SNARE
System iNtrusion Analysis & Reporting Environment

SNARE Agent for Windows v 4.0.2.2 - Release Notes

Copyright (c) 2012 InterSect Alliance International Pty Ltd.

Snare is a program that facilitates the central collection and processing of Windows NT/2000/XP/2003 Event Log information. All three primary event logs (Application, System and Security) are monitored, and the secondary logs (DNS, Active Directory, and File Replication) are monitored if available. Event information is converted to tab delimited text format, then delivered over UDP to a remote server.

Snare is currently configured to deliver audit information to a SYSLOG server running on a remote (or local) machine. A configuration utility allows you to set the appropriate syslog target and priority, as well as the target DNS or IP address of the server that should receive the event information. It should be noted that many syslog servers are not designed to cope with the sorts of volume of data that multiple snare agents can potentially generate.

The Snare service will automatically start after you have completed the initial configuration process. It is recommended that you configure each of your event logs to 'overwrite as required', as opposed to 'overwrite > 7 days', which is the default on Windows 2000 machines.

We also recommend that you configure appropriate access controls on the Snare registry entries using regedt32.exe - perhaps restricting the permission to read or modify the keys and values to Local or Domain Administrators only. Snare stores it's registry settings in:
HKEY_LOCAL_MACHINE\SOFTWARE\InterSect Alliance\AuditService

Please remember that event monitoring is a complex area in most modern operating systems, and is not often very granular. Turning on significant event monitoring for a system can often produce unpredictable results, and could seriously detract from the resources available to the rest of your system or network. We recommend that you have a good understanding of exactly what event information is going to be used for, prior to enabling event monitoring on your servers.

Versions of Snare for Windows after 2.4.3 can be installed without removing a previous version. Versions of Snare for Windows after 2.6.0 do NOT support the GUI, Snare.exe should therefore be removed.

Version History For Windows Agent:

Version	Description
BackLog 1.0	• initial public release.
BackLog 1.01	• Included a registry write when the system advises the software that system shutdown is pending. Thanks to Adrian Mink of FIData for the suggestion.
BackLog 1.1	• Installation process modified so that service startup is automatic on installation, and service will be automatically stopped prior to removal.
BackLog 1.2	• Fixed a loop that did not respond quickly to service exit requests. • Created a StartLog executable that sets the initial log tally prior to first service execution. Thanks to John Yu of Boston University for the suggestion.
BackLog 1.3	• Fixed a nasty problem relating to sending data to local* Syslog identifiers 12-15 were reserved for other purposes.
BackLog 1.4	• Version 1.3 did not correctly fix the local* problem.
BackLog 1.5	• Update to cater for events that do not provide a correct event id template (eg: sshd for windows)
BackLog 1.6	• Memory leak removed.
BackLog 1.6a	• Removed Debug log file that was accidently included in 1.6.
BackLog 1.6b	• Snare can use a significant amount of CPU time in some rare circumstances. This is a test build to look for a potential fix.
BackLog 1.7	• Log file 'catchup' has been removed due to poor boot performance. Snare only forwards logs when it is active. 'Startlog.exe' therefore removed from the distribution. • Test build 1.6b proved to be a success. Changes integrated into 1.7
BackLog 1.7b	• Included customisable delimiter as a registry entry.
BackLog 1.7c	• Fixed events with embedded newline characters in the DATA section.

For more information, contact your SNARE Server Sales Representative

symtrex inc.
Network Security Specialists
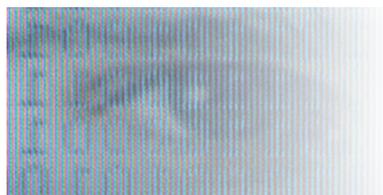
Who's Watching Your Network?

