



System Intrusion Analysis & Reporting Environment

SNARE Epilog for Windows Agent - Release Notes

Epilog is a program that facilitates the central collection and processing of Windows text-based log files. Log information is converted to tab delimited text format, then delivered over UDP/TCP to a remote server.

Epilog 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 Epilog service will automatically start after you have completed the initial configuration process. We recommend that you configure appropriate access controls on the Epilog registry entries using regedt32.exe - perhaps restricting the permission to read or modify the keys and values to Local or Domain Administrators only. Epilog stores its registry settings in:

HKEY_LOCAL_MACHINE\SOFTWARE\InterSect Alliance\Epilog

- | | |
|------------|---|
| Epilog 1.0 | Initial working release |
| 1.1 | <ul style="list-style-type: none">• Fixed problem with SMTPSvc logging format• Added support for filename format strings to allow an administrator to identify which file names should be monitored within a given directory. |
| 1.2 | <ul style="list-style-type: none">• Removed need for backslash on directory names |
| 1.3 | <ul style="list-style-type: none">• Repair for reading blank lines (Exchange logs, SMTPSvcLogs)• Patch for Log Name Format to prevent the agent from crashing.• Added better wild card support, now supporting alphabetical precedence (e.g. file01.log, file02.log, etc).• Fixed file locking problem.• Updated Log format names, added "custom" option to allow user defined labels.• Decreased max event length to 4K and improved handling of large events to prevent possible stack problems.• Migrated code to MS secure functions.• Added support for silent installs (/verysilent) |
| 1.3.1 | <ul style="list-style-type: none">• Updated fopen_s function to use _fsopen to allow resource sharing between Epilog and the program creating the log file |
| 1.3.2 | <ul style="list-style-type: none">• Extra measures to prevent excessive CPU usage |
| 1.3.3 | <ul style="list-style-type: none">• Bug fix for log entries starting with 10 or more spaces (Internal release only)• Improved file change detection• Repaired problem in outgoing message format• Modified space and newline handling functions |
| 1.4.0 | <ul style="list-style-type: none">• Added threaded remote control interface• Added granular debug levels• Fixed memory leak when using syslog• Added alternative SYSLOG header• Increased web output size (allowing for more log configurations) |
| 1.5.0 | <ul style="list-style-type: none">• Added multi-line capability for fixed row and line separated events• Batch processing capability to process and send entire files (-x command line parameter)• Minor updates to log rotation handling code |
| 1.5.1 | <ul style="list-style-type: none">• Updated HTML data handling in Recent Events window• Added dynamic ordering to the Objective Configuration window• Fixed objective order processing, now top to bottom• Sped up objective processing• Improved memory handling, substantially decreasing page faults• Minor wording changes |

For more information, contact your SNARE Server Sales Representative

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?



System iNtrusion Analysis & Reporting Environment

- 1.5.2
 - Rolled back memory handling updates as they don't work on all configurations
 - Added option to sending comment (lines starting with #)
- 1.5.3
 - Updated date checking function for % format specifier
- 1.5.4
 - Security update to prevent Cross Site Request Forgery
- 1.5.5
 - Fixed bug when flushing objective list that would occasionally lead to the agent freezing
 - Updated maximum supported record size (now 16kB)
 - Updated Exchange Win2008 LogType specifier
- 1.5.6
 - Added support for files over 2GB
 - Added fix for 2008 file update capture problem
 - Improved file name matching
 - Improved event detection
 - Extended web interface token timeout
- 1.5.6.1
 - Updated micro web server
 - Updated file name matching to support date (%) formats

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?