IPSWITCH

WhatsUp Event Analyst v10.x User Guide

CHAPTER 1 WhatsUp Log Management Help and User Guide

CHAPTER 2 WhatsUp Event Analyst Menu Descriptions

CHAPTER 3 Accessing and Viewing Event Log Sources

CHAPTER 4 Events and Filters

CHAPTER 5 Settings, Preferences, and Other Options

CHAPTER 6 Exporting

CHAPTER 7 Working with Reports

CHAPTER 8 Managing Syslog Reports

CHAPTER 1

WhatsUp Log Management Help and User Guide

In This Chapter

WhatsUp Event Analyst Overview and Architecture

What Does WhatsUp Event Analyst Do?

WhatsUp Event Analyst is an interactive tool for network and security administrators that allows them to mine for critical events happening on their server and workstation event logs. Administrators can work with a variety of event log data formats, such as active computer EVT/EVTX log files, saved EVT/EVTX log files, comma-delimited text files (exported from the Microsoft Event Viewer or Ipswitch's WhatsUp Event Archiver program), or database tables created by Ipswitch's WhatsUp Event Archiver, WhatsUp Event Alarm, or WhatsUp Event Analyst programs. Furthermore, administrators can create basic or advanced filters and use them to mine for specific subsets of events present in an event log source. Users of WhatsUp Event Analyst can run pre-built or custom-designed reports interactively or on a scheduled basis to present critical information to management and other interested parties.

What Are WhatsUp Event Analyst's Primary Features?

WhatsUp Event Analyst provides the network administrator with a multi-threaded, multiple window interface for working with event log entries from a variety of sources. Because of this architecture, administrators can switch rapidly back and forth between different event log sources at the same time. Furthermore, certain operations like event log reading, filtering, printing, and exporting can occur in the background while other tasks continue in the foreground.

In addition, WhatsUp Event Analyst comes with a local database full of predefined log filters. Besides those filters provided by the program, you can add your own frequently used filter/event definitions to the local database for later use. Then, whenever they are needed, you can quickly summon them by name from the database.

WhatsUp Event Analyst ships with many pre-built reporting modules that can produce commonly demanded reports for the network administrator and management. These report modules produce professional-looking HTML reports and/or compact CSV datasets on demand, or you can use the WhatsUp Event Analyst Service to schedule automatic report generation at off peak times. A custom report designer is also available to the administrator who wishes to track event activity in an area where a pre-built report is not already provided.

How Does WhatsUp Event Analyst Work?

The WhatsUp Event Analyst program can be subdivided into 2 major parts:

The WhatsUp Event Analyst GUI Program: This is the centralized GUI administration console that you use to filter, view, export, and report on event log sources throughout your network. To read more about its user interface, visit the WhatsUp Event Analyst's Main Interface topic in this help file.

The WhatsUp Event Analyst Service: This is the service that produces scheduled reports for the administrator. When it is time to produce a report, the service instructs WhatsUp Event Analyst to create a report on disk, and optionally email it to selected parties.

Deployment and Usage Scenarios

Occasional Forensic Analysis

Some users may only need to perform occasional review of event log entries in their active or saved EVT/EVTX files. In this case, a WhatsUp Event Analyst user can build an ad-hoc report by working directly with a single EVT/EVTX file, or, if necessary, can manually import a few EVT/EVTX files into a Microsoft Access (.mdb file) database and then open the table containing the exported entries inside WhatsUp Event Analyst.

Routine Analysis and Reporting On a Small Network

If routine analysis of event logs in a small network setting (e.g. 5 - 20 servers) is desired, we recommend purchasing an appropriate amount of Ipswitch's WhatsUp Event Archiver licenses, and setting up a regular event log collection strategy that funnels events into an Access or Microsoft SQL Server database. Then, you can create a link to these WhatsUp Event Archiver database tables inside WhatsUp Event Analyst, and routinely run/schedule reports or queries (filters) against those tables to obtain desired information from multiple computer sources in one view/report.

Routine Analysis and Reporting On a Large Network

On a network with greater than 20 servers, we recommend using the same strategy as the one mentioned above for small networks, except use WhatsUp Event Archiver to funnel events into a Microsoft SQL Server database. Microsoft SQL Server can scale to a much greater degree than Microsoft Access, and can handle the inflow of large volumes of event log information. Furthermore, you can create advanced table indexes (either on your own, or using WhatsUp Event Analyst) to speed filter queries or report generation against these data sources.

Well-connected Local Area Networks

Deploying WhatsUp Event Archiver in a Local Area Network environment is one of the easiest ways to configure and use the application. If all machines whose logs will be collected reside in the same domain (or trusting domains) and are well connected by 10Mbit, 100Mbit, or Gigabit Ethernet links, simply choose one server or workstation that will run WhatsUp Event Archiver. If you have more than 100 servers whose logs must be archived, consider setting up multiple WhatsUp Event Archiver instances on different servers for better load balancing. Then, from the WhatsUp Event Archiver Control Panel, Click the **Tools** menu, and then select **Step-By-Step Wizards**. From the sub-menu, select **Choose Setup Archiving for Multiple Computers at Once** to establish a log collection strategy across multiple machines.

If you have a well-connected LAN with non-trusting domains, set up an WhatsUp Event Archiver system in each separate domain, or create custom domain mappings in WhatsUp Event Archiver and establish a common local administrator account across all systems under which the WhatsUp Event Archiver Service runs.

Wide Area Networks (WANs) or Demilitarized Zones (DMZs)

Deployment of WhatsUp Event Archiver in a WAN environment or DMZ setting is a little more complex, but still manageable.

Starting in Version 7 of WhatsUp Event Archiver, you can also utilize a "Working Directory" that is local to the machine where WhatsUp Event Archiver is installed. If you plan to do a lot of processing to a log after it is archived, such as creating an MD5 hash of the file, converting it to another format (e.g. text file or database table), and/or zip compressing it, WhatsUp Event Archiver will consume substantially less bandwidth if the EVT/EVTX file is first transferred to the WhatsUp Event Archiver server before such processing. You can control how large a file must be before WhatsUp Event Archiver transfers it to the "Working Directory" by selecting WhatsUp Event Archiver Preferences from the **Options** menu, and then selecting the Bandwith Optimizer tab. All files larger than the size limit are moved into the Working Directory with log processing performed locally, and all files smaller than the size limit are not moved, with log processing taking place across the network. You can experiment with the size of files that should be copied across the WAN link before processing.

If reliable log archiving cannot be accomplished by using the Working Directory, consider setting up one WhatsUp Event Archiver system at each end of the WAN link. This reduces traffic flowing across the often bandwidth-limited WAN link. If data needs to flow from the remote WAN site to the central network, instruct WhatsUp Event Archiver to push the data upstream using TCP/IP-based ODBC connections, or have WhatsUp Event Archiver compress flat files (EVT/EVTX or Text) into ZIP files and then transport them using traditional Microsoft File and Print Sharing or via an FTP server. Only the finished product of log processing will then be sent over the WAN link.

For database collection in extremely bandwidth-limited WANs, or if auditing requirements produce log file sizes in excess of what WAN link bandwidth can support, contact Ipswitch Support (*http://www.whatsupgold.com/support* (*http://www.whatsupgold.com/support/library/index.aspx*)) regarding the WhatsUp Event Archiver Importer utility, which is designed to process compressed EVT/EVTX and TXT files into a centralized database automatically when these files arrive at a local fileshare.

Demilitarized zones often do not allow typical Microsoft networking connections between machines, so you should install WhatsUp Event Archiver to each machine residing in the DMZ. If you have a large number of machines in the DMZ, contact *Ipswitch Support* (*http://www.whatsupgold.com/support/library/index.aspx*) for a tool that will help you automate the individual rollout of the product using unattended setups. Once the software is installed on each machine, configure the machines to push the data back inside the protected network using TCP/IP-based ODBC connections or FTP servers over specific ports. You may need to adjust certain firewall settings in order for data to flow inward as described.

Event Log Data Formats - Pros and Cons

Choosing which event log data format to use with WhatsUp Event Analyst is ultimately a function of what your log analysis needs are. The following section discusses the different log types compatible with WhatsUp Event Analyst, and their advantages/disadvantages.

EVT/EVTX Files (From Active Computers or Previously Archived Logs)

EVT files are the native format for event logs from Microsoft Windows XP and 2003 systems. EVTX files are the native format for event logs from Microsoft Windows Vista, Windows 2008 Server, and Windows 7. WhatsUp Event Analyst can work with active and saved EVT/EVTX files; active computer EVT/EVTX files being the files that the EventLog service is still writing events to, and saved EVT/EVTX files being the files archived by the Microsoft Event Viewer, Ipswitch's WhatsUp Event Archiver, or another program.

Pros: No conversion is required to work with these log files. Files can be analyzed/reported on even when still active on a system.

Cons: Generally slower to read/analyze than event log entries in a text file or database table, and EVT files cannot be indexed. WhatsUp Event Analyst must work with them one at a time, so cross-computer analysis is impossible unless they are first converted into a database table. In many cases, access to the original network is required for the most complete reporting, as EVT and EVTX files hold lookup references to other necessary data (such as account names on a PDC, or message files from the originating server):

Comma-Delimited Text Files (Microsoft Event Viewer or WhatsUp Event Archiver Format)

Comma-delimited event log files typically separate each event log record by a carriage-return line-feed sequence, and separate each field within a record with a comma. WhatsUp Event Analyst can work with comma-delimited event log files created by the Microsoft Event Viewer or Ipswitch's WhatsUp Event Archiver tool.

Pros: Easily importable into Access, Excel, and other third-party data analysis tools. Relatively fast to read.

Cons: WhatsUp Event Analyst must work with one at a time, so cross-computer analysis is impossible unless they first converted into a central database table.