BackLog 1.7d	• Fixed events with embedded newline characters throughout the event - thanks to Patrick Monate.
BackLog 1.8	• Snare now adheres to the SysLog RFC by prefixing the event with hostname and date/time. Thanks to Patric Fors.
BackLog 1.8a	• Added a Delimiter between the new syslog RFC fields and the normal Snare data - thanks to Patrick Monate.
BackLog 1.8b	• A buggy registry entry made the delimiter character '\t' rather than a true TAB character.
	• Slightly changed the formatting of the 'strings' section of the event to remove ancilliary spaces after newlines.
BackLog 1.9	• Fixed a problem introduced by Windows 2000 Service Pack 2 that caused Snare not to display the "strings" section of event logs.
	• Changed reporting of EventID's so they match Event Viewer in all circumstances, by only displaying the last 16 bits of the event ID number. Thanks to Travis Silva.
	• Added configurable Delimiter character.
	• Also introduced some back-end code to provide further event filtering. Note that this feature is not yet enabled.
BackLog 1.9a	• Included the following Windows 2000 logs:
	* Directory Service
	* DNS Server
	* File Replication Service
BackLog 1.9b	• A slight incompatibility with a Windows HOTFIX, and the "User Type" field caused 1.9/1.9a not to forward log data appropriately.
Snare 2.0 alpha	• New version, which now includes
	* Front end filtering by userID, search term, and event ID
	* Event display on the configuration GUI
	* Auto-set of audit configuration and file SACLs (if configured).
	* Micro-web server for remote control (userid / password and
	IP address restriction.
	* User / Group listing for configuration checking
Snare 2.0	• Fixed memory leak in user/group listing
	• Fixed endless loop in service restart.
Snare 2.1	• Fixed potential memory leak in FILE-OPEN events.
	• Fixed service termination in response to strange Win2k/XP 'file already exists' error when reading from the event log.
	• Changed service restart code to work with non-english installs.
	• Modified default objectives so that ALL events are only enabled when SNARE is NOT in control of the eventlog configuration.
Snare 2.1a	• Caught a small memory leak in 'File Handle Closed' events.
Snare 2.1b	• Internal debug release
Snare 2.1c	• Included some additional debugging information for service startup.
Snare 2.1d	• Now includes User SID information in micro-web server user information strings.
	• Modified eventid examination code to work with buggy applications that do not fill out the full 'dword'.
Snare 2.1e	• Introduced a 'try/catch' block around the MS FormatMessage system call due to problems with some non-standard eventlog messages.
Snare 2.1f	• Backed out the 'eventid' modifications made in 2.1d due to problems caused to some application logs.
Snare 2.1g	• Added Snare internal eventlog counter per source log.
Snare 2.2	* Configured snare to set 'overwrite as needed' for each of the eventlogs.
	- Web Server can now request that objectives be reread without needing the service to be restarted.
	- Fixed modify/add objective in micro-web server.
	- Added a gethostbyname check for the destination server in the GUI.
	- Now using strftime rather than asctime. (Thanks Kris!)
	- Debug messages now flushed faster.
	- Speedup for objective checks by migrating strncpy's out of a loop.
	- Timeout added to check for new events, just in case notify changeeventlog does not pick up new events correctly.
	- Reapply from web server now reconfigures all other config settings.
	- Fixed application event strings for some events.
	- Removed 'first run' question for non-priv users.
Snare 2.3	• Various bugfixes and enhancements
	• Takes advantage of Win2k+ capability of recursive (and continually applied!) audit configuration for directories.
	• Now loops through the 'audit DLL' files defined by an application for string data if there is more than one DLL configured.
Snare 2.3a	• Uses DLL Delay Loading to make the snare exe happy on both windows NT and 2000+
Snare 2.3b	• Correction to the audit DLL looping code to work with later win2k service packs (Thanks to Rich Adamson).
Snare 2.3c	• Hostname resolution finally working correctly for destination server
	• Flags in 'domain user' information under remote control micro-web server now being reported correctly. MS Doco for user enumeration was unfortunately unclear.
	• Version information for binaries now set in visual C, which means that Snare can probably be 'upgraded' rather than

Who's Watching Your Network?

