SIMCommander Enterprise Logger Appliance

SIMCommander Enterprise Logger (SIMC-EL) is a log management solution that helps organization to deal with large volumes of computer-generated log messages (also known as audit records, audit trails, event-logs, etc.). The SIMC-EL covers log collection, centralized aggregation, long-term retention, log search, as well as NTP server. Some additional features such as web portal authentication and reporting are provided as optional modules.

Product Functionalities

Logger

The Logger can be deployed in either centralized log mode or in-line log mode. Log collection is done via both agent-less and agent based mechanisms. Example of agent-less includes UDP and TCP Syslog, where agent based component will be installed on host or server that does not support agent-less.

Log Indexer

Log indexer collects, parses, and stores log messages to facilitate fast and accurate information retrieval. It is designed to optimize speed and performance in finding relevant documents for a log message search. Without an index, the search engine would scan every document in the corpus, which would require considerable time and computing power.

Log Search

Google like (Full-text) Log Search allows you to type certain keywords and get what you are searching for in seconds. Using Log Search functionality, you can get the desired information you need to take proactive measures to secure your network and mitigate network threats.

Regulatory Compliance

To comply with laws and regulatory compliances, log messages collected will be archived into files then MD5 or SHA-1 hashes of the files can be produced and encrypted with AES algorithm to prevent unauthorized access to the hashed values.

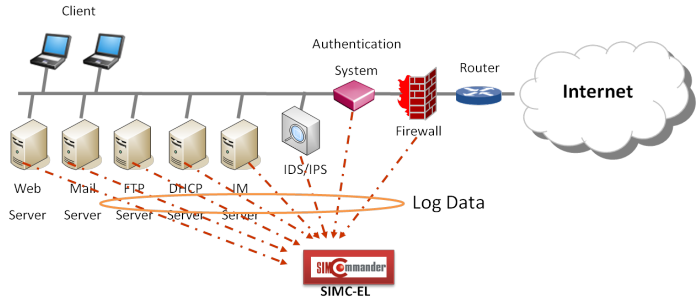
"Enterprise Log Management Solution"

Network Time Server

The network time server helps to synchronize the time of all devices and computers in an organizational network resulting in an improvement of accuracy in usual operational tasks performed by security analyst such as log data correlation and security incident tracking.

SIEM/Reporting

Log messages can be forwarded to SIMC Enterprise and 3rd party SIEM solutions via TCP and UDP Syslog protocols for further real-time incident tracking and analysis, together with its built-in reporting engine, statistical and detailed reports can be generated based on message header such as device name, IP address, severity level, etc.

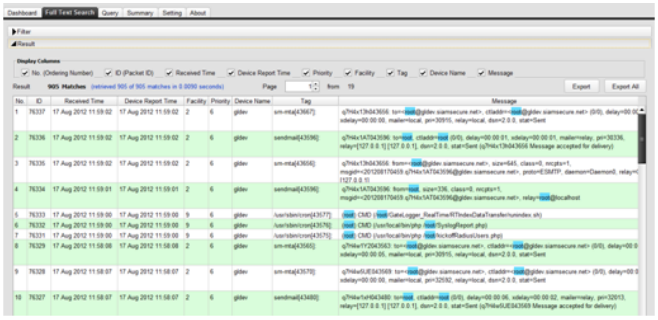


Web Portal Authentication

Enforces organizational wide security policy via an implementation of "User Authentication" before granting user access to critical resources on the network and the Internet.

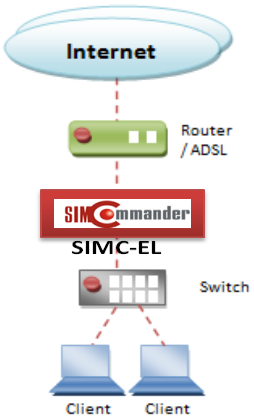
Sample Screen Shots

Example of Real-time Dashboard

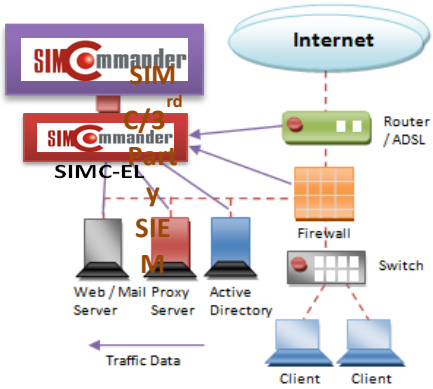


Example of Raw log Search

Deployment Mode



In-line Log Mode



Centralized Log Mode

Model & Features

Hardware Model	EL-1050	EL-1200	EL-3200	EL-5200	EL-6200L	EL-6200
Management	Web Brower (HTTP,HTTPS) CLI (Telnet, SSH) SNMP					
Deployment	Centralized Log Mode/ Inline Log Mode					
EPS	6,000	12,000	20,000	40,000	60,000	60,000
Compression Ratio (Average)	10:1					
Supported Sources	▪ Syslog (UDP, TCP) ▪ Log file (Text, XML based sources) via agent ▪ Host/Application Logs via agent ▪ ODBC (TCP 1433) via agent ▪ OPSEC via agent					
Log Indexer	✓					
Log Search	✓					
Real-time Monitoring	✓					
NTP Server	✓					
User Authentication	✓ Optional					
Compliance Report	✓ Optional (ISO/IEC 27001)					

SIMC Log Analyzer / SIEM	***Optional***				
Number of Devices Supported	***Unlimited***				
Physical Specifications					
Enclosure	***1U rack mountable***				***2U rack mountable***
10/100/1000 Ethernet Port	***2***				
Storage (RAID) Default/Extended	***500GB/-***	***1TB/-***	***(RAID 0,1) 2x1TB/-***	***(RAID 0,1,5,10) 2x1TB/2x1TB, 2x2TB***	***(RAID 0,1,5,10) 1x2TB/6x2TB***
Power Supply	***Single Supply (100-240 VAC)***				***Dual Supply (100-240 VAC)***
Compliance	***FCC, CE, UL***				

SIMCommander
Unit 301, 3/F, Assun Pacific Centre, 41 Tsun Yip Street, Kwun Tong, Hong Kong
Tel: (852) 2827 0393, Fax: (852) 2877 2604, Email: info@simc-inc.com