Access Database Tables

Microsoft Access databases can house event log data from multiple computers in a single table and can be indexed, allowing for rapid filtering of log data and more comprehensive reports. WhatsUp Event Analyst can work with Microsoft Access database tables created by Ipswitch's WhatsUp Event Archiver or WhatsUp Event Alarm programs, as well as database tables created by WhatsUp Event Analyst itself via its Export menu.

Pros: Rapidly searchable and viewable. Can contain event log entries from different event log sources, easing cross-computer analysis. Easy to setup and maintain.

Cons: Not as scalable as an ODBC database server, such as Microsoft SQL Server. Each Access database created on disk can only hold 2 gigabytes worth of data. Access cannot support as many simultaneous users as well as a database server can.

Microsoft SQL Server Database Tables (ODBC)

Like Microsoft Access, ODBC database server tables can house event log data from multiple systems in single tables, can be indexed, and subsequently can produce fast and comprehensive filters and reports. WhatsUp Event Analyst can work with ODBC database server tables created by Ipswitch's WhatsUp Event Archiver or WhatsUp Event Alarm programs, as well as database tables created by WhatsUp Event Analyst itself via its Export menu.

Pros: Rapidly searchable and viewable. Can contain event log entries from different event log sources, easing cross-computer analysis. Highly scalable, even for large networks producing massive amounts of event log data.

Cons: Requires some additional knowledge to maintain. Additional software licensing costs for the database server itself may apply.

Initial Setup

The links below open topics in the WhatsUp Event Analyst Quick Setup Help Guide.

Installation Requirements (on page 15)

Before You Begin (on page 16)

Microsoft Vista, Server 2008, and Windows 7 Requirements and Recommendations (on page 18)

Other Recommendations (on page 18)

Configuring the WhatsUp Event Analyst Service Account (on page 44)

WhatsUp Event Analyst's Feature Areas

WhatsUp WhatsUp Event Analyst's Feature Areas

In order to make the administration of your network's event logs as simple as possible, WhatsUp Event Analyst implements a multiple document view so that you can work with log entries from multiple sources at the same time. WhatsUp Event Analyst allows you to view and filter event log entries from active computers, archived event log (EVT / EVTX) files, archived comma-delimited text log files, as well as Access database tables and ODBC database tables populated by WhatsUp Log Management. Furthermore, you can save and clear event logs from active computers, plus export log entries from any source into a variety of other formats (e.g. text, HTML, Access, and ODBC). You can print customized HTML and CSV reports of filtered and non-filtered log data, or produce one of Ipswitch's many prebuilt reports. For additional convenience, these reports can be automated and scheduled by the WhatsUp Event Analyst Service.

Here are the 3 components of the WhatsUp Event Analyst interface:

WhatsUp Event Analyst Menus

Each of the seven Control Panel menus has a different set of commands to help you manage your event logs. To find out more about each menu, click on each menu name below:

File (on page 20)

Edit (on page 21)

View (on page 22)

Options (on page 22)

Export (on page 23)

Reports (on page 23)

Help (on page 24)

Toolbar

The toolbar serves as a quick access mechanism to many of the commands present in the 6 of the 7 WhatsUp Event Analyst menus. If you hover over any toolbar button, descriptive text displays, indicating what menu option the button controls.

Log View Window

Every source of event log entries, be it an active computer log, saved EVT/EVTX file, text file, or Access/ODBC database tables, is represented in the Log View Window. This window presents options for quickly seeking through the log chronologically or by date and time, and also allows the user to add events to the internal WhatsUp Event Analyst events and filters database, copy them into the clipboard, or research them online.

Organization- Managing Licenses

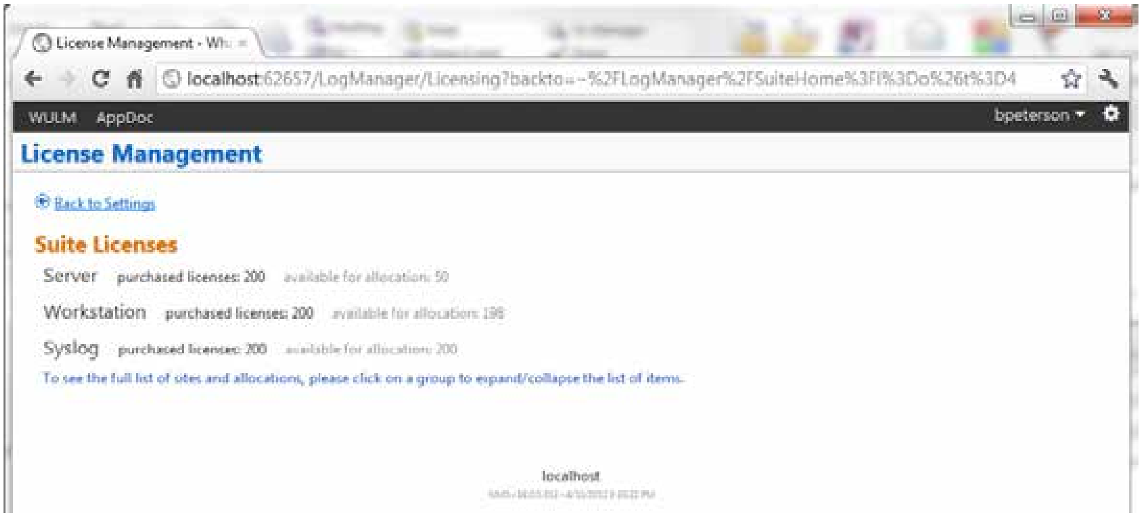
After installing WhatsUp Log Management, you must run the Licensing Management tool. The tool is accessible from both the installation wizard and your Start menu (Start > All Programs > WhatsUp Log Management > Manage WhatsUp Log Management License).

From the License Management tool, paid WhatsUp Log Management users can enter their serial number; non-paid WhatsUp Log Management users can request a 30 day evaluation license.

During your evaluation period, you can use WhatsUp Log Management to work with, analyze, and report on logs on up to 250 different devices.

Call us at **781-676-5700** or visit *Ipswitch's sales website* (*http://www.whatsupgold.com/online-shop/log-management.aspx*) to make a purchase with a credit card, purchase order, or to find resellers in your area.

After purchasing WhatsUp Log Management, access the License Management area of the Web interface to allocate licenses across business units and sites.


License Management - Wh
localhost:62657/LogManager/Licensing?backto=~%2FLogManager%2FSuiteHome%3Fl%3Do%26t%3D4
WULM
AppDoc
bpeterson
Back to Settings
localhost

License Management

Suite Licenses

Server purchased licenses: 200 available for allocation: 50

Workstation purchased licenses: 200 available for allocation: 198

Syslog purchased licenses: 200 available for allocation: 200

To see the full list of sites and allocations, please click on a group to expand/collapse the list of items.

If, after registering WhatsUp Log Management, you discover you need more licenses, contact Ipswitch sales by phone or access *Ipswitch's sales website* (*http://www.whatsupgold.com/online-shop/log-management.aspx*). After your licensing needs are processed, you must return to the License Management tool and re-run the tool to update WhatsUp Log Management.

Your license determines the areas of WhatsUp Log Management to which you have access. The example in the above screen shot is for a full WhatsUp Log Management Suite license, providing access to Event Archiver, Event Alarm, and Event Analyst and the ability to work with servers, workstations, and syslogs. A base WhatsUp Log Management License provides access to Event Archiver and the ability to work with servers.

A note about licensing enforcement: If you have a license for working with servers but not workstations or syslogs, if you attempt to use WhatsUp Log Management to work with workstations or syslogs, all of your license allocations are reset to zero (0); including the areas of WhatsUp Log Management for which you have licenses.

Troubleshooting/Contacting Technical Support

If for any reason logs are not being monitored correctly (e.g. missed or missing notifications), always check the Application Event Log on the machine or machines running the WhatsUp Event Alarm program. WhatsUp Event Alarm logs information about any monitoring errors in the local Application Event Log. Look closely for any warning or error events from the WhatsUp Event Alarm Service, and if they exist, read the description of the error or warning to ascertain the reason why monitoring failed on a particular log.

The easiest way to review these log entries is to use the built-in WhatsUp Event Alarm Log Entries Viewer dialog available from the Tools menu.

Also, check the statistics about when logs were last checked, by pressing F5 in the main window of WhatsUp Event Alarm. If there is a large difference between the time the logs were last checked and the current time on the WhatsUp Event Alarm server, you may have a permission problem, a load balancing problem, or a network connectivity issue.

If logs are being checked in a timely manner but notifications are not arriving you may have either configured your notifications incorrectly or firewalls and/or SMTP relay permissions may be preventing WhatsUp Event Alarm from sending out notifications when alarms are detected.

Have this information ready when you visit Ipswitch's Knowledge Base or Support Web Site to research your problem further.

Common WhatsUp Event Alarm Misconfiguration Problems

There are numerous issues that can cause problems with log monitoring, but the issues listed below are the most common:

Is the WhatsUp Event Alarm Service running with full Domain Admin rights, or at least under an account that has local administrator rights on each member server/workstation it monitors?

Monitoring event logs, especially security logs, is a highly privileged operation, so the WhatsUp Event Alarm Service should be running under the context of a Domain Admin (if working with logs in a domain) or an OU Admin (if working with logs in an organizational unit)

Notification messages are arriving in a very delayed fashion, and the delay continues to get worse the longer the WhatsUp Event Alarm Service is running.

There is too much of a load being placed on the WhatsUp Event Alarm Service and its related log monitoring processes. In the WhatsUp Event Alarm Preferences dialog, consider moving the slider closer to the More Immediate Notification setting, consider enabling Turbo Scanning Mode, and also consider increasing the number of dedicated event log scanning processes. If after adjusting these settings and starting and stopping the WhatsUp Event Alarm Service, conditions do not improve, begin removing servers that are generating the greatest number of events until notifications arrive in a timely manner. Then, set up a separate WhatsUp Event Alarm installation solely responsible for monitoring the server logs generating the greatest number of events. For even better results, consider installing WhatsUp Event Alarm locally on these servers, so that WhatsUp Event Alarm is only be responsible for monitoring the logs where it is installed.