	removed/reinstalled.
Snare 2.3.4	* New version scheme to fit in with MS metadata requirements. • Fix for objective addition/modifications via micro-web server for Return codes • More information displayed in the objective summary page in the micro-web server. • Removed outdated htmlhelp, linked documentation to InterSect resources web page. • Updated win2k+ systems to use the new security ACL application API rather than the old deprecated system call (still used on NT). This means that win2k+ systems will apply file security to directories much faster.
Snare 2.3.5	• User inclusion and exclusion now supports multiple users, comma separated. • Querying the registry for event string data will no longer trigger Windows 2003 registry audit settings related to the security log.
Snare 2.4.0	• MD5 passwords are now used in the registry, rather than plaintext * Split Objective checking process into two routines for speed. • Try/Catch loop around User SID Conversion routine due to MS bug in Win2003 (Thanks to Kelly Gilmore for the very valuable assistance!) • New Dynamic syslog destination capability - Syslog priority can be based on Snare event criticality. • Ability to write log data out to a file in the directory <systemroot>/system32/Logfiles/Snare, with a filename of YYYYMMDD. log • "First match" rather than "most critical match" checking as an option. This should reduce CPU usage on systems where the administrator is not concerned about match criticality. • Snare Event counter replaces the windows event counter.
Snare 2.4.1	• Removed the PASSWD_NOTREQD flag, as it is no longer significant in win2k+ • Changed a flag check that caused Domain Group Enumeration to terminate prematurely, and therefore not display all users.
Snare 2.4.2	• Added event checksum capability (md5 based). • Address restriction for micro-web server can now be a DNS name if required.
Snare 2.4.3	• Bug in address lookup for DNS name change in 2.4.2 fixed.
Snare 2.4.4	• Bug in web server associated with quadruple backslashes. • Changed group member retrieval code to work with AD in native mode. • Added registry dump capability. • Modified GUI to display a maximum 1000 nodes in the list.
Snare 2.4.5	• Fixed version number in about box. • Additional debug information available surrounding flakey MS API calls. • System log eventID's mangled to cope with MS's wierd numbering system. (eventid & 65535). • Basic 'last known log position' restoration re-implemented (see snare 1.7),with a basic flood-protection capability included (ie: Only restores position where the last position is within 5000 log entries of the current log position.
Snare 2.5	• Workaround for a MS LookupAccountSid/malloc related issue. • TCP delivery capability & Event caching enabled in the event of TCP connectivity problems. (Note: TCP only included where someone has explicitly identified a requirement for it - not recommended for normal usage). • Attempted fix for issue where systems with zero objectives, were still causing some events to be sent.
Snare 2.5.1	• Fix for memory issue in Domain Group Members listing via embedded web server.
Snare 2.5.2	• Fix for some application / system logs that have not initialised the first few bits in their eventID structure to zero, and therefore have huge eventIDs. • Fix for events that do not have any strings to expand - just report the raw string data. • Fix for the 'duplicate log' problem on some servers (particularly win2003). • Default 'process tracking' objectives has been configured to only watch for cmd.exe, in order to cut down the data volume on default install.
Snare 2.5.3	• Recompile of Snare 2.5.2 using an updated compiler set, which fixes a crash issue associated with local and domain group downloads.

Snare 2.6.0	• GUI support removed and features migrated into the mirco web server.
	    - Fixes for memory leaks around socket handling.
	    - Minor changes in some variable handling.

Snare 2.6.1	• Added multi-host support for micro web server "Restrict IP".
	    - Additional duplicate prevention code.
	    - Password age, max password age and account expiry included in user output (LocalUsers and DomainUsers).
	    - Granular logging added.

