15	SNAREs-MacBook-Air.local	4319	setsockopt(2)	header,79,11,setsockopt(2),0,Mon Jan 13 14:02:15 2014, + 943 msec argument,1,0x8,fd subject,snare,snare,staff,snare,staff,137,100003,50331650,0.0.0.0 return,success,0 trailer,79
CRITICAL	Jan 13 14:02:15	SNAREs-MacBook-Air.local	4318	open(2) - write	/Users/snare/Library/Saved Application State/com.apple.ActivityMonitor.savedState/windows.plist subject
CRITICAL	Jan 13 14:02:15	SNAREs-MacBook-Air.local	4317	unlink(2)	/Users/snare/Library/Saved Application State/com.apple.ActivityMonitor.savedState/windows.plist path
CRITICAL	Jan 13 14:02:15	SNAREs-MacBook-Air.local	4316	unlink(2)	/Users/snare/Library/Saved Application State/com.apple.ActivityMonitor.savedState/window_4.dat path

Figure 7: Latest Events

Additionally this page shows the status for each Destination that was configured for logging. An example of this destination status is:

TCPDestination: 10.1.1.30:6161:CONNECTED:Available:1:ReadyToSend:1

This information can be used to help debug potential logging issues. The status can be explained as follows:

- **Log destination Type: ie: TCPDestination**
  The protocol of the remote connection. Possible values are TCPDestination, UDPDestination, SSLDestination or FileDestination
- **Host/Port: ie: 10.1.1.30:6161**
  The host ip/name and port that logs will be sent too.
- **The current State of the connection: ie: CONNECTED**
  This field indicates what snare is currently doing with the connection. You will see many different states including:
  - INITIAL
    The remote log location is about to begin setup
  - RESOLVING
    DNS resolution for a hostname is occurring
  - RESOLVE_DELAY(x)
    DNS resolution failed, a retry will occur in X seconds
  - CONNECTING
    Snare is trying to connect to the destination
  - CONNECT_FAILED
    The connection to the destination failed
  - CONNECT_DELAY(x)
    Connecting to the remote end failed, it will be retried again in X seconds
  - CONNECTED
    Snare has an active connection to the destination
  - SENDING
    Snare is currently sending logs to the destination
  - DISCONNECTED
    The destination has disconnected the snare agent.. a reconnection will occur automatically.
  - HANDSHAKE
    A SSL/TLS Handshake is in progress
  - HANDSHAKE_FAILED
    The SSL/TLS Handshake failed
  - OPENING
    Opening a a file destination is inprogress
  - WRITING
    Writing is occurring to a file
  - WRITE_FAILED
    A write to file failed

- CLOSED
  A file has been closed

Additionally two other statuses give instant feedback about what Snare is doing:

- ***Available***
  - Indicates if Snare can use the destination to send logs. A value of 1 indicates that logs can be sent. A value of 0 indicates logs can't be sent
- ***ReadyToSend***
  - Indicates if the destination is setup in a state where logs can be sent. For instance if Snare is already sending to the destination, ReadyToSend will be 0.

5 Snare Server

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

The Snare Server, as shown in Figure 8 collects events and logs from a variety of operating systems, applications and appliances including, but not limited to: Windows (NT through 2012), Solaris, AIX, Irix, Linux, Tru64, ACF2, RACF, CISCO Routers, CISCO PIX Firewall, CyberGuard Firewall, Checkpoint Firewall1, Gauntlet Firewall, Netgear Firewall, IPTables Firewall, Microsoft ISA Server, Microsoft IIS Server, Lotus Notes, Microsoft Proxy Server, Apache, Squid, Snort Network Intrusion Detection Sensors, IBM SOCKS Server, and Generic Syslog Data of any variety.