To better determine which servers are taking the longest to scan, press "F5" in the main WhatsUp Event Alarm program window and view the Scan Duration column value. The logs with the longest scan durations may need to be isolated on a different installation of WhatsUp Event Alarm.

Events that match alarm criteria are being generated, but no notifications are being sent.

1 If using network popups, verify that you are sending popups to computer names as opposed to user names. Also verify that NetBIOS over TCP/IP is enabled, and that the Messenger service is running on your machine.

2 If using e-mail, verify that your SMTP server can relay mail from the WhatsUp Event Alarm server. Make sure IP restrictions are not preventing mail relay. If you have changed your SMTP server in WhatsUp Event Alarm, shut down and restart the WhatsUp Event Alarm service so it will use the new SMTP server. Test your email server's relaying capabilities by using the Test button in the Define Notifications dialog. Ensure no local or remote firewall is preventing communication over port 25 with the SMTP server. To test this, type: "telnet mysmtpserver 25" at the Run line, where "mysmtpserver" is the name or IP address of your mail server. If you receive a response from the server, you can communicate with it.

3 Ensure the WhatsUp Event Alarm service account has sufficient (e.g. Domain Admin/OU Admin) rights on the machines it is monitoring

4 Verify that you have created the alarm(s) successfully. Leave all fields blank that you do not want to filter on. Make sure that you have checked the type (or types) of events you are interested in (e.g. warnings, errors). Check that no extra whitespace (e.g. tabs and spaces) exist in the Description field if filtering based on description contents. Ensure the Source name and other fields are not misspelled.

Excessive notifications are being sent after adding a new log to the monitoring list

You may not be running the WhatsUp Event Alarm Control Panel with Domain Admin or OU Admin rights. You must be logged on as a domain admin or OU admin so the product can determine the number of entries currently in the event log. Otherwise, it starts scanning from the start of the event log, causing many notifications to be generated at once.

Alternatively, the server in question may be generating massive amounts of events, many of which match alarms you have attached to its logs. You may need to reduce the number of alarms associated with logs on that server, or add additional ignore events to prevent less relevant events from generating notifications.

Are the hidden shares (C$, D$, Admin$, etc) enabled and functioning on all your servers?

These shares must be open and enabled for WhatsUp Event Alarm to monitor logs remotely. If these must be locked down, you will need to install WhatsUp Event Alarm on each machine and let each computer monitor its own event logs individually.

Is the Remote Registry Service enabled on each remote machine?

This service must be running in order for WhatsUp Event Alarm to monitor event logs remotely. On Windows 2003 and later operating systems, the Remote Registry Service can be enabled or disabled.

Does the WhatsUp Event Alarm Service account have Full Control access to the HKLM\System section of the registry on each remote server?

By default, Domain Admins have full control over this section of the registry on all machines in a domain. However, if you have hardened your servers, you may have restricted the Access Control Lists in this section of the registry. Verify that the WhatsUp Event Alarm Service account has full control by using the regedt32.exe utility.

Are name resolution methods working properly on the system running WhatsUp Event Alarm?

WhatsUp Event Alarm depends on name resolution methods like DNS, WINS, and/or NetBIOS to locate monitored systems.If the WhatsUp Event Alarm server cannot resolve system names to IP addresses, monitoring fails and/or performance is affected.

Visiting the Ipswitch Knowledge Base

If you are encountering an error or problem with WhatsUp Event Alarm that is not addressed in this User's Guide, please first visit our Knowledge Base.

Enter in any applicable error numbers or messages in the Search field, or simply leave the Search field blank to browse all articles applicable to WhatsUp Event Alarm.

Contacting Ipswitch Support

If you cannot find a resolution to your issue in our Knowledge Base, please open a support ticket at our Support Web Site.

International Issues and Log File Conversion

When WhatsUp Event Analyst displays or attempts to export log files from their native EVT or EVTX format into other formats, such as comma-delimited text or database tables, it must use a date standard that is acceptable to the receiving format. For example, when exporting log entries to text, it can export them using either the U.S. format (mm/dd/yy), or other country formats, such as (dd/mm/yy). You can choose between these two options by Accessing the Analyst Preferences page and selecting the Regional/Locale tab.

The format you choose has very important repercussions. If you export your log entries to text in a U.S. format, and then try to import them into a database using a European locale, the days and months may be reversed. Likewise, if you export log entries directly into a database, you must make sure that the server running WhatsUp Event Analyst has the same locale defined as the database server. Alternatively, you can override these locale considerations by making all exported entries adhere to a U.S. date format. Regardless, it is important to give this topic consideration as you plan your log analyzing and export strategy.

Legal Information / License Agreement

Legal Information Including Patent and Trademark Notices

WhatsUp Event Analyst is protected by U.S. Patent # 7,155,514. Other patents pending.

WhatsUp, Event Archiver, Event Analyst, Event Alarm, and Event Rover are trademarks or registered trademarks of Ipswitch, Inc.

Microsoft Windows XP®, Microsoft Windows 2003®, Microsoft Windows Vista®, Microsoft Windows Server 2008®, Microsoft Windows Server 2012® Microsoft Windows 7®, Microsoft Access®, and Microsoft SQL Server® are all registered trademarks of Microsoft Corp. Microsoft Windows XP®, Microsoft Windows 2003®, Microsoft Windows Vista®, Microsoft Windows Server 2008®, Microsoft Windows 7®, Microsoft Access®, Microsoft Exchange® and Microsoft SQL Server® will hereafter be referred to as XP, 2003, Vista, 2008, 2012, Windows 7, Access, Exchange, and SQL Server respectively. All other products or technologies not specifically mentioned here are the registered trademarks of their respective companies, and are used by permission.

WhatsUp Event Analyst License Agreement

Ipswitch License Agreement

READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY BEFORE LOADING, AND/OR OTHERWISE USING THE SOFTWARE. THE TERMS OF USE OF THE SOFTWARE ARE DESCRIBED IN THE IPSWITCH LICENSE AGREEMENT OR LICENSE AND MAINTENANCE AGREEMENT FOR THE SOFTWARE WHICH MUST BE EXECUTED BETWEEN YOU (OR YOUR COMPANY OR INSTITUTION) AND IPSWITCH, INC. IF NO SUCH AGREEMENT HAS BEEN EXECUTED, THEN THIS AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE SOFTWARE BETWEEN YOU AND IPSWITCH, AND IT SUPERSEDES ANY PRIOR PROPOSAL OR UNDERSTANDING BETWEEN YOU AND IPSWITCH. BY DOWNLOADING OR INSTALLING THE SOFTWARE, AND/OR USING THE SOFTWARE, YOU ARE ACCEPTING AND AGREEING TO THE

TERMS OF THIS AGREEMENT, AND ARE THEREBY CREATING A CONTRACTUAL AGREEMENT BETWEEN YOU AND IPSWITCH. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, YOU SHOULD NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND PROMPTLY RETURN THE SOFTWARE AND ASSOCIATED DOCUMENTATION.

1. LICENSE GRANT

Ipswitch grants to you, and you accept, a non-exclusive and non-transferable license to use software program(s) provided by Ipswitch, and the accompanying user documentation ("Documentation"), (collectively, the "Software") as purchased by you only as authorized in this Agreement. You may not assign, transfer, rent, or sublicense the Software (any violation of the foregoing will result in automatic termination of the license without any right of refund). The Software consists of proprietary products of Ipswitch or its third party suppliers, and the proprietary rights that protect such property may include, but are not limited to, U.S. and international copyrights, trademarks, patents, and trade secret laws of general applicability. All right, title and interest in and to the Software are and shall remain with Ipswitch or its third party suppliers, as applicable. This Agreement does not convey to you any interest in or title to the Software, but only a limited right of use revocable in accordance with its terms.

You may use the Software on a specific number of computers, as identified at the time of purchase. Each instance of a Virtual Machine (VM) and each instance of a session in an environment where multiple users share computer resources are considered one computer. For Software in which more than one feature set (e.g. "standard", "premium") is available, you may solely use one specific feature set. If you desire a different feature set, you must purchase an upgrade. Feature sets are defined in the Documentation and identified at the time of purchase.

For Software in which more than one level (e.g. "100 users", "300 devices") is available, you may solely use one specific level. If you desire a different level, you must purchase an upgrade. Levels are defined in the Documentation and identified at the time of purchase.

For Software provided to you for an evaluation period, you may use the Software until the completion of the evaluation period.

For Software provided to you as a subscription, you may use the Software until the completion of the subscription period.

For Software acquired by you under a perpetual license, you may use the Software indefinitely.

For Software in which more than one network environment (e.g. "internally owned and operated", "externally owned and operated") is available, you may solely use the Software in a specific network. If you desire a different network environment, you must purchase an upgrade or a separate license. Network environments are defined in the Documentation and identified at the time of purchase.

For Software which includes dynamic content (e.g. anti-virus and anti-spam definitions), said content is sold on a subscription basis and remains current as long as you maintain an active subscription with Ipswitch.

For Software designated as Software Development Kits (SDK), you may create, reproduce and distribute solutions, plug-ins or other derivative works (collectively "applications") solely to end users who have a valid and current license for the associated Software. For SDK Software designated as "Internal Use", you must further restrict distribution solely to end users in your organization.

2. CONSENT TO USE OF DATA

You agree that Ipswitch and its subsidiaries may collect and use technical and related information, including but not limited to technical information about your computer, system and application software, and peripherals, that is gathered periodically to facilitate the provision of software updates, product support and other services to you (if any), and to verify compliance with the terms of this License.