Snare 2.6.2	• Initial USB detection routines now included for Windows 2000 and above
	    - Fixed local7 syslog issue
	    - Fixed bug in capturing first event after event log cleared (e.g 517 - security event log cleared)
	    - Fixed memory handling error in Objective code
	    - Fixed multiple bugs in user and group retrieval code

Snare 2.6.3	•Fixed unresolved symbols in object access logs
	• Further development of USB audit events
	• Added "last_logon" to local and domain user logs
Snare 2.6.4	• Updated exception handling to prevent application failures
Snare 2.6.5	•Migrated to MS secure functions
	• Corrected USB auditing to be optional (users must have an USB objective to enable USB auditing)
	• Added extra error checking on USB events
	• Enabled threaded web server, web pages should still operate even when the agent is under load
Snare 2.6.6	• Resolved intermittent crashing on large events (event size >8k). Most likely to affect cluster nodes and application servers.
	• Fix for web interface failures. Additional debugging also added.
	• Resolved duplicate messages on reboot, shutdown message now handled correctly on Windows XP and 2003.
	• Remove "Enable remote control" option from web interface. There are now start menu options to enable and disable remote access.
	• Fix binary problem with previous X64 build.
	• Added support for silent installs
Snare 2.6.7	• Repaired NT4 support.
	• Added ability to exclude event IDs.
	• Fixed handle leaks.
	• Fixed DomainGroupMembers function in mixed AD.
	• Added further Web server repairs to prevent failures.
Snare 3.0.0	• Fixed audit policy configuration logic
	• Changed "Latest Events" refresh timeout to 30 sec
	• Improved corrupt event log detection and notification
	• Fixed bug in user and group retrieval routines
	• Removed USB device tracking support (3.0 release only)
Snare 3.1.0	• Re-introduced USB auditing with modifications.
	• Further code simplification.
	• Added service description and changed default service recovery options (this update only applied when using the installer).
	• Fixed auditing inheritance for auditing sub-folders.
	• Added feature to strip CR and LF characters from user and group output.
	•Fixed objective matching bug when an event matches all available objectives.
	• Extended supported features (see website for details).
Snare 3.1.1	• Minor remote control interface update.
Snare 3.1.2	• Fixed issue causing excessive page faults.
Snare 3.1.3	• Fixed potential buffer truncation.
	• Improved backend objective handling, significantly reducing CPU usage.
Snare 3.1.4	• Further speed improvements
	• Added capability to re-order objectives
	• Fixed problem matching event IDs under certain conditions
	• Sped up DomainGroupMemebers
Snare 3.1.5	• Added target arch/actual arch reporting to the Status window
	• Updated objective order processing, now top to bottom. This means any exclusion objectives should be moved to the top of the list
	• Config/LeaveRetention(DWORD) added to prevent agent from setting "overwrite as needed"
	• Fixed minor string error in remote control interface
	• Fixed category lookup problem
	• Fixed slowdown when sending to multiple hosts using DNS names and one or more DNS names does not exist
	• Fixed error in LocalUsers causing blank username, full name and SID
	• Included extra user account flags in local/domain users
Snare 3.1.6	• Added event IDs 551 and 552 to the logon/logoff category
	• Stripped special HTML characters from records shown in Latest Events
	• Fixed problem resolving variables in some event records
	• Fixed problem resolving event records when multiple files are listed in "EventMessageFile" registry entry
	• Corrected "empty" comments in Domain/Local Users
	• All user/group reports now use pre-Windows 2000 names (eg group names in DomainGroupMembers).
	• Fixed DomainUsers report where non-DCs would use local account SIDs in DomainUsers report
	• Modified the objective rules to allow "Access a file or directory" to configure any path if "handle file audit settings" is disabled
Snare 3.1.7	• Updated the REG_BINARY output module in "Registry Dump" to correctly output binary data
	• Fixed socket problem when using multiple hosts (supported version)
	• Updated web interface to re-enable event ID filter for non-Security events
Snare 3.1.8	• Security update to prevent Cross Site Request Forgery
	• Default configuration updated
Snare 3.1.9	• Fixed bug in DomainUsers function
	• Added feature to objective registry syntax to allow the use of keywords, therefore, future updates to High Level events will automatically be applied.
Snare 3.1.9.1	• Bug fix in RegDump function

Who's Watching Your Network?

