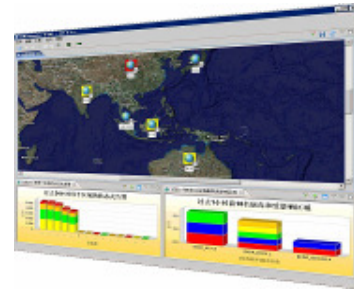


SIMCommander Express

Windows Event Log Management

SIMCommander Express Overview

SIMCommander Express is slim, easy to use Windows Event Management software designed for company of all sized and government organizations to centrally monitor, analysis, report and archive their Windows event logs. SIMCommander Express automatically collects, correlates, visualizes and store Windows event logs from any Windows servers and workstations and transforms these collected data into meaningful and actionable information.



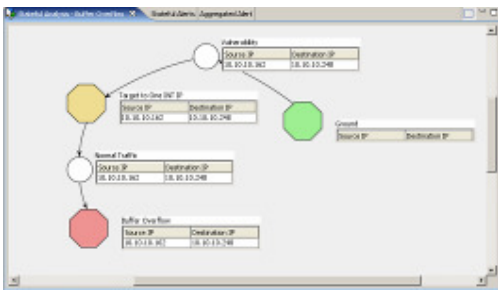
Features Overview:

Windows Event Log Collection

With SIMCommander Express, you can consolidate and monitor Windows event logs in real-time. SIMCommander Express collects application, system, and security event data from all Windows systems within your network and automatically stores them all in a centralized database.

Out-of-the-box Advanced Correlation Rule

SIMCommander Express includes a powerful and flexible real-time correlation engine which provides out-of-the-box scenario-based correlation rules that allow you to start detecting policy violations, abnormal activities and security related events immediately. For example, a file server in the sales department is a critical server that stored all customers and businesses information which no one should be allowed to access the server unless they are authorized.



Key Benefits:

- Graphical user interfaces for easy monitoring, analysis and reporting on critical business servers
- Comprehensive reports and centralized archival of all Windows event logs for meeting audit and regulatory requirements
- Comparison report allows you to compare the current and historical data to proactively identify potential system problems
- Powerful and flexible correlation rules detect abnormal activities and policy violations
- Improve visibility and security intelligence on production and critical servers
- Drill-down capabilities to access events detail information for analysis
- Fast and easy deployment
- Maximize business servers uptime to increase productivity and operational efficiency

Real-time Alert Notification

SIMCommander Express proactively notifies you when a security incident is occurred or an event over the pre-defined threshold configuration in real-time. Alert notification can be defined globally or by individual Windows node.

SIMCommander Express Alert Response includes various notification types including Email, SMS, SNMP traps, Sounds, run a command line and Helpdesk integration (Remedy, HP OpenView, and SIMCommander IMM).

Comprehensive Reports

SIMCommander Express out-of-the-box report templates including Management reports, Administrator reports, Alert Statistics and Compliance reports to target different levels of audiences within the organization. SIMCommander Express also allows you to customize these pre-defined report templates to suit your specific requirements.

SIMCommander Express Real-time Reports act as a dashboard to visualize and summarize major Windows event logs and alerts in graphical views. The reports display real-time event logs or real-time security trends according to the user-defined configurations with drill down capabilities to help you in meeting audit and industrial regulation requirements.



Trend Analysis and Comparison Reports

SIMCommander Express provides report comparison function that allows you to compare Windows event logs by weekly or monthly basis to provide the trend of user or server activities. System administrators can review the comparison reports to improve system maintenance and security effectively.

Compliance Reporting

SIMCommander Express enables you to reduce the cost and effort to comply with internal audit, regulations and industry standards such as PCI-DSS with just simple clicks.

Create Reports for New Compliances

SIMCommander Express reports also can be tailored to meet your specific audit and compliance requirements.

Visualize Windows Event Logs

Visualize information can significantly improve productivity. SIMCommander Express expands the visibility from the large amounts of event logs data into graphical map view for you rapidly and easily to pinpoint which Windows systems are having problem or being attacked.

Windows Event Logs Query

Log query is a very important step to analyze large amount of raw data. You can list down your search criteria and filter out non-related data. SIMCommander Express provides a fast and easy query function for you to query the Windows event logs data effectively.

Supported Windows System

- Windows 2003 / 2008 server event logs,
- Windows NT/ 2000 event logs,
- Windows XP event logs, and
- Windows Vista event logs.

System Requirements

- Intel Dual-Core 2.0GHz Processor
- 2GB Memory
- 500GB Hard Disk Space
- Windows 2003 or 2008 Server with latest Service Pack
- SQL 2008 Server Express Edition