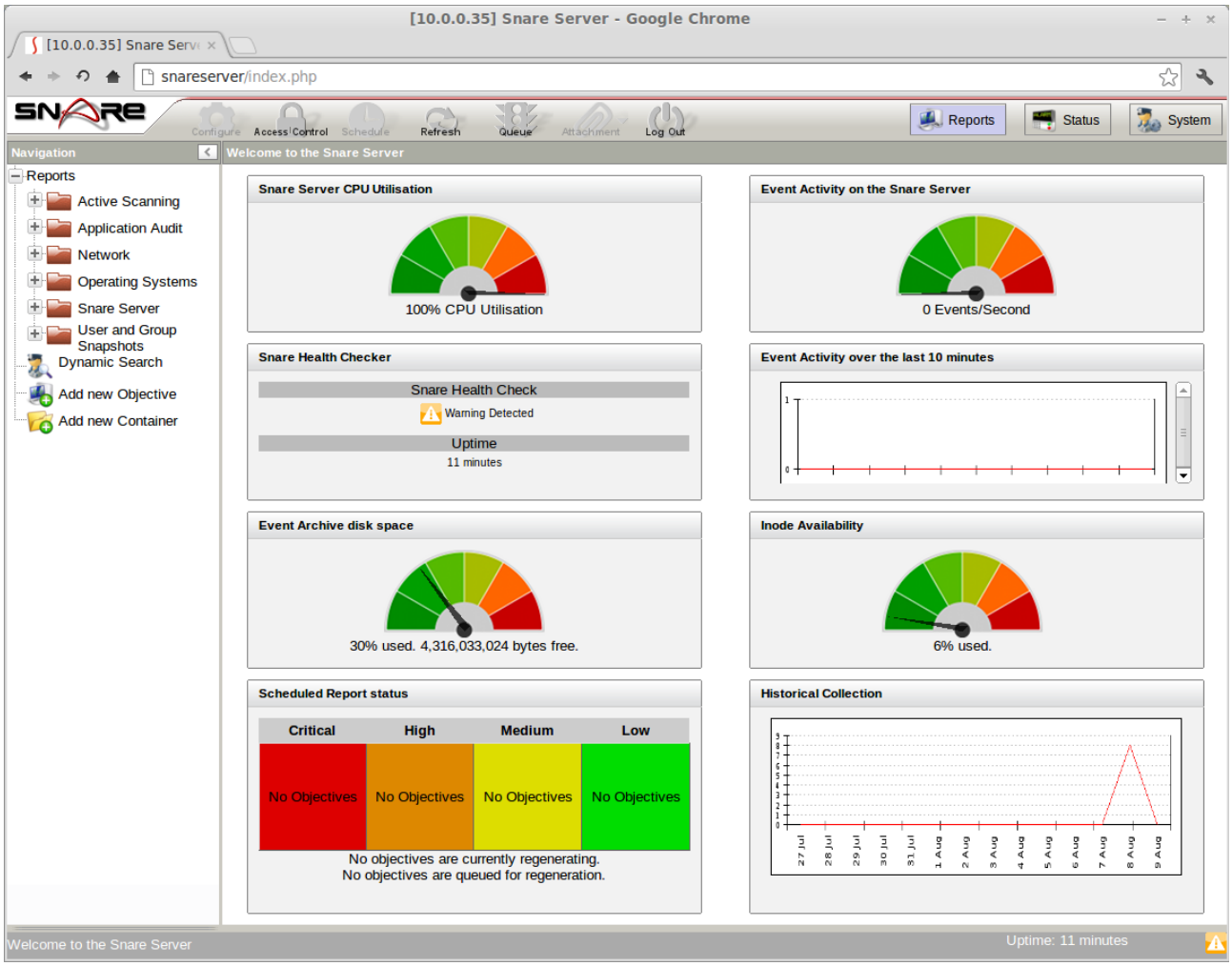


Figure 8 Welcome to the Snare Server

Some of the key features of the Snare Server include:

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

6 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 8211 6188 Adelaide Australia

Europe and the UK +44 (797) 090 5011

Email intersect@intersectalliance.com

Visit www.intersectalliance.com

Appendix A - Configuration File Description

Details of the audit configuration are discussed in the section on Audit Configuration. The purpose of this section is to discuss the makeup of the configuration file. The Snare configuration file is located at */etc/security/snare.conf*, and this location may not be changed. If the configuration file does not exist, the audit daemon will not actively audit events until a correctly formatted configuration file is present.

Snare can be configured in several different ways, namely:

a. Via the embedded web server (r*ecommended for novice users*), or
b. By manually editing the configuration file (r*ecommended for advanced users*).

The format of the **audit configuration file** is discussed below. Any line beginning with "#" will be treated as a comment line and ignored. Also, any number of tabs or spaces can be used. Major tokens such as [Config] must be surrounded by the square brackets.

[Config]	This section allows you to specify settings relating to the operation of the Snare agent.
name=override	The hostname of the client. If no hostname is set, the value of "hostname --fqdn" will be used
syslog_facility=facility	The SYSLOG facility used when sending to a SYSLOG server.
syslog_priority=priority	The SYSLOG priority used when sending to a SYSLOG server.
cache_size=(0 - 100000)	This value determines the size of the event cache,ie; the number of events, that Snare should keep if it cannot reach at least one of the hosts. The value must be between 0 and 100000. This feature only appears in Enterprise Agents only.
use_utc=1	Enable UTC (Universal Coordinated Time). This feature only appears in Enterprise Agents only.