Snare is a program that facilitates the central collection and processing of Windows Vista Event Log information. All three primary event logs (Application, System and Security) are monitored. Event information is converted to tab delimited text format, then delivered over UDP or TCP to a remote server.

Snare is currently configured to deliver audit information to a SYSLOG server running on a remote (or local) machine. A configuration utility allows you to set
the appropriate syslog target and priority, as well as the target DNS or IP address of the server that should receive the event information. It should be noted that many syslog servers are not designed to cope with the sorts of volume of data that multiple snare agents can potentially generate.

The Snare service will automatically start after you have completed the initial configuration process. It is recommended that you configure each of your event logs to 'overwrite as required' (this is the default in Vista)

We also recommend that you configure appropriate access controls on the Snare registry entries using regedt32.exe - perhaps restricting the permission to read or modify the keys and values to Local or Domain Administrators only. Snare stores it's registry settings in:
HKEY_LOCAL_MACHINE\SOFTWARE\InterSect Alliance\AuditService

Please remember that event monitoring is a complex area in most modern operating systems, and is not often very granular. Turning on significant event monitoring for a system can often produce unpredictable results, and could seriously detract from the resources available to the rest of your system or network.
We recommend that you have a good understanding of exactly what event information is going to be used for, prior to enabling event monitoring on your servers.

Version History For VISTA Agent

Snare Vista 0.1	• Initial customer release (beta).
Snare Vista 0.2	• Added feature to exclude events
	• Modified event IDs for Vista compatibility
Snare Vista 0.3	• Added Workaround for "file not found" bug
	• Added Silent install option (/silent and /verysilent)
Snare Vista 1.0	• Improved audit control (especially Object Access events and Packet Filtering) resulting in lower resource usage
	• Improved memory and handle usage
Snare Vista 1.0.1	• Changed default objectives to reduce resource usage
Snare Vista 1.0.2	• Added code to clear existing audit settings on install
Snare Vista 1.1.0	•Added new features to manage default audit settings on c:\Windows. Use "snarecore.exe -s" to strip the default settings and "snarecore.exe -r" to restore them.
Snare Vista 1.1.1	• Fixed auditing inheritance for auditing sub-folders.
	• Added feature to strip CR and LF characters from user and group output.
	• Fixed objective matching bug when an event matches all available objectives.
	• Extended supported features (See Website for Enterprise SNARE Agent features).
	• Fixed potential buffer truncation.
	• Improved backend objective handling, significantly reducing CPU usage.
Snare Vista 1.1.2	• Further speed improvements
	•Added support for DNS Server, Directory Service and DFS replication event logs
	• Added support for custom event logs (supported feature)
	• Fixed startup error when STATUS registry settings value were invalid (e.g. imported settings from a Windows 2003 agent). Invalid values are now ignored and monitoring will continue from the end of the event log
	• Added capability to reorder objectives
	• Fixed problem matching event IDs under certain conditions
	• Updated objective order processing, now top to bottom. This means any exclusion objectives should be moved to the top of the list
	• Config/LeaveRetention(DWORD) added to prevent agent from setting "overwrite as needed"
	• Fixed minor string error in remote control interface
	• Included extra user account flags in local/domain users
	• Stripped special HTML characters from records shown in Latest Events
	• Corrected "empty" comments in Domain/Local Users
	• All user/group reports now use pre-Windows 2000 names (eg group names in DomainGroupMembers).
	• Fixed DomainUsers report where non-DCs would use local account SIDs in DomainUsers report
	• Modified the objective rules to allow "Access a file or directory" to configure any path if "handle file audit settings" is disabled
	• Strip spaces from destination address in Network Configuration

symtrexinc.
Network Security Specialists

Who's Watching Your Network?

