# WhatsUpGold

# WhatsUp Log Management

requirements

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

**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

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.

Received Syslog Messages	Consolidated	Syslog Messages		
itical Events (Enors, Falure Audits)				
Date Logged	Alam	Log Type	Account Name	
10.30.2014 4.17.40 PM	All Errors and Warnings	System	NONE	
10.30.2014 4 23:26 PM	Logon Falure - All Types	Security	NONE	
10.30.2014 4 23.26 PM	Logon Falure - All Types	Security	NONE	
10.30.2014 4/23/26 PM	Logon Falure - All Types	Security	NONE	
10.30.2014 4:30:15 PM	Logon Falure - All Types	Security	NONE	
10.30.2014 4:30:15 PM	Logon Falure - All Types	Security	NONE	
10.30.2014 4:30:15 PM	Logon Falure - All Types	Security	NONE	
ming Events				
	Alarm	Log Type	Account Name	
øs Logged	Alam	Log Type	Account Name	
de Logerd	Alam	Log Type	Account Name	
in Logged	Alen			
the Logged mattern Events and Success Audits	Alam	Log Type	Account Name	
in Logged material Events and Success Audio Met Logged	Alem Successful Network Logon			
the Logged matter Creeks and Success Audio Histoped Histoped 1932 2014 42 de 194	Alam	Log Type Stocaly	Account Name NODE	
the Logged makeout Events and Success Audits To 2004 4 2 4 4 16 March 10 2004 4 2 4 16 March 10 2004 4 16 March 10 2 4 16	Alam Successful Network Logon Successful Logolf	Log Type Securly Securly	Access Name NOAE NOAE	
#t logged metro Funct and Science Aulty #t logged 100 2014 6 June 10 PM 100 2014 6 June 10 PM 100 2014 6 June 10 PM	Jatan Social Hand Logis Social Hand Logis Social Hand Logis	Log Tops Secoly Secoly Secoly	Account Name VOIGE NOISE	
Mr Loggel Mr Loggel Hr Loggel 113 2014 4 Al M 113 2014 4 Al M	Alem Successful Network Logen Successful Logel Successful Logel Successful Logel	Lay Teo Socialy Socialy Socialy Socialy Socialy	Account Name NODE NODE NODE NODE	
Me Logent Me Logent Median C. Vera and Locens Ludis Me Logent 110 2014 E 4 de 1 Me 110 2014 E 4 de 1 Me 110 2014 E 4 de 1 Me	Atom Socienti A Neuvi Lopin Socienti A Neuvi Lopin Socienti A Neuvi Lopin Socienti A Neuvi Lopin	Log Type Socity Socity Socity Socity Socity Socity	Account Name NOGE NOGE NOGE NOGE NOGE	

Quickly detect unauthorized activity and security threats.

