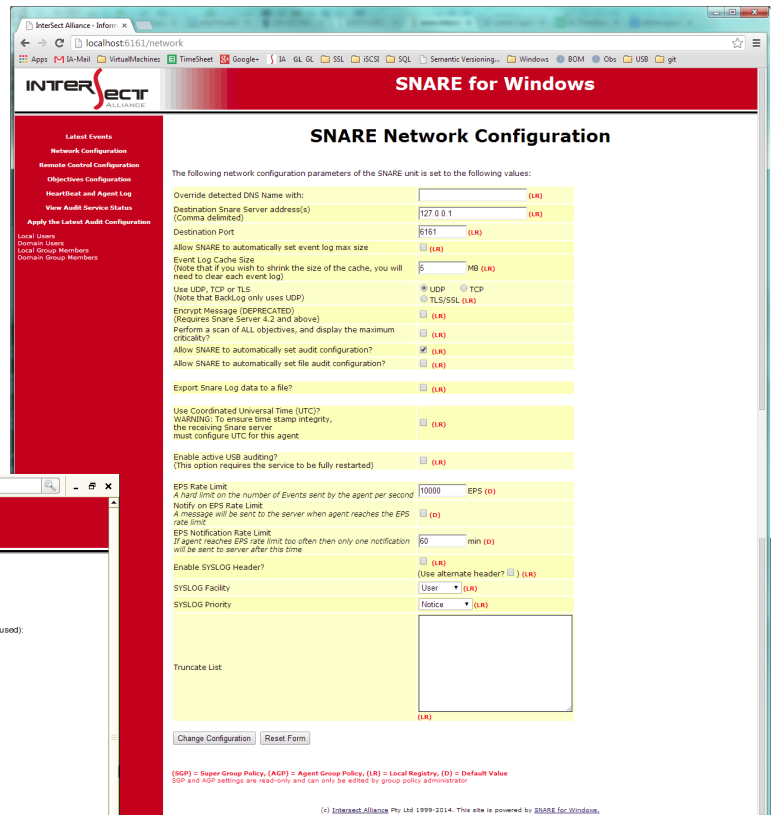


Snare Enterprise Agents

Centralized log management and analysis is essential to review activity on your network, not to mention a requirement for most compliance regulations. The question sometimes is how to capture the critical events in a timely fashion as well as guarantee that they will reach their destination, in particular for Windows. The Snare Enterprise Agents, developed by Intersect Alliance, provide an essential tool to accomplish this task.

The agents which are installed on the individual devices are light weight programs, that provide the ability to capture event logs, sending them in real time to either a Snare Server or the Security Event Information Management tool of your choice.

Using an intuitive web interface, you can either select specific information or all relevant data.



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



Who's Watching your Network?

Snare Enterprise Agent Features/Benefits

The features of the Enterprise Agents are quite extensive and include the following:

Encryption

Using the NIST recommended Triple DES algorithm, Snare Enterprise Agents are able to protect the confidentiality of the log messages in transit to the Snare Server. Once the messages are received by the Server, they are decrypted and processed as normal messages. By utilizing the Centralized Configuration Management, agent message encryption can be quickly rolled out across the network.

Event Log Caching

Event Log Caching enhances the integrity of the overall log management system by storing undelivered messages in memory on the originating host in the event of a transmission failure.

Common sources of these failures include:

- Network stack malfunction on the host machine
- Network device failure or misconfiguration
- Destination server being offline
- Network outages

Once the Enterprise Agent is notified of any problems delivering messages to the destination server, the event log cache is used to preserve subsequent messages as long as the destination server is unavailable. The size of this cache is configurable (for Windows cache size, refer to [Microsoft Knowledge Base—KB Article ID 957662](#)), and if the agent needs to be stopped or restarted, any remaining events will be written to disk. Once a new connection can be established with the server, the cached events are gradually forwarded to their destination.

Guaranteed Log Message Delivery

System administrators and security professionals are under ever increasing pressure to ensure the completeness and integrity of the logs. Leveraging the features of TCP, Snare Enterprise Agents are notified of any problems encountered during transmission and take appropriate actions to preserve event log continuity and completeness.

