

Log Management Suite for WhatsUp Gold

Log files contain a wealth of information to reduce an organization's exposure to intruders, malware, damage, loss and legal liabilities. Log data needs to be collected, stored, analyzed and monitored to meet and report on regulatory compliance standards like Sarbanes Oxley, Basel II, HIPAA, GLB, FISMA, PCI DSS, MiFID, NISPOm and – in Europe – multiple country specific regulations including UK and France Data Protection Acts and the German Federal Data Protection Act.

Yet, monitoring log files is impossible without the right tools since log files come from many different sources, in different formats and in massive volumes.

THE WHATSUP LOG MANAGEMENT SUITE

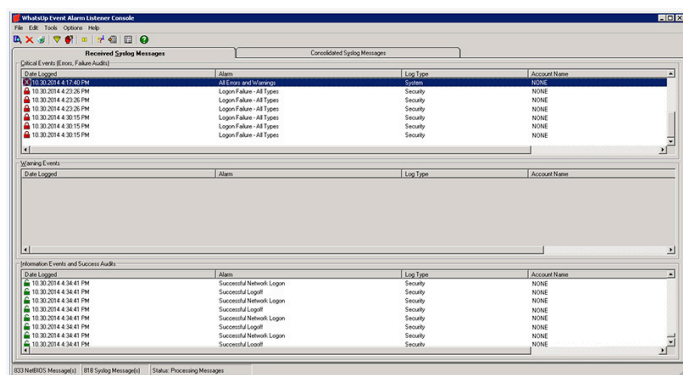
A modular set of applications that can automatically collect, store, alert, analyze and report on Windows Event, Syslog and W3C/IIS log files for real-time security event detection and response, and compliance assurance and forensics. And, when you integrate the suite with your installation of WhatsUp Gold, you'll have insight into your network and log data from a SINGLE pane of glass.

Event Archiver: Automate log collection, clearing and consolidation. Great for assisting in auditing and regulatory compliance.

Event Alarm: Monitor log files and receive real-time notification on key events. Great for intrusion detection and monitoring for domain controller lock-outs and file or folder access.

Event Analyst: Analyze and report on log data and trends. Automatically distribute reports to management, security officers, auditors and other key stakeholders.

Event Rover: Single console for in-depth forensics across all servers and workstations to increase efficiency and save time.



Quickly detect unauthorized activity and security threats.

Awarded the US Army's Certificate of Networthiness (CoN):
 Cert #201004611 – Complete confidence that the WhatsUp Gold family meets strict security, sustainability and interoperability requirements

Document and prove compliance for key compliance initiatives such as HIPAA, SOX, MiFID, etc., with out-of-the-box, point-and-click reporting

Cryptographic hashing on archived logs (key for evidentiary use)

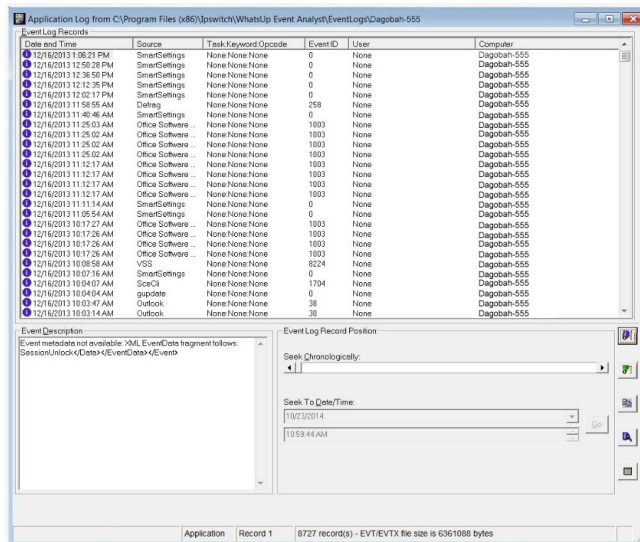
Identify unauthorized events immediately (i.e. access to folders containing sensitive data)

Collect automatically Windows Event, Syslog or W3C/IIS log files across your entire infrastructure

Store log data as long as you need to – multi-year data storage capabilities help you comply with key regulations

Analyze and extract the right information across thousands of log entries

Report on critical errors or compliance-centric failures right from a WhatsUp Gold dashboard



Save time and effort by automating log collection and archiving.

IT operations, compliance officers and security personnel can be sure that the WhatsUp Log Management Suite will not only capture and document every event, but also deliver:

- Comprehensive visibility into internal and external security threats
- Automated collection of Windows Event, Syslog or W3C/IIS logs across your entire infrastructure
- Easier regulatory compliance with point-and-click reporting
- Multi-year data storage to comply with key regulations (i.e. HIPAA mandates six years of retention)
- Ability to correlate events from different sources in a single, holistic view
- Protection of archived log data from tampering via FIPS 140-2 validated cryptographic hashing – key for evidentiary use
- FIPS 140-2 encryption & validation – the highest level of cryptography
- Real-time data views, status and alerting
- Reduced effort to locate and remediate events
- Achieving regulatory compliance at reduced cost

Remote and Agent-Based Collection of Syslog, W3C/IIS and Windows Event Files

Adapts to your network security policies, simplifies configuration tasks and saves time

Supports EVT and EVT-X Format

Easily open and correlate Windows events generated in a heterogeneous environment from one single console – Server 2008 and later, Vista, Server 2003, XP, 2000, NT 4.0

Tiered “Per Server” Licensing for Predictable Budgeting

No need to keep track of how much log data you generate, no hidden costs if your log files grow

Includes Patented Log Healer Technology

Our solution handles and even repairs corrupted Microsoft EVT-X event logs.

The WhatsUp Gold Suite of Integrated Products

Unified IT Monitoring from One Single View



WhatsUp Gold Application Performance Monitor

Monitors, alerts, and reports on application health and performance.



Flow Monitor

Provides visibility into network traffic and bandwidth utilization.



WhatsConfigured

Automates configuration and change management for network devices.



WhatsVirtual

Monitors, alerts, and reports on your VMware environment.



VoIP Monitor

Monitors and reports Voice over IP network performance.

See individual Plug-in Data Sheets

or www.WhatsUpGold.com for more details.

NEXT STEP

**Try Log Management
Free for 30 Days**

[www.whatsupgold.com/free-trial/
log-management.aspx](http://www.whatsupgold.com/free-trial/log-management.aspx)

ABOUT IPSWITCH

Ipswitch helps solve complex IT problems with simple solutions. The company's software is trusted by millions of people worldwide to transfer files between systems, business partners and customers; and to monitor networks, applications and servers. Ipswitch was founded in 1991 and is based in Lexington, Massachusetts with offices throughout the U.S., Europe and Asia. For more information, visit www.ipswitch.com.

Ipswitch, Inc.
83 Hartwell Avenue
Lexington, MA 02421 USA
(781) 676-5700

Kingsfordweg 151
1043 GR Amsterdam
The Netherlands

Ipswitch Japan 株式会社
〒106-0047
東京都港区南麻布4-11-22
南麻布T&Fビル 8階



www.WhatsUpGold.com