[Remote]	This section allows you to specify settings relating to the Remote Control Interface used to control Snare.
allow=[1|0]	Turn the Remote Control Interface on or off.
listen_port=6161	Set a port that the Snare for OSX agent should listen on.
accesskey=md5password	Md5 checksum of the password used to protect the embedded web server
restrict_ip=1.2.3.4	IP address of a system that is used to remotely control the Snare for OSX agent. All requests from other systems will be dropped.

[Output]	By default, if no output section exists within the configuration file, the audit daemon will not send any data to anywhere. Otherwise, audit events will be sent to all valid destinations specified in the Output section. As such, events can be sent to one or all of a file, or to a remote network destination
file=/fully/qualified/file/name	The audit daemon will send data to the fully qualified filename specified within the [Output] section. The directory must exist. The file will be created if it doesn't exist.
network=hostname:port:protocol:format	Data will be sent to the remote host, and network port specified here. Audit data can be sent to a remote system using the `UDP` or `TCP` protocol. SSL may also be used to indicate an encrypted TCP connection. Format may be either `SNARE` or `SYSLOG`.

[Objectives]	This section describes the format of the objectives. Objectives are composed of: 1. Criticality - an integer between 0 and 4 that indicates the severity of the event. 0 is 'clear', 4 is "critical". Any integer less than 0 will cause the line to be rejected. 2. The event - this must either correspond to a valid syscall event, or a series of events separated by commas, and surrounded with round brackets (). Note that the embedded web server will convert the generic "groups" in the Audit Configuration window to the required events. For example, the abstracted group 'Administrative Events', will result in the event entry: 'event=(*reboot,settimeofday,clock_settime, setdomainname,sethostname*)' being written. 3. Return - either Success, Failure or * to indicate both Success and Failure 4. User - The users(s) to watch. This can be a single user, a list of users separated with commas or * to indicate all users 5. match - An optional string to match. This can be either a string literal, a regular expression or .* to indicate all events Note that whitespace will be trimmed from the start and end of items.
criticality=1 event=execve return=Success user=george match=/sbin	Report at criticality level 1, whenever the user 'george', attempts to execute a binary within /sbin, criticality=`0` for Clear (ordinary security level), `1` for Information, `2` for Warning, `3` for Priority, `4` for Critical.

Shown below is an example */etc/security/snare.conf* file. It is an example file only, and should NOT be used for operational purposes. It has been included to demonstrate the key concepts of formulating a snare.conf file, as discussed above.

Example snare.conf file

```
# This is a comment line with no leading spaces

# "set_audit" is wrong
[Config]
      name=
      cache_size=500
      syslog_facility=kernel
      syslog_priority=emergency
      use_utc=0

[Remote]
      allow = 1
      listen_port = 6161
      restrict_ip = 127.0.0.1
      accesskey = 536515b971214c61217ae42faf565ed2

# This is the output section
# TCP and multiple network entries only allowed by the Enterprise agent
[Output]
      network=10.0.1.14:6161:TCP:SNARE
      network=10.0.2.3:514:UDP:SYSLOG
      file=/var/log/filewatch.log

# This is the objectives section
[Objectives]
        criticality=4   event=exec,execve       return=Success  user=.* match=.*
        criticality=4
event=open_rc,open_rt,open_rtc,open_w,open_wc,open_wt,open_wtc,open_rw,open_rwc,open_rwt,
open_rwtc,creat,mkdir,mknod,xmknod,link,symlink,rmdir,unlink,rename,truncate,ftruncate
return=Success  user=.* match=.*
        criticality=4   event=connect,shutdown,setsockopt       return=Success  user=.*
match=.*
        criticality=4   event=rmdir,unlink      return=Success  user=.* match=.*
        criticality=4   event=open_r,readlink   return=Success  user=.* match=.*
        criticality=4
event=setgroups,setpgrp,setuid,setgid,seteuid,setegid,setauid,setreuid,setregid,setuid,os
etpgrp return=Success  user=.* match=.*
        criticality=4   event=chmod,fchmod,chown,fchown,mctl,fcntl,lchown,aclset,faclset
return=Success  user=.* match=.*
        criticality=4
event=login,logout,telnet,rlogin,su,rexecd,passwd,rexd,ftpd,admin_authenticate,ssh
return=Success  user=.* match=.*
```