Log Message Simulcasting

Each Enterprise Agent is able to simultaneously direct event logs to multiple destination servers for redundancy or disaster recovery planning. Deployed along with a hot standby Snare Server, or other SIEM tool, provides for an extremely cost-effective, high availability log management system, as well as facilitating a best of breed approach to log and Security Event Management.

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada, M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477



Who's Watching your Network?

Advanced Remote Control

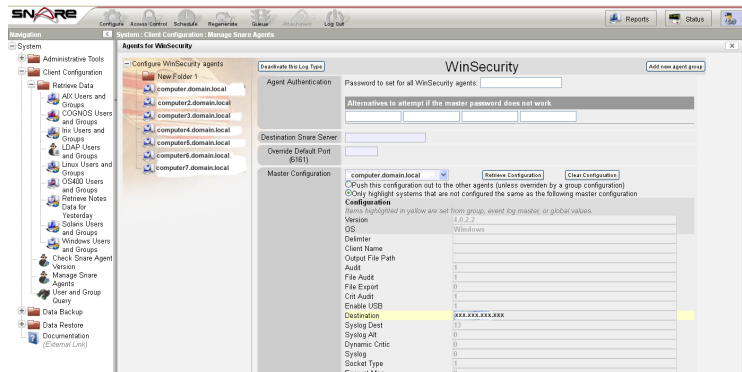
The advanced remote control feature allows each agent to be remotely configured from a set of "administrator" IP addresses or the IP address associated with a backup Snare Server.

Dynamic DNS Support

If DNS names are used in the configuration of either the Advanced Remote Control or Log Message Simulcast features, generally the host name is resolved only once as the agent starts up. With dynamic DNS support, the agent will automatically refresh the associated IP address every 10 minutes. This setting is crucial for installing new Snare Servers or dynamically changing the destination server in the event of a network or site failure (disaster recovery) without having to reconfigure or restart a single agent.

Centralized Configuration Management

In large networks with hundreds or thousands of log sources, maintaining a standard Snare Agent configuration has presented a challenge. Now leveraging technology in the Snare Enterprise Agents, the Snare Server Console is able to query all deployed agents for their current configuration settings. The Snare Server will then automatically compare deployed agents with the "master" agent template and remotely apply, and activate, an updated configuration if necessary.



Custom Windows Event Logs

Snare Enterprise Agents for Windows and Epilog extend beyond the core Windows Event logs. The Enterprise Agents enable the collection, filtering and transmission of non-standard and third party Windows Event Logs.

Monitoring Registry Events

The ability to monitor specific sections of the registry to look for software that is being added without approval or to capture the insertion of malware into a system.

For a complete list of all features please see the table attached.

If you have any questions about the Enterprise Snare Agents or the Snare Server, contact us at 866-431-8972 or sales@symtrex.com.

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



Who's Watching your Network?



System Intrusion Analysis & Reporting Environment

Features	Open Source	Enterprise
Gather operating system specific events	✓	✓
Easy to use Installer	✓	✓
Silent Install Option	✓	✓
Upgrade option to preserve existing configuration settings	✓	✓
Provide access to local and network users and groups	✓	✓
Remote Control Interface	✓	✓
UDP and Syslog transmission options	✓	✓
Objective-event based filtering	✓	✓
Debug Mode	✓	✓
Encryption (to Snare Server) as well as TLS/SSL		✓
Event Log Caching		✓
Guaranteed log message delivery (TCP)		✓
Log message simulcasting		✓
Advanced remote control		✓
Dynamic DNS Support		✓
Centralized configuration management		✓
Custom Window Events Logs		✓
Support and upgrades		✓
Monitoring Registry Events		✓
Monitoring USB Devices		✓
UTC Time Zone Normalization		✓
Agent Heartbeat		✓
Single MSI for multiple platforms		✓
Monitor Policy Status		✓
Serve Tracking		✓
Group Policy Support		✓
Monitor Agent Configuration Changes		✓
Regular expression for General Search March		✓
Truncation of Verbose Event Text		✓
Log Server Connection Status		✓

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



Who's Watching your Network?