3. INSTALLATION AND RESTRICTIONS

You assume responsibility for selection of the Software to achieve your intended results and for the installation, use, and valid operation of the Software. You agree at all times to maintain records specifically identifying the Software and the personal computers on which the Software is being used and to make such records available for inspection by Ipswitch during normal business hours.

You may make copies of the software media solely for backup, disaster recovery, or archival purposes, which copies shall contain Ipswitch's copyright and other proprietary notices. You may not modify, translate, adapt, decompile, disassemble, decrypt, extract, or otherwise reverse engineer or attempt to discover the confidential source code and techniques incorporated in the Software. You may not create derivative software based on any trade secret or proprietary information of Ipswitch.

4. LICENSE FEES

The license fees paid by you are in consideration of the licenses granted under this Agreement. If the Software is under evaluation and no license fees have been paid, this Agreement will expire at the end of the evaluation period unless you have purchased a license key to enable subsequent activation. If the Software is provided on a subscription basis, this Agreement will expire at the end of the subscription period unless you have purchased a renewal subscription.

5. TERMINATION

This License Agreement is effective until terminated. You may terminate this License Agreement at any time. This License Agreement will also terminate if you fail to comply with any terms and conditions set forth elsewhere herein. You agree upon any termination to destroy the Software together with all copies, modifications and merged portions in any form, and certify in writing that you have done so.

6. LIMITED WARRANTY

For twenty one (21) days (the "Warranty Period") from your date of purchase, Ipswitch warrants for your benefit alone, that (i) the Software will substantially conform to the applicable Documentation and (ii) the media on which the Software is distributed and the Documentation (if any) are free from defects in materials and workmanship and, (iii) during the Warranty Period, the Software will operate substantially in accordance with the Documentation. If during the Warranty Period an error in the Software occurs, you may return the Software to Ipswitch for either repair or replacement, or if so elected by Ipswitch, refund of the license fee paid by you under this Agreement. For any breach of the foregoing warranty during the Warranty Period, your exclusive remedy and Ipswitch's entire liability will be as described in the previous sentence. THE FOREGOING ARE THE ONLY WARRANTIES PROVIDED BY IPSWITCH AND IPSWITCH DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

7. LIMITATION OF LIABILITY

Because computer software is inherently complex and may not be completely free of errors, it is your responsibility to verify your work and to make backup copies, and Ipswitch will not be responsible for your failure to do so. Ipswitch's cumulative liability to you or any party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the license fee paid to Ipswitch for the applicable Software.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL IPSWITCH BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, ECONOMIC, EXEMPLARY, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE IPSWITCH PRODUCTS OR SERVICES, INCLUDING, WITHOUT LIMITATION, DAMAGES OR COSTS RELATING TO THE LOSS OF PROFITS, BUSINESS, GOODWILL, DATA, OR COMPUTER PROGRAMS, EVEN IF IPSWITCH HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

8. U.S. GOVERNMENT RESTRICTED RIGHTS

If the Software is acquired on behalf of a unit or agency of the United States Government this provision applies.

For units of the Department of Defense (DoD), this Software is supplied only with "Restricted Rights" as that term is defined in the DoD Supplement to the Federal Acquisition Regulations, 52.227-7013(c)(1)(ii) and:

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 52.227-7013. Contractor: IPSWITCH, Inc., 10 Maguire Road, Lexington, MA 02421

Government personnel using this Software, other than under a DoD contract or GSA Schedule, are hereby on notice that use of this Software is subject to restricted rights, which are the same as, or similar to those specified above.

9. GENERAL

This Agreement will be governed by the laws of the Commonwealth of Massachusetts without regard to conflict of law principles. The export of this product is governed by the U.S. Bureau of Industry and Security under Export Administration Regulations and may be exported to appropriate countries and end-users based upon their license exception. Export compliance information for each Ipswitch product can be found on the Ipswitch website at http://www.ipswitch.com/company/export_compliance/product.asp. The appropriate classification for each product is specified on Ipswitch's website. It is the responsibility of the exporter to adhere to appropriate Export Administration Regulations. You shall remain fully responsible for and certify compliance with all applicable Export laws and regulations, and you agree to indemnify Ipswitch from all costs, expenses, and liability for such compliance.

Should any term of this Agreement be declared void or unenforceable by any court of competent jurisdiction such declaration shall have no effect on the remaining terms hereof.

IPSWITCH, INC.

83 Hartwell Ave.

Lexington, MA 02421

(781) 676-5700

Fax: (781) 240-5813

Installation Requirements

The following platforms are supported:

- Microsoft Windows XP Professional SP2
- Microsoft Windows 2003 Server SP2
- Microsoft Windows Vista (Business and Ultimate)
- Microsoft Windows Server 2008 / Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows 7

Installation is supported on both 32-bit and 64-bit versions of the above operating systems.

Recommended Hardware Requirements

- Dual-core 2GHz or faster processor
- 2 GB RAM
- 4 GB available hard disk space minimum for database storage, if detected events are stored in a database. Size depends on the volume of log data stored in a database.

Microsoft Access (optional)

WhatsUp Event Analyst can convert event logs into Microsoft Access database tables, so you need Microsoft Access installed if you wish to view these tables directly. However, WhatsUp Event Analyst can still read and operate on event logs stored in Microsoft Access database tables within its own interface.

Microsoft SQL Server 2005/2008/2012 (Workgroup Edition or Later), or Microsoft SQL Server Express 2008 (optional)

WhatsUp Event Analyst can view, report, and filter event log information from certain ODBC server database tables (Microsoft SQL Server). Microsoft SQL Server is the recommended database server platform for LANs generating a great deal of event log activity. It is best to install WhatsUp Event Analyst to a *different* machine than the ODBC database server.

Before You Begin

1 Determine which domain(s) you want WhatsUp Event Analyst to analyze event logs from. If you want to analyze logs from more than one domain, you must choose a primary domain that is trusted by other domains. WhatsUp Event Analyst refers to this primary domain as the default domain. When prompted, enter the default domain you have chosen.

> **Note**: If you are installing WhatsUp Event Analyst to a server or workstation not participating in a domain, please enter its workgroup instead.
>
> **Note**: If you only plan to analyze event log entries stored in text files, Microsoft Access database table(s), or ODBC database table(s), enter the domain or workgroup name of your workstation

2 Make sure you are logged in with local administrator rights on the machine where you are installing the product. In addition, if the product is used to work with active or saved EVT/EVTX files in a domain, make sure you have domain administrator or organizational unit admin rights as well. Fundamentally, your domain account (or primary domain group) needs to be in the local Administrators group of all machines whose logs you will access. Otherwise, you may not be able to work with and convert all types of event log files (e.g. security logs). If you only plan to work with event log entries from Access database tables or ODBC database tables, install the software with local administrator rights, and make sure you have read and indexing rights on the database tables being viewed/reported against.

3 If you do not have an established user account with domain admin or OU admin rights that services can run under in your organization, and you plan to schedule reports against active or saved EVT/EVTX files, create a user account with Active Directory Users and Computers and place it into the Domain Admins or an OU Admins group. Also, make sure that this account has administrator rights (either by itself or via group membership) on the local machine you installed WhatsUp Event Analyst on. To prevent scheduled report interruption, make sure this account's password does not expire. The WhatsUp Event Analyst Service will run under this account, in order to have full rights across the domain when it creates reports against EVT/EVTX log files.

> **Note**: If you are installing WhatsUp Event Analyst to a server or workstation not participating in a domain, or if you will only be running reports against Microsoft Access or ODBC database tables, please enter a local user account that is an Administrator of your workstation (e.g. SERVERNAME\Administrator or Domain\UserWithLocalAdmin).

4 Depending on your network structure, choose the most appropriate computer retrieval option when prompted with the Computer Name Retrieval Dialog.

Note: If you are in a large, flat domain with many computer accounts, it may be best to choose either The browse list option or The following OU option to prevent lengthy timeouts associated with enumerating all computer accounts in the domain

5 If you want WhatsUp Event Analyst to email reports to interested parties after the reports are created by the WhatsUp Event Analyst Service, locate an available SMTP server on your network (we recommend the Microsoft SMTP Service that ships free with Microsoft's Internet Information Server), and adjust its security settings so that the machine(s) running WhatsUp Event Analyst may relay mail through it. Then, from the **Options** menu > **WhatsUp Event Analyst Preferences > Report Emailing** tab, enter the fully-qualified domain name or IP address of this server in the SMTP Server field. When scheduling reports, enter the email addresses of the persons wanting copies of the report in the Email Recipients field, separating each email address with a comma.

If you are installing WhatsUp Event Analyst on Windows XP

1 Open the **Component Services Tool** from **Administrative Tools** (or **Control Panel > Administrative Tools**). On Windows Vista or later, start it directly by locating and opening **windows\System32\comexp.msc**.

2 Expand **Component Services > Computers > My Computer**.

3 Right-click **My Computer**, and then select **Properties**. Click the **Default COM Security** tab.

4 Under **Access Permissions**, explicitly add the **Authenticated Users** identity.

5 Click **Add** to browse for this identity, select it, verify that **Allow** is checked for this user, and then click **OK** to close the dialog.

Note: The security identity Authenticated Users is defined by Microsoft as follows: Includes all users and computers whose identities have been authenticated. Authenticated Users does not include Guest even if the Guest account has a password.

Note: You are free to tighten COM security as you see fit. However, test your settings thoroughly to make sure that the WhatsUp Event Analyst Service can create scheduled reports when no user is logged on, and also verify that other interactive programs function properly after adjusting these access permissions.

6 Under **Launch Permissions**, explicitly add the user account that the WhatsUp Event Analyst Service runs/will run under. Click **Add** to browse for the account, select it, verify that **Allow** is checked for this user, and then click **OK** to close the dialog.

