



System Intrusion Analysis & Reporting Environment

SNARE Server Version 4.7.1/5.1.1 - Release Notes

The Snare Server 4.7.1/5.1.1 combination builds on the foundation of the 4.7/5.1 release (see release notes below), providing further bug fixes and performance increases. Due to the nature of the updates, these patches can only be applied to existing 4.7/5.1 installations. Customers on other versions of the Snare Server will need to upgrade to 4.7/5.1 before installing the latest corresponding update.

Changes between version 4.7/5.1 and 4.7.1/5.1.1 include:

- Updates to modules, batch processes and objectives. Minor updates to a broad range of features to improve performance or address reported issues.
- Event collection. A number of updates have been made to the event collection facility, including:
 - Improved handling of very large events (up to 64kB)
 - Corrected IP address detection of reflected events
 - Fixed date padding problem
 - Fixed file handle management problem
- [Version 5.1.1] PHP updates. Replaced deprecated PHP functions and added support for updated PHP functionality
- SYSLOG Configuration. Added SYSLOG configuration options to the Configuration Wizard.
- Database management. Updated configuration database management
- IPDB update. Updated regular expression support to fix anchor filtering problem.
- Windows user and group retrieval. Updated host and database management for better speed and error detection/correction. The objective has also been updated to including Active Directory information retrieval options .
- Data Backup and Import objectives. Revamped Data Backup and Import objectives , now including support for USB devices.
- Real Time reporting. Updated real time objective handling.

SNARE Server Version 4.7/5.1 - Release Notes

The SNARE Server 4.7/ 5.1 provides additional enhancements, and again are available as either updates for existing clients or for net new installations.

The most significant improvements are the ability to manage the Enterprise SNARE Agents, and a significantly improved Data Archive capability.

The following points detail the key or major features over the previous Snare Server version:

*For more information, contact your SNARE Server Sales Representative
snaresales@symtrex.com | 1-866-431-8972*

Who's Watching Your Network?

SNARE Server Version 4.7/5.1 - News Update

- **DHCP Server Log Functionality.** Windows DHCP Server logs can now be received and processed by the Snare Server. MAC address to vendor conversion is available, sourced from the IEEE standards body registry.
- **Sophos Data Control Logs.** Logs from Sophos Data Control have been allocated to their own logtype.
- **Bulk upload of IIS Web Logs.** Snare has always been able to process IIS web logs, presented in the default format. Customized log formats that meet minim field requirements, are now also supported.
- **Active Directory.** In addition to the normal user and group retrieval via the Snare Agents for Windows, the “Retrieve User and Group information from Windows Servers” objective can now attempt to directly consult an organizational Active Directory server for details
- **Agent Configuration.** The “Check Agent Configuration” and “Select Individual Client Systems” objectives have been replaced by a new “Agent Management” objective. The new objective provides the ability to ‘group’ agents into folders, and set master configurations for both log-types, and individual agent groupings. The objective will be able to manage the configuration of agents bought out by InterSect Alliance in the future, without significant updates. At present, Windows, Solaris and Epilog are supported management targets
- **Windows - Locked Accounts.** A new objective, that details windows accounts that have been locked, has been added to the Configuration Checking section of Snare
- **Network Security Scanner.** A new configuration interface has been added for the Network Security Scanner objective, derived from our Snare Server version 6.0 code-base
- **Data Archive.** The data archive objective has been updated significantly. USB Drives and USB Keys are now valid destinations for data archival. For users who wish to use corporate or local SAN drives as a backup destination, sending files to the SAN is now also a viable option, with some assistance from your Snare Server support team. For both USB and SAN destinations, Snare will use a file synchronization algorithm, to only copy files across, that do not already exist on the target device.
- **Data Import.** In addition to supporting the USB/SAN options available in the Data Archive objective, the new Data Import objective has an updated user interface, which will make the process of selecting particular types and dates of data, much simpler
- **Monitor Live Data.** By using a network sniffer to monitor incoming data, the new Monitor Live Data objective does not inject itself into the path of Snare’s normal collection system. As such, it provides useful real-time statistical information, without risking UDP collection performance drops
- **Total Events Overview.** Drilling down through the information provided by the “Total events plotted per 15 minutes” objective, within the “Status and Statistics” category, has become much faster, and more intuitive, with a revamp of the user interface.
- **Agent Heartbeat.** The Snare Server can now listen for agent heartbeat data. Information is incorporated into a new ‘AgentHeartBeat’ logtype, and can be queried using standard event selection tools.
- **Virus Scanner.** A rogue software checker runs on the Snare Server. A new interface has been added to the Snare Server, providing the ability to update virus signatures, and display problem notifications

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477 fax
snaresales@symtrex.com
www.symtrex.com
www.snare-server.com



Who's Watching Your Network?