10/16/2013 16/02 FM         Benef-Sering         Near-Score Nore           10/16/2013 15/02 FM         Senef-Sering         Near-Score Nore           10/16/2013 15/02 FM         Critics Schweire         Near-Score Nore           10/16/2013 11/02 FA         Critics Schweire         Near-Score Nore           10/16/2013 11/03 FA         Critics Schweire         Near-Score Nore	0 0 258 0 1003 1003 1003 1003 1003 1003 1003 0 0 1003 1003 1003 1003 1003 1003	None None None None None None None None	Dagobah-555 Dagobah-585	
1/12 (r/1011)         12:5:5:5:5         SmmelSemign         Name Nove Nove Nove Nove Nove Nove Nove Nov	0 0 258 0 1003 1003 1003 1003 1003 1003 1003 0 0 1003 1003 1003	None None None None None None None None	Dagobah-855 Dagobah-856 Dagobah-858 Dagobah-858 Dagobah-856 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855	
1/21/K20131122: T2: ES PM         Smert Glemings         None None None           1/21/K20131122: T2: T2: SF PM         Smert Gleming         None None None           1/21/K2013112: T2: T4: T4: T4: T4: T4: T4: T4: T4: T4: T4	0 258 0 1003 1003 1003 1003 1003 1003 1003 0 0 1003 1003 1003	None None None None None None None None	Dagobah-855 Dagobah-855 Dagobah-856 Dagobah-856 Dagobah-856 Dagobah-856 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-856 Dagobah-855 Dagobah-855 Dagobah-855 Dagobah-855	
1/21/4/2013 12:02:17.PM         StandSelmigs         None None None None None None None None	0 258 0 1003 1003 1003 1003 1003 1003 1003 0 0 1003 1003	None None None None None None None None	Digiotan-555 Digotan-555 Digotan-555 Digotan-555 Digotan-555 Digotan-555 Digotan-555 Digotan-555 Digotan-555 Digotan-555 Digotan-555 Digotan-555 Digotan-555 Digotan-555	
1/2/16/2011 11:85:54.4         Defeng         None None None           1/2/16/2011 11:85:54.4         Defeng         None None None           1/2/16/2011 11:80:54.4         Defeng         None None None           1/2/16/2011 11:80:54.4         Otto Sehmers         None None None           1/2/16/2011 11:80:54.4         Otto Sehmers         None None None           1/2/16/2011 11:80:54.4         Otto Sehmers         None None None           1/2/16/2011 11:80:74.4         Otto Sehmers         None None None           1/2/16/2011 11:21:74.4         Otto Sehmers         None None None           1/2/16/2011 11:27:84.4         Otto Sehmers         None None None           1/2/16/2011 11:27:84.4         Otto Sehmers         None None None      <	258 0 1003 1003 1003 1003 1003 1003 1003 0 0 1003 1003 1003	None           None	Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555	
1/2/16/2011 11:85:54.4         Defeng         None None None           1/2/16/2011 11:85:54.4         Defeng         None None None           1/2/16/2011 11:80:54.4         Defeng         None None None           1/2/16/2011 11:80:54.4         Otto Sehmers         None None None           1/2/16/2011 11:80:54.4         Otto Sehmers         None None None           1/2/16/2011 11:80:54.4         Otto Sehmers         None None None           1/2/16/2011 11:80:74.4         Otto Sehmers         None None None           1/2/16/2011 11:21:74.4         Otto Sehmers         None None None           1/2/16/2011 11:27:84.4         Otto Sehmers         None None None           1/2/16/2011 11:27:84.4         Otto Sehmers         None None None      <	0 1003 1003 1003 1003 1003 1003 1003 0 0 1003 0 0 1003 1003	None           None	Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555	
1/21/K2011118-06-AM         Seme6Seings         Name Nove Nove           1/21/K2011118-01-AM         Office Softwares         Name Nove Nove           1/21/K2011118-01-AM         Office Softwares         Name Nove Nove           1/21/K20111112-01-AM         SomeSoftware         Name Nove Nove           1/21/K20111112-01-AM         SomeSoftware         Name Nove Nove           1/21/K20111101-01-AM         Office Software         Name Nove Nove           1/21/K20111101-01-AM         Office Software         Name Nove Nove           1/21/K20111101-24-AM         Office Software         Name Nove Nove           1/21/K20111101-24-AM         Office Software         Name Nove Nove<	0 1003 1003 1003 1003 1003 1003 1003 0 0 1003 0 0 1003 1003	None None None None None None None None	Dagoban-655 Dagoban-655 Dagoban-655 Dagoban-655 Dagoban-655 Dagoban-655 Dagoban-655 Dagoban-655 Dagoban-655 Dagoban-655 Dagoban-655 Dagoban-655	