Click **OK** to close the **My Computer Properties** dialog, and then close the Component Services tool. The WhatsUp Event Analyst Service should now be able to generate scheduled reports, even when no interactive user is logged on.

Microsoft Vista, Server 2008, and Windows 7 Requirements and Recommendations

In Microsoft Vista and later operating systems, the default security settings are much stronger than in previous Microsoft operating systems. This is in keeping with Microsoft's focus on reducing the potential surface area for attacks over the network.

In WhatsUp Event Analyst version 10, the software was redesigned with these considerations in mind, using only the bare minimum of network access techniques to read and manage log files from Microsoft Vista systems. As has been the case in the past, if you can remotely view and manage your event logs with the Microsoft Event Viewer, our software should have no issues operating on them.

In WhatsUp Event Analyst version 10, we have added special technology that now allows the software to open and report on EVTX log files from Vista and later operating systems, ***even when installed on a legacy operating system like Windows XP** or **Windows 2003.*** In that scenario, you need to add a few additional exceptions to the Windows Firewall in order for EVTX logs to be processed successfully when WhatsUp Event Analyst is installed on a legacy operating system. You also need to establish a Group Policy to make sure that the Remote Registry Service is running on all of your servers/workstations targeted by WhatsUp Event Analyst.

If you install WhatsUp Event Analyst on a Windows Vista or later operating system, and will be working with EVTX log files, you will need to allow the Remote Event Log Management exception in the Windows Firewall in order for WhatsUp Event Analyst to successfully read and work with logs from Microsoft Vista or later machines. The easiest way to do this is in a domain is to use a Group Policy Object that governs all Vista workstations. On workgroup or standalone machines, you can either manually set the exception under the Windows Firewall Exceptions tab on each computer, or you can create a Local Security Policy template targeting the Windows Firewall with Advanced Security area and apply it to the Local Security Policy on each machine with the **secedit** command line tool.

If you install WhatsUp Event Analyst on a legacy pre-Vista Windows operating system, and will be working with EVTX log files, you need to allow the Remote Event Log Management Exception, the File and Printer Sharing Exception, the Remote Administration Exception, and the Remote Service Management exception in the Windows firewall in order for WhatsUp Event Analyst to successfully read and work with EVTX logs from Microsoft Vista or later machines. You also need to establish a Group Policy that makes sure that the Remote Registry Service starts automatically and continues to run on all servers and workstations targeted by WhatsUp Event Analyst over the network. Please review the aforementioned paragraph for guidance on how to do this.

Other Recommendations

WhatsUp Event Analyst works best in a well-connected LAN environment (e.g., 100 Mbit Ethernet). If you plan to convert event logs into text, Access databases, or ODBC databases, it is best to locate your WhatsUp Event Analyst server near your Primary Domain Controller /

Active Directory Server for the purpose of account lookups. Likewise, if you plan to read and/or filter active computer event logs and event log files, the reading time will be reduced if the software has adequate amounts of bandwidth to the remote server and the PDC. If you plan to use WhatsUp Event Analyst in a WAN environment, it is beneficial to install a copy of WhatsUp Event Analyst locally at each local point to speed up conversion, reading, filtering, and reporting. Use of remote desktop type software (Microsoft Terminal Services, VNC, etc) is useful in such a scenario. Optionally, you can instruct WhatsUp Event Analyst to make a copy of a live log when it is opened and transfer it to the system where WhatsUp Event Analyst is running to minimize total WAN traffic.

Another way to optimize reading, conversion, filtering, and reporting operations inside WhatsUp Event Analyst is to work with event log formats other than active computer and saved EVT/EVTX log files. Event log information stored inside EVT/EVTX files is not completely self-contained. In order to display full record information, message files and account information must be looked up across the network. Therefore, to speed up the reading process, make sure that the WhatsUp Event Analyst workstation is well connected to the primary domain controller (Active Directory Server) for account name lookups, and the actual machine where the EVT/EVTX file came from. If you do not need to perform account lookups, you can turnoff SID to account name resolutions under **Options > WhatsUp Event Analyst Preferences**. In addition, you can change the number of record WhatsUp Event Analyst reads at a time by changing the **Record Window** setting under **Options > WhatsUp Event Analyst Preferences**. Analysis using database tables is always quicker than EVT files, and Ipswitch's WhatsUp Event Archiver automatically collects your event log information into database tables that WhatsUp Event Analyst can read from.

If you plan to run scheduled reports on event logs from many different event log sources, it is beneficial to space out their report schedules. Having WhatsUp Event Analyst attempt to report on 20 different event log sources at the same time can be a severe drain on server resources. Therefore, it is best to space out reporting times and dates. All scheduled reports log a success or failure event in the Application log where WhatsUp Event Analyst is installed. Use the Application Log to check for errors if reports are not being generated properly. If scheduled reports are not running, and no errors are being logged by the WhatsUp Event Analyst Service, make sure that a.) the WhatsUp Event Analyst Service is running, and b.) your COM security settings are set correctly (see the aforementioned section on COM).

You should use filters and indexes to your advantage when working with large database tables full of event log information (inside Access or ODBC). If there are over 50,000 log records in a database table, you should use the Filter button to attach a filter to the data source before opening it. This reduces the number of records in the result set, and also reduces the time it takes to open the table. The same rule of thumb applies when scheduling a report: filters can also greatly reduce the amount of data the report module must work with. To create new filters with limiting criteria (e.g. a computer name, date range), select **Define Basic Filter** or **Define Advanced Filter** from the **Edit** menu. Indexes can also help return records more quickly. When setting up a data source in the Database Table Links Manager dialog, use the **Index Table** button when available to create a default set of indexes on your database table. These indexes help WhatsUp Event Analyst retrieve data more quickly, especially if you are limiting the data to recent dates.

CHAPTER 2

WhatsUp Event Analyst Menu Descriptions

In This Chapter

Using the File Menu

The File menu allows you to view event log sources, modify log settings, and audit policies for individual computers, save and clear active computer logs, and print detail reports on filtered and unfiltered log sources.

File menu options:

Connect To Computer Log. Opens the Connect to Computer Log dialog, so you can connect to an active event log on a remote computer, or make a backup copy of an active log and transport it to the local machine for review. Direct reporting options are also available.

Open Saved EVT/EVTX File. Opens the Open EVT/EVTX Log File dialog, so you can open or report against a previously saved event log file (in native .EVT or .EVTX format).

Open Comma-Delimited Text File. Opens the Open Comma-Delimited Text File dialog, so you can open or report against a comma-delimited text event log file (.TXT, .CSV).

Open Database Table Links. Opens the Select Database Table Link dialog, so you can open or report against an Access or ODBC database table or view that contains event log entries previously stored by WhatsUp Event Archiver, WhatsUp Event Analyst, or WhatsUp Event Alarm.

Recently Opened Logs. Remembers the last 10 event log sources you have opened from any of the above dialoges. If you need to open one of these logs again, click on its menu item to quickly reload it.

View/Manage Event Logs Folder. Opens Windows Explorer and shows the compressed event logs directory (e.g. <WhatsUp Event Analyst Install Directory>\Eventlogs). WhatsUp

Event Analyst places files extracted from zipped EVT/EVTX files here, as well as active log files that have been backed up and transferred locally to the local computer for review. This is similar to a general temporary or working directory for EVT and EVTX files. From here, you can manage and remove unneeded log files.

Manage Database Table Links. Opens the Database Table Links Manager dialog, so you can add, edit, and remove links to database tables and views you wish to use with WhatsUp Event Analyst. Once established, use the links to quickly access the stored data within WhatsUp Event Analyst for review or reporting.

Log Settings. Opens the Log Settings dialog, so you can modify the log settings (e.g. size, retention) for an event log on a particular computer.

Audit Policy. Opens the Audit Policy dialog, so you can establish different audit policies for individual computers and/or domains.

Clear Log. Clears an active event log on a remote or local computer; this erases all event log entries from the log, so if necessary, save the log before clearing it.

Save Log. Allows you to save an active computer event log to an EVT or EVTX file for later use; if you elect to save the log to a disk not on the source machine, WhatsUp Event Analyst first backs up the log to the SystemRoot (e.g. C:\Windows) folder on the source machine and then moves it to your desired location. This is in accordance with the Microsoft Windows 2003 security policy.

Print Log Entries to HTML. Allows you to export the current log view to an HTML document; If the log source is filtered, only filtered events are exported. Otherwise, all events from the given source are exported. This is a quick and easy way to generate detailed reports. After the HTML file is created, you can immediately view it in your default browser.

Using the Edit Menu

The Edit menu allows you to add commonly sought after event log entries to a local database, which you can use as a basis for searching through an event log source. In addition, you can define and categorize event log filters for only displaying certain types of events in a Log View window.

Define Events. Launches the Define Events dialog, where you can add new event log entries.

Find Event. Displays the list of defined events, from which you can select an entry to begin a search in the active Log View window.

Find Next Event. Looks for the next event in the Log View window.

Define Basic Filters. Opens the Define Basic Filters dialog, where you can add and categorize new basic event log filters for future use.

Define Advanced Filters (For Database Sources Only). Opens the Define Advanced Filters dialog, where you can add and categorize new advanced event log filters for future use on database sources.

Apply Filter. Displays the list of defined filters, and then applies a selected filter to the active Log View window.

Remove Filter. If necessary, removes the filter from the active Log View window and redisplays all the event log entries.

Using the View Menu

Refresh. Re-queries a log source to display any new event log entries, if available. You can also use F5 as a keyboard shortcut to perform the same operation.

Stop Action. Aborts the current log viewing, seeking, or printing action, if possible.

Using the Options Menu

The Options menu lets you configure WhatsUp Event Analyst's default operating behaviors and settings.