Snare Vista 1.1.3 (internal)	• Added option to exclude General Match in Objective Configuration • Updated event handling to prevent memory overloading • Improved username recognition (meaning the username field should be populated more often)
Snare Vista 1.1.4	• Updated Keyword handling to correctly identify and tag Audit Success/Failure events • Update Level handling to improve multilingual support
Snare Vista 1.1.5	• Security update to prevent Cross Site Request Forgery • Default configuration updated
Snare Vista 1.1.6	• Update custom event log capturing to include Microsoft\Windows channel support (supported feature)
Snare Vista 1.1.7	• Update custom event log capturing to exclude Forwarded Events until an appropriate handler can be written and tested • Added feature to objective registry syntax to allow the use of keywords, therefore, future updates to High Level events will automatically be applied. • Added support for capturing Critical, Verbose and ActivityTracing event levels • Fixed a bug in the DomainUsers function • Fixed excessive memory usage when the agent could not resolve the Destination DNS name • Improved event handling • Further speed improvements
Snare Vista 1.1.7.1	• Bug fix for RegDump function
Snare Vista 1.1.7.2	• Added memory limitations on event buffering
Snare Vista 1.1.7.3	• Fixed interpretation of "Classic" event type
Snare Vista 1.1.7.4	• Event handling redesign • Minor changes to Latest Events • Increased Change Token timeout period
Snare 4.0.0	• Merged Windows agents in a new installer with in built silent install support • Added configuration export feature for silent install support (snarecore.exe -x) • Minor updates to the micro web interface service • [Vista/08/Win7] Rebuilt log collection and monitoring system • [Vista/08/Win7] Fixed bug in DomainGroupMembers which caused the agent to crash on x64 systems • [Vista/08/Win7] Added support for collecting both FRS and DFS-Replication logs
Snare 4.0.0.1	• Updated installer to remove CRT dependency
Snare 4.0.0.2	• [Vista/08/Win7] Fixed problem with DNS name override setting
Snare 4.0.1.0	• Updated micro web server authentication (digest). WARNING: this will require you to reset the password. • Removed MD5 string from /remote web page • Added cookie support for Change Tokens • Added POST support to micro web server • Added pre-submit MD5 hashing of remote access password in /remote web page • Added quotes to string values when generating a template file (snarecore.exe -x) • Improved Windows 2000 support for new installer
Snare 4.0.1.1	• Fixed objective re-order buttons • Added Remote/EnableCookies option to control the use of cookies
Snare 4.0.1.2	• Fixed bug in silent deployment of remote access password
Snare 4.0.2.0	• Modified DomainGroupMembers to supply either samAccountName or CommonName • Added heartbeat capability, see new HeartBeat and Agent Log option • Added Policy Change and Service tracking abilities, see new HeartBeat and Agent Log option
Snare 4.0.2.1	• Added SourceName filtering • Minor Objectives Configuration interface redesign • [NT/2000/XP/2003] Added General Search Term Match Type • [Vista/08/Win7] Added Alternative Syslog Header option • [Vista/08/Win7] Added USB Auditing
Snare 4.0.2.2	• Enabled TCP_NODELAY to prevent TCP buffering by the OS • Fixed Unquoted Service Path vulnerability for installs and upgrades • Switched to fixed locale for date information • Upgraded DomainUsers to search all DCs for most recent LastLogon (LastLogon and LastLogonTimestamp)

These updates have some very important implications:

- TCP_NODELAY should fix the fragmented packets and "ghost" hostnames seen at Snare sites using TCP.
- The Unquoted Service Path vulnerability was recently brought to our attention and is fixed in this release for all fresh installs and upgrades
- The fixed locate should allow operating systems with a default language other than English to send correctly formatted audit records
- The DomainUsers update now means that you no longer need to get the Snare Server to contact all DCs to resolve the LastLogon time, the agent will handle this for you *and* it will include the LastLogonTimestamp as well when evaluating the most recent time.
- For more details on the difference between these two settings, see http://aducadmin.com/ad-attributes-last-logon-timestamp/

symtrexinc.

Network Security Specialists

Who's Watching Your Network?