1/12/6/071111136/0744         Ottos Sohwima         Narea Nove Inore           1/12/6/07111136/0744         Ottos Sohwima         Narea Nove Inore           1/12/6/07111136/0744         Ottos Sohwima         Narea Nove Inore           1/12/6/07111136/0744         Ottos Sohwima         Narea Nove Inore           1/12/6/07111137/0744         Ottos Sohwima         Narea Nove Inore           1/12/6/071111127/1444         Ottos Sohwima	1003 1003 1003 1003 1003 1003 1003 1003	None None None None None None None None	Dagobah-655 Dagobah-655 Dagobah-655 Dagobah-655 Dagobah-655 Dagobah-655 Dagobah-655 Dagobah-655 Dagobah-655 Dagobah-655 Dagobah-655 Dagobah-655	
1/27/4/2013 11:32:02:04         Ottos Solvensa         Nane Noren Fore           1/27/4/2013 11:32:02:04         Ottos Solvensa         Nane Noren Fore           1/27/4/2013 11:32:02:04         Ottos Solvensa         Nane Noren Fore           1/27/4/2013 11:32:04         Sone Solvensa         Nane Noren Fore           1/27/4/2013 11:32:04         Sone Solvensa         Nane Noren Fore           1/27/4/2013 11:32:04         Sone Solvensa         Nane Noren Fore           1/27/4/2013 11:32:04         Ottos Solvensa         Noren Noren Fore           1/27/4/2013 11:32:04         Ottos Solvensa         Noren Noren Fore           1/27/4/2013 11:32:04         Ottos Solvensa	1003 1003 1003 1003 1003 1003 1003 0 0 1003 1003 1003	None None None None None None None None	Dağobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555	
1/27/6/2013 113 (20: A4         Office Software         Name None None           1/27/6/2013 113 (20: A4         Office Software         Name None None           1/27/6/2013 113 (20: A4         Office Software         Name None None           1/27/6/2013 113 (20: A4         Office Software         Name None None           1/27/6/2013 113 (21: A4         Office Software         Name None None           1/27/6/2013 111 (21: A4         Office Software         Name None None           1/27/6/2013 111 (21: A4         Office Software         Name None None           1/27/6/2013 111 (21: A4         SmedSoftware         Name None None           1/27/6/2013 111 (21: A4         SmedSoftware         Name None None           1/27/6/2013 111 (21: A4         Office Software         Name None None           1/27/6/2013 111 (21: A4         Office Software         Name None None           1/27/6/2013 111 (21: A4         Office Software         Name None None           1/27/6/2013 111 (21: A4         Office Software         Name None None           1/27/6/2013 111 (21: A4         Office Software         Name None None           1/27/6/2013 111 (21: A4         Office Software         Name None None           1/27/6/2013 111 (21: A4         Office Software         Name None None           1/27/6/2013 111 (21: A4	1003 1003 1003 1003 1003 1003 1003 0 0 1003 1003	None None None None None None None None	Dagotah-555 Dagotah-555 Dagotah-555 Dagotah-555 Dagotah-555 Dagotah-555 Dagotah-555 Dagotah-555 Dagotah-555 Dagotah-555	
1/20/2013/11/35/02.44         Office Software         Near None None           1/20/2013/11/27.44         Office Software         Near None None None None None None None None	1003 1003 1003 1003 0003 0 0 1003 1003	None None None None None None None None	Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555	
1/21/6/201311/217.A44         Oftice Software         Nene None None           1/21/6/201311/257.A44         SmartSoftware         Nene None None           1/21/6/201311/257.A44         Oftice Software         Nene None None	1003 1003 1003 1003 0 0 1003 1003 1003	None None None None None None None	Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555	
1/21/5/2013 11:21:7.AM         Oftice Softwere         Nene None None           1/25/6/2013 11:22:7.AM         Oftice Softwere         Nene None None           1/25/6/2013 11:22:7.AM         Oftice Softwere         Nene None None           1/25/6/2013 11:25:7.AM         Smart Softwere         None None None           1/25/6/2013 11:25:7.AM         Oftos Softwere         None None None           1/25/6/2013 11:25:7.AM         Oftos Softwere         None None None           1/25/6/2013 11:25:7.AM         Oftos Softwere         None None None           1/25/6/2013 11:25:AM         Oftos Softwere         None None None	1003 1003 0 0 1003 1003 1003 1003	None None None None None None None	Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555	