WhatsUp Event Analyst Preferences (on page 40). Opens a dialog you can use to customize WhatsUp Event Analyst's behaviors to your liking, such as the default domain whose computers' logs you will be analyzing, the number of event log records you wish displayed at any given time, regional date/time settings, and reporting options.

Set Service Account (on page 44) - Opens the Set Service Account dialog, where you can control what user account context the WhatsUp Event Analyst Service runs under.

Start the WhatsUp Event Analyst Service. Starts the WhatsUp Event Analyst service so that scheduled reports can be generated at specified times.

Stop the WhatsUp Event Analyst Service. Stops the WhatsUp Event Analyst service.

Manage Custom Domain to Computer Mappings (on page 46). If your network structure requires it, you can create custom domains in WhatsUp Event Analyst, and map computer names to the custom domains you create. For example, you may need to manage a set of different computers spread out across multiple organizational units, or you may have computers located in different workgroups that share a common administrator account. In both scenarios, you can create a custom domain to bind together unrelated computers into a logical group and then can reference that custom domain when selecting computers for log viewing, report scheduling, etc.

Retrieve Computer Names From. Opens the *Computer Name Retrieval Dialog* (on page 47), which determines how WhatsUp Event Analyst prepares the list of computers in various dialogs throughout the program. Depending on whether you are managing a workgroup, an entire domain, or a single OU inside a domain, choose the most appropriate option.

Manage Custom Logs (on page 30). Opens the Manage Custom Logs dialog, where you can add any additional Windows Custom Event Logs that may exist on your workstations or servers beyond the standard six.

View WhatsUp Event Analyst Log Entries. The WhatsUp Event Analyst Service logs all of the actions it takes when building reports in the local Application Event Log on the computer where it is running. Use this menu option to open the *WhatsUp Event Analyst Log Entries Dialog* (on page 48) which displays all WhatsUp Event Analyst Service entries present in the local Application log. You can filter entries by type (e.g. error, warning, information) as well as export them to an HTML file if necessary.

Using the Export Menu

The Export menu presents several different formats for conversion from any given event log source.

Export To Comma-Delimited Text. Opens the *Export To File* (on page 50) dialog, where you can create a new comma-delimited text file and export log entries to it as comma-delimited records.

Export To HTML. Opens the Export To File dialog, where you can create a new HTML file and export log entries to it as an HTML table.

Export To Access. Opens the *Export To Database* (on page 50) dialog, where you can export event log entries to an existing or new Access database table.

Export To ODBC. Opens the *Export To Database* (on page 51) dialog where you can export event log entries to an existing or new ODBC database table.

Using the Reports Menu

The Reports Menu allows you to run a report on demand (manually), or schedule it with the WhatsUp Event Analyst Service.

Run a Report Now (on page 55) dialog, where you can select a report to run against the opened event log source currently in focus.

Schedule a Report For the Active Log Source (on page 56) dialog, and pre-populates it with information about the active log source you are currently viewing in WhatsUp Event Analyst (e.g. the log type, filename or database being used, filter information, etc). This makes it very easy to schedule a report against the log data you are currently reviewing.

Schedule a Report For Any Log Source (on page 56) dialog, which you can use to schedule report generation at a certain time against any log source available on your network.

Custom Reports Designer (on page 58) dialog, which you can use to create or modify custom report layouts (e.g. organize field sorts and groupings). You can then pair custom report layouts with filtered log data to produce customized reports.

Manage Friendly Event ID Definitions (on page 60) dialog, which allows you to add new or change existing Friendly Event ID definitions. Friendly Event ID definitions are used to add clarity to custom reports, as the friendly definition displays along the Event ID number in each custom report that is generated.

View/Manage Manual Reports Folder. Launches an instance of Windows Explorer, and navigates to the default location where WhatsUp Event Analyst stores reports generated manually (e.g. when an administrator uses the **Run a Report Now** option as mentioned above). From here, administrators can view and/or delete previously created reports.

View/Manage Scheduled Reports Folder. Launches an instance of Windows Explorer, and navigates to the default location where WhatsUp Event Analyst stores reports generated automatically by the WhatsUp Event Analyst Service (e.g. when an administrator uses the **Schedule a Report** options mentioned above). From here, administrators can view and/or delete previously created reports.

Using the Help Menu

The Help menu contains links to the Ipswitch Network Management homepage, the WhatsUp Event Analyst help file, and allows you to register and activate WhatsUp Event Analyst and/or upgrade your total number of computer licenses.

Visit Ipswitch Network Management Online. Attempts to connect to the Ipswitch Network Management home page using your default browser.

Register WhatsUp Event Analyst / Upgrade WhatsUp Event Analyst Licenses. Display the License Manager dialog, which you can use to initially register and activate WhatsUp Event Analyst as well as add more computer licenses to the product.

WhatsUp Event Analyst Help File. Displays the help file you are currently viewing.

WhatsUp Event Analyst Quick Tips. Opens a dialog where you can review frequently asked questions about this program.

About WhatsUp Event Analyst. Displays the current WhatsUp Event Analyst version and splash screen.

CHAPTER 3

Accessing and Viewing Event Log Sources

In This Chapter

Connecting to a Computer Log

Use the Connect To Computer Log dialog to open a local or remote computer's active event log. To open the dialog, click the **File** menu, and then select the **Connect to Computer Log** option.

Connecting to a Computer Log dialog field descriptions:

Domain. Select the domain of the computer with logs you wan to open.

Computer. Select the computer with logs you want to open. To choose how WhatsUp Event Analyst selects the computers displayed here, click the **Options** menu, and then select **Retrieve Computer Names From** to open the *Computer Name Retrieval* (on page 47) dialog.

Log Type. Select the log on the computer you want to open.

Make a Backup Copy Of This Log. In many cases, analysis and reporting of native event log files (e.g. EVT files) is faster when working with a local copy. If this option is checked, WhatsUp Event Analyst automatically attempt to backup the log from the computer in question and automatically copy it to the system running WhatsUp Event Analyst, placing it in the special Eventlogs folder. You can manage and delete files from the Eventlogs folder at any time by clicking the **File** menu, and then selecting **View/Manage Event Logs Folder**.

Note:: If you are attempting to review EVTX logs from a Windows Vista or later operating system when WhatsUp Event Analyst is installed on a legacy operating system (e.g. Windows XP, Windows 2003), the above option must be checked prior to opening the log.

View Earliest/Latest Events First. Choose the order in which you want to view events in the Log View dialog.

Open in Window. Loads the event log entries from the active computer into a Log View dialog.

Build Report. Opens the Report Chooser dialog and sets its focus to the active event log file you selected. You can immediately generate a report manually without having to view the records in WhatsUp Event Analyst.

Cancel. Closes the dialog without retrieving log entries.

Opening a Saved EVT/EVTX File

Use the Open EVT File dialog to select an archived event log (.EVT, .EVTX) file or zipped event log file (.EVT.ZIP, .EVTX.ZIP) from disk. To open the dialog, click the **File** menu, and then select the **Open a Saved EVT/EVTX File** option.

Open EVT/EVTX File dialog field descriptions:

File Name. Type the path to the EVT or EVTX file on disk.

Browse(...). Use this button to browse for an EVT or EVTX file on disk.

Log Type. Select the actual log type of this EVT file (e.g. Security log, System log, etc)

View Earliest/Latest Events First. Choose the order in which you want to view events in the Log View dialog.

Open in Window. Loads the event log entries from the EVT or EVTX file into a Log View dialog.

Load Message Files/Metadata From. In some cases, you may have an EVT or EVTX file that came from a computer on a different network. In order to properly display some of the data from that log, you can instruct WhatsUp Event Analyst to load message files and other related data from a surrogate computer on your network.

Note: If you choose to load message files from a different computer when working with a security log, you should make sure that the surrogate computer being used matches the Windows platform of the machine that generates the EVT/EVTX file. If you have a security event log from an external Windows 2003 server, you should load message files from a local Windows 2003 server, etc.

Build Report. Opens the Report Chooser dialog and sets its focus to the archived EVT or EVTX file and filter you have supplied. You can then immediately generate a report manually without having to view the records first in WhatsUp Event Analyst.

Cancel. Closes this dialog without retrieving log entries.

Opening a Comma-Delimited Text File

Use the Open Comma-Delimited Text File dialog to select and view an archived, comma-delimited event log text file. To open the dialog, click the **File** menu, and then select the **Open Comma-Delimited Text File** option.

WhatsUp Event Analyst reads both Microsoft Event Viewer comma-delimited event log files as well as WhatsUp Event Archiver and WhatsUp Event Analyst comma-delimited event log files.

Open Comma-Delimited Text File dialog field descriptions:

File Name. Type the path to the text file on disk.

Browse(...). Use this button to browse for an existing comma-delimited log file on disk.

Log Type. Select the originating log type of this text file.

View Earliest/Latest Events First. Choose the order in which you want to view events in the Log View dialog.

Open in Window. Loads the event log entries from the text file into the Log View dialog.

Build Report. Activates the Report Chooser dialog and sets its focus to the comma-delimited text file you supplied. You can then immediately generate a report manually without having to view the records in WhatsUp Event Analyst.

Cancel. Closes the dialog without retrieving log entries.

Managing Database Table Links

The Database Table Links Manager dialog allows you to build links to WhatsUp Event Archiver/WhatsUp Event Alarm/WhatsUp Event Analyst-compatible database tables stored in Microsoft Access or Microsoft SQL Server databases.

To open the dialog, click the **File** menu, and then select the **Manage Database Table Links** option.

By creating friendly names for frequently accessed database sources, you can save time when needing to connect to or scheduling reports against one of these data sources.

Database Table Links Manager dialog field descriptions:

Add. Allows you to add a new link to a database and table(s)/view(s).

Edit. Allows you to edit an existing link to a database and table(s)/view(s).

Delete. Deletes the existing link from WhatsUp Event Analyst.

Name. A descriptive name for the database source, such as Security Log Table from SQLServer10 or Application Events from Server Group B.

Database Type. For Access databases, select **an Access Database**. For Microsoft SQL Server databases, select **an ODBC database**.

Select Database. This field should either contain an ODBC connection string or the path to the Access Database (.mdb) file on disk.

Browse(...). Use this button to either browse for an Access database file (.MDB) on disk, or open up the ODBC connection manager.

Select Table(s) and/or View(s). Displays a list of tables and views in the Access/ODBC database. Tables and views each have different icons to distinguish themselves from one another. Choose one or more Ipswitch (WhatsUp Event Archiver or WhatsUp Event Alarm) compatible table(s) or view(s) to continue.

Note: If you are instructing another one of our log management tools (e.g. WhatsUp Event Archiver or WhatsUp Event Alarm) to place log entries into an Access or ODBC database rather frequently (e.g. every few hours or so), you may want to set up a view to that table inside your database. Instructing WhatsUp Event Analyst to work against a view is beneficial because no significant record locking takes place. If record locking happens frequently enough, this can prevent WhatsUp Event Archiver or WhatsUp Event Alarm from placing data into your database table(s) in a timely manner.

The only restriction placed on the creation of WhatsUp Event Analyst-compatible views is that they must return all fields from the table. E.g. the start of the SQL syntax for the view should begin with "SELECT *". Whether you choose to limit the number of records returned with a WHERE clause is up to you.

Index Table. Attempts to apply a default index to the selected table. Indexes are useful in speeding up the amount of time it takes to return data from a database table when a filter is applied.

Save. Saves the database source link for future use.

Cancel. Abandons modifications to the database source link.

Opening Database Table Links

Use the Select Database Table Link dialog to select one or more of Ipswitch's compatible event log data sources (e.g. WhatsUp Event Archiver/WhatsUp Event Alarm database table(s) or view(s)) from an Access or ODBC database source. Once selected, you can view the contents of filtered data inside WhatsUp Event Analyst, or directly build a report against that data.

To open the dialog, click the **File** menu, and then select the **Open Database Table Links** option.

If you open a database table or view containing more than 50,000 records, it may take a while for the Log View window to display the results. This is because the database server must build the cursor (collection of all the entries) of records, and then transmit it over the network. You can streamline performance and minimize opening delays by choosing to apply a filter before opening the table. In order to do this, click the **Filters** button, select the filter you want, and then open the data source. Use the *Define Filters* (on page 36) dialog to add your own new filters based on dates, Event IDs, users, and other criteria to the local WhatsUp Event Analyst database. Also, you can quickly filter a large group of event log records by bounding them by date. Use the **Enable Date Filter** button for this purpose. Finally, if you have not already, remember to apply a default set of indexes to your WhatsUp Event Archiver/WhatsUp Event Alarm database tables with the **Index Table** button in the *Database Table Links Manager* (on page 27) dialog. Indexes speed retrieval of data when filters revolve around certain key fields, such as Date/Time and Event ID.

Select Database Table Link dialog field descriptions:

Database Table Link. Choose a database table link containing event log data you want to work with. If this is your first time using WhatsUp Event Analyst, click the **Create a New Database Link** button to build a link to an Access or ODBC database table.

Create a New Database Link. Clicking this button opens the *Database Table Links Manager* (on page 27) dialog, which is used to maintain links to frequently used event log database tables. Such links typically consist of one or more tables or views in an Access or ODBC database.

Log Type. Select the log type whose entries you want to view from the database source. Individual database tables or views can contain data from more than one log type, so it is necessary to specify this explicitly.

Filter. Lists the filter to be applied to the log source when it is opened, if defined.

Filters. Use this button to attach (or remove) a filter from a log source before it is opened.

Enable Date Filter. Clicking this button allows you to bound a log source with a starting and ending date, subsequently reducing the number of records returned from the database. Click it again to remove the date filter.

Note: You can only use the Date Filter option in conjunction with another filter if the other filter is a basic filter. Advanced filters, by definition, can contain advanced date querying information defined within them; therefore, if an advanced filter is selected, the Enable Date Filter button is disabled.

Begin Date. Enter the earliest date returned by WhatsUp Event Analyst for records in your database.

Note: If a Basic Defined Filter has been selected which also has a starting date defined, this date overrides it.

End Date. Enter the latest date returned by WhatsUp Event Analyst for records in your database.

Note: If a Basic Defined Filter has been selected which also has a ending date defined, this date overrides it.

View Earliest/Latest Events First. Choose the order in which you want to view events in the Log View dialog.

Open In Window. Loads the event log entries from the database table into a Log View dialog.

Build Report. Activates the *Report Chooser* (on page 55) dialog and sets its focus to the database link and filter you supplied. You can then immediately generate a report manually without having to view the records in WhatsUp Event Analyst.

Cancel. Closes the dialog without retrieving log entries.

Opening Recently Opened Logs

You can quickly re-open recently viewed logs by clicking the **File** menu, and then selecting the **Recently Opened Logs** option. A sub-menu opens displaying the names of recently opened log; select the recently opened log that you want to re-open.

Organization - Managing Custom Event Logs

Traditionally, there are six standard Windows event logs present on Microsoft Windows server and workstation operating systems; the Application, System, and Security logs display on all Windows operating systems, and the DNS Server, Directory Service, and File Replication Service logs are found on server operating systems.

Various third-party applications now create their own custom Windows event logs for error tracking and reporting. WhatsUp Event Analyst provides the option of defining custom event logs, so they can be collected alongside standard logs.

To define a custom event log for use within WhatsUp Event Analyst, click **Organize**, and then, in **Common Settings**, click **Manage Custom Logs**. You can then browse to various computers to view the custom Windows event logs present on any given system. If you want to make a custom event log available for use by WhatsUp Event Analyst, select it from the list, and then click **New > Add Custom Log**. Similarly, if you no longer want to see a particular custom event log as available throughout WhatsUp Event Analyst, select it from the **Custom Event Logs Defined** list, and then click the **Delete** button.

In some cases, you may not be able to enumerate custom logs on a remote machine (e.g. the Remote Registry Service may be disabled, for instance), so you can also choose to add a custom log manually by clicking **New > Add Custom Log Manually**. In the resulting dialog, specify both the **Custom Log Display Name** (e.g. the name of the log as shown in the Microsoft Event Viewer) and the **Custom Log Internal Name** (e.g. the internal registry name for the log). In pre-Microsoft Vista operating systems, such as Windows XP and Windows 2003, the custom log internal name is always the same as the display name. In Microsoft Vista and later operating systems, the internal name may be different, and you need to determine the internal name by finding the log's subkey under the HKLM\System\CurrentControlSet\Services\EventLog section of that computer's registry.

Viewing and Managing the Event Logs Folder

To view your event logs folder in Microsoft (MS) Windows Explorer, click the **File** menu, and then click **View/Manage Event Logs Folder**. MS Windows Explorer opens and makes the Event Logs folder active. From here, you can move and manage your event logs folder structure.

Setting Up Databases and Making Connections

In order to prepare a new ODBC-compliant database to receive logs from WhatsUp Event Analyst, create (or have your Database Administrator create) a new database (or schema/tablespace) on your database server with default settings. Ipswitch recommends Microsoft SQL Server 2005/2008/2012 as these platforms have been tested and work well with WhatsUp Event Analyst.

Then, if necessary, create a new database login that has full read and write permissions to this database. In Microsoft SQL Server, it is recommended that the username and password be a standard security login as opposed to an Windows account-based integrated login. If you do opt to use integrated Windows security, make sure that the WhatsUp Event Analyst Service account has full read permissions to the database for reporting, and if necessary, full write permissions to import individual log files into a database table.

For more information on creating a Microsoft SQL Server database, please refer to the Creating a WhatsUp Logs Database on Microsoft SQL Server help file.

Once the database and login is created, use the ODBC connection manager to create a connection string to that database. The most important thing to remember is that this connection should be set up as a File DSN instead of a System DSN.

After the File DSN is created, you do not have to change these ODBC settings again, unless your database server or login is modified. All you need to do after creating the File DSN is to link to various tables inside the database pointed to by the File DSN. This is accomplished by using the Database Table Links Manager dialog.

Here are sample screen shot walkthroughs of how to set up a File DSN for a Microsoft SQL Server database connection:

Creating an ODBC file data source for Microsoft SQL Server

1 Open the Data Sources (ODBC) Applet under the Control Panel or Administrative Tools. Select the **File Data Source** tab, and then click the **New** button.

2 Select the SQL Server driver.

3 Type a name for the Data Source you are creating.

4 Click **Finish**.

5 Select the SQL Server you want to connect to, or type in the IP address of the server.

6 Choose an authentication method. SQL Server authentication is recommended.

7 Change the default database to the database your DBA created to store your event logs.

8 Leave the settings on their defaults.

9 Test the data source, and then click **OK** if the test succeeds.

10 Now, whenever specifying an ODBC data source inside WhatsUp Event Analyst, select the file data source you just created.

Managing Log Settings

WhatsUp Event Analyst allows the administrator to adjust log retention and log size settings on individual servers and workstations. This is useful when organizations do not use Group Policy to control log retention and size settings, or are managing computers in one or more workgroups instead.

Note: If you are running a Microsoft Windows 2003 or 2008 domain and have Group Policies enabled, you should use the Group Policy Editor to manage your log size and retention settings for related groups of computers.

Note: Adjusting log settings on Microsoft Vista computers is not yet supported. In the interim, use the Local Security Policy tool and/or Group Policy Editor to adjust these settings on Microsoft Vista computers.

Use the Log Settings dialog to set individual event log file sizes and retention properties.

To open the dialog, click the **File** menu, and then select the **Log Settings** option.