1/216/2013111217 AM Office Softwere None None None None None None None None	1003 1003 0 1003 1003 1003	None None None None None None	Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555	
112/16/2013 111:217.AM Office Softwere None None None 112/16/2013 111:217.AM SmertSettings None None None 12/16/2013 11:1114 AM SmertSettings None None None None 12/16/2013 10:1727 AM Office Softwere None None None 12/16/2013 10:1726 AM Office Softwere None None None 12/16/2013 10:1726 AM Office Softwere None None None None 12/16/2013 10:1726 AM Office Softwere None None None None None None None Non	1003 0 1003 1003 1003	None None None None None	Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555	
112/16/2013 11.11.14 AM SmeriSettings None None None 112/16/2013 11.0554 AM SmeriSettings None None None None 12/16/2013 10.1727 AM Office Software None None 12/16/2013 10.1726 AM Office Software None None None None	0 0 1003 1003 1003	None None None None None	Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555 Dagobah-555	
112/16/2013 11:05:54 AM         SmertSettings         NoneNoneNone           112/16/2013 10:17:27 AM         Office Software         NoneNoneNone           12/16/2013 10:17:26 AM         Office Software         NoneNoneNone	0 1003 1003 1003	None None None None	Dagobah-555 Dagobah-555 Dagobah-555	
112/16/2013 10:17:27 AM         Office Software         None:None           112/16/2013 10:17:26 AM         Office Software         None:None           112/16/2013 10:17:26 AM         Office Software         None:None:None           112/16/2013 10:17:26 AM         Office Software         None:None:None	1003 1003 1003	None None None	Dagobah-555 Dagobah-555	
H12/16/2013 10:17:26 AM Office Software None:None:None     V12/16/2013 10:17:26 AM Office Software None:None:None     V12/16/2013 10:17:26 AM Office Software None:None:None	1003 1003	None None	Dagobah-555	
12/16/2013 10:17:26 AM Office Software None:None:None 12/16/2013 10:17:26 AM Office Software None:None:None	1003	None		
12/16/2013 10:17:26 AM Office Software None:None:None				
		None	Dagobah-555	
	8224	None	Dagobah-555 Dagobah-555	
12/16/2013 10:02:58 AM VSS None:None:None 12/16/2013 10:07:16 AM SmartSettings None:None:None	8224	None	Dagobah-555 Dagobah-555	
12/16/2013 10:07/16 AM SmartSettings None:None:None 12/16/2013 10:04:07 AM SceCli None:None:None	1704	None	Dagobah-555 Dagobah-555	
12/16/2013 10:04:07 AM Scecil None:None:None 12/16/2013 10:04:04 AM gupdate None:None:None	0	None	Dagobah-555	
12/16/2013 10:04:04 AM gupdate None:None:None 12/16/2013 10:03:47 AM Outlook None:None:None	38	None	Dagobah-555	
12/16/2013 10:03:47 AM Outlook None:None: 12/16/2013 10:03:14 AM Outlook None:None:None	38	None	Dagobah-555 Dagobah-555	
12/16/2013 10:03:14 AM Outlook None:None:None	30	None	Dagopan-555	
ent Description ent metadata not available: XML Even/Data fragment follows:	Event Log Recor	d Position		[
ssionUnlock	Seek Chronologi	icelly:		
	4			•
				-
	Seek To Date/Time:			
	10/23/2014			1
	10/23/2014			Go
	10.59.44 AM			
	1			-
Ψ				

Save time and effort by automating log collection and archiving.



# WhatsUp Log Management

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 EVTX 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 EVTX 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.

# 62

## VoIP Monitor

Monitors and reports Voice over IP network performance.

See individual Plug-in Data Sheets or <u>www.WhatsUpGold.com</u> for more details.

# **NEXT STEP**

### Try Log Management Free for 30 Days

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

Copyright © 2015, Ipswitch, Inc. All rights reserved. WhatsUp Gold is a registered trademark and Ipswitch is a trademark of Ipswitch, Inc. Other products or company names are or may be trademarks or registered trademarks and are the property of their respective holders. DS-WuG-Log-1506-v2.0