Log Settings dialog field descriptions:

Log Type. Use this list to choose an individual event log from the computer to modify settings on.

File Size. Type a new size into the text box, or use the up/down arrows to adjust the file size. Due to the architecture of the Microsoft Event Log subsystem, your size entry is rounded to the nearest 64 kilobyte increment.

Event Log Retention. When an event log becomes full, there are three actions a Microsoft Windows operating system can take. One is to start overwriting all events, beginning with the oldest and working forward. This is a relatively low security setting, because once events are overwritten, they cannot be recovered. A slightly more secure setting is to only allow events to be overwritten if they are a certain number of days old or older. The optimal setting from a security standpoint is to prevent the event log system from overwriting any events.

Setting the Audit Policy

WhatsUp Event Analyst allows the administrator to adjust audit policies on an individual machine when viewing that machine's active computer event log (EVT/EVTX file). To adjust the audit policy on a member server or workstation:

1. Open an active event log on the desired computer by selecting **File > Connect To Computer Log**, and choosing a domain, computer name, and log type.
2. When the active event log is open, select **File > Audit Policy**.

The Audit Policy dialog allows you to change what security events you want to audit on an individual machine (such as a standalone workstation or server), or across an entire domain (in the case of a Primary Domain Controller or Active Directory Server). If you choose to display audit policies on a domain controller, the focus automatically shifts to that domain.

Note: If you are running a Microsoft Windows 2003 or 2008 domain and have Group Policies enabled, use the Group Policy Editor to manage your audit policy settings for related groups of computers.

Audit (Security Event Logging) on \\ComputerName is. Setting this option to Enabled turns on security event logging on the specified Windows computer or domain. Switching to Disabled turns off all auditing, regardless of the way each audit category is configured.

Audit Categories

For each audit category, you can choose to record successful events (by checking success), failed events (by checking failure), both (by checking both), or neither (by checking none).

(The following descriptions of each category were taken from the Microsoft Platform SDK, June 17, 1999).

System Events. Audit attempts to shutdown or restart the computer. Also, audit events that affect system security or the security log.

Logon Events. Audit attempts to log on to or log off from the system. Also, attempts to make a network connection. Does not audit centralized Active Directory logons; see Account Logons below.

Object Access. Audit attempts to access securable objects, such as files.

Privilege Use. Audit attempts to use Windows NT privileges.

Process Tracking. Audit events such as program activation, some forms of handle duplication, indirect access to an object, and process exit.

Policy Change. Audit attempts to change policy object rules.

Account Management. Audit attempts to create, delete, or change user or group accounts. Also, audit password changes.

Directory Service Access (Windows XP/2003/Vista/2008/2012/Win 7 only). Audit attempts to access objects inside Active Directory.

Account Logons (Windows XP/2003/Vista/2008/2012/Win 7 only). Audit logon attempts by privileged accounts that log on to the domain controller. These audit events are generated when the Kerberos Key Distribution Center logs on to the domain controller and by MSV1_0 for Windows NT 4.0 - style logons.

Saving and Clearing Active Event Logs

Should you need to save a copy of an active event log (EVT/EVTX) file to disk from a server or workstation in your domain, complete the following steps:

1. Open the event log file in WhatsUp Event Analyst by clicking **File > Connect to Computer Log** option.
2. Save the event log file by clicking **File > Save Log** option.

You can also clear all events from an event log:

1. Open the event log file in WhatsUp Event Analyst by clicking **File > Connect to Computer Log** option.
2. Select **File > Clear Log** option.

To perform these operations successfully, you need administrator (and in some cases, Domain Admin) rights on the member servers or workstations affected.

CHAPTER 4

Events and Filters

In This Chapter

Defining Events

Use the Define Events dialog to add new frequently searched for events to the local WhatsUp Event Analyst database.

To open the dialog, click the **Edit** menu, and then select **Define Events**.

After a new event is defined, you can search for it using the **Find Event** option from the **Edit** menu.

Define Events dialog field descriptions:

Events. Displays a list of currently defined events, so you can edit or delete existing event definitions.

Add. Clears the Event Characteristics fields so that you can complete and then save a new event definition to the database.

Edit. Unlocks the Event Characteristics fields so you can modify an existing event definition.

Delete. Deletes the currently selected event from the database.

Save. Stores the newly defined event (see Add button above) in the WhatsUp Event Analyst database.

Name. A unique name used to identify a particular event definition in the database.

Comment. A detailed description about an event definition's purpose.

Source. Identifies the application, hardware device, or OS subsystem which writes a given event to the event log. This field is used in event searching.

Event ID. Identifies the source-specific identifier assigned to a particular event to the event log. This field is used in event searching.

Log. Identifies the event log where this event is found. This field is used in event searching.

Close. Closes the dialog.

Event Research Window

The Event Research Window allows a WhatsUp Event Analyst user to find out more information about the currently selected event they are viewing in the *Log View* (on page 48) dialog. Once loaded, this window connects to the Ipswitch Event Logs Resource site, http://www.eventlogs.com, and submits information about the selected event to that site. The website in turn offers links on where to find out more information about that particular event, as well as recommending specific WhatsUp Event Analyst reports that can track that event's activity.

Note: The only information about the event submitted to the website includes the Type of Event (e.g. Error, Warning), Source name, and Event ID fields. No computer or domain-specific information, such as the computer name, user account name, or information inside the Description field is transmitted to the website.

Back. Goes back one page in the web page sequence.

Forward. Goes forward one page in the web page sequence.

Close. Closes the Event Research Window.

Defining Basic Filters

Basic filters allow the administrator to limit the amount of event log entries returned by specifying specific values that must be present in an event log record. For example, an administrator could create a basic filter for events that occur when Norton Antivirus detects a virus, by entering "Norton AntiVirus" in the Source field, entering "5" in the Event ID field, and checking "Error" for the type of event.

As a convenience for administrators, WhatsUp Event Analyst ships with many predefined basic filters, many of which relate to security log events.

Basic filters can be applied to any event log source, including EVT files, text files, and database tables.

To create a basic filter, click the **Edit** menu, and then select the **Define Basic Filters** option.

Filter Information

Add, Edit, and Delete Event Filters. This tree view control allows you to drill down and search for filters by operating system, log type, and category. Expand any item by double-clicking the item.

Name. Enter a name for the basic filter.

Comment. When a filter is selected, the comment field displays a detailed description about its purpose.

Add. Sets up the dialog to receive a new filter definition from the information you provide.

Edit. Loads the filter definition of the selected filter, and allows you to modify its fields.

Delete. Deletes the selected filter or category. A category can only be deleted if it has no child filters.

Close. Closes the dialog.

Single Filter Add/Edit View

Only fill out fields which you intend to filter upon. Leave blank all fields which should be ignored.

Filter By Date. If you want to define a filter with a specific date range, choose **Yes** and configure the **Beginning Date** and **Ending Date** appropriately. Otherwise, choose **No**.

Source. Enter the registered application, hardware, or OS subsystem name whose events you want to filter.

Category. Limits events by task or category.

User. Limits events by user account.

Computer. Limits events by computer.

Event ID. Limits events by source-specific event identifying number.

Description. If you want to search for a specific sub-string in the event description, select **Contains** and type the phrase to search for. Otherwise, if you want to match the complete string, choose **Match Description Exactly**.

Type. To filter by type, check only those types which you want to include in the filter definition. If you do not want to filter by type, leave all check boxes blank.

Save. Saves/adds your filter definition to the local WhatsUp Event Analyst database.

Abandon.Aborts the current operation without adding/updating the filter in the local database.

Defining Advanced Filters

The Define Advanced Filters page allows you to add, edit, clone, and delete advanced filters from WhatsUp Event Analyst's database. To open the page, click **Organize > settings > Analyst Settings > Define Advanced Filters**.

Define Advanced Filters page button descriptions:

Add. Opens the Advanced Filter Builder page, allowing you to create a new advanced filter.

Edit. Opens the Advanced Filter Builder page, allowing you to edit an existing advanced filter.

Clone. Copies the settings out of the currently selected advanced filter, and then opens the Advanced Filter Builder page, where you can adjust those settings and save the new filter.

Delete. Deletes the selected advanced filter.

Exporting Filters

Use the Export Filters dialog to transfer sets of filters from one WhatsUp Event Analyst installation to another. After you export filters to a file, you can always import them from the Import Filters dialog.

Export Filters dialog field descriptions:

- **File to Export Filters Into**. Click the Browse (...) button to select a file that will receive the exported filters. Navigate to the directory where you want to save the exported file, and type in a new file name. WhatsUp Event Analyst creates the file and exports the filters when you click **OK**.
- To prepare a filter for export, drag it from the left side (Available Filters column) of the dialog to the right side (Filters For Export column). Click the **Add** button to move selected filters from the left side to the right side.
- To not export a filter, select it in the right side list, and then click **Remove Filter(s)**.
- **OK**. Exports all of the items in the Filters to Export tree to the file you selected.
- **Cancel**. Closes the dialog without exporting your filters.

Importing Filters

Use the Import Filters dialog to import filters exported by another WhatsUp Event Analyst installation into the local WhatsUp Event Analyst system. This can be very useful if you need to set up a uniform set of filters across multiple WhatsUp Event Analyst installations. If you want to export filters to a file for use on another system, you may do so from the Export Filters dialog.

Import Filters field and button descriptions:

- **Import Filters from File**. Click the Browse (...) button to choose a file containing exported filters from a different WhatsUp Event Analyst installation. After you select this file, the filters housed in that file are displayed in the Filters to Import listing.
- **View**. Displays more detailed information about the filters you have selected in the Filters to Import listing.
- **Remove**. Removes the filters out of the Filters to Import listing. Deleted filters are not imported when the Import button is selected.
- **Import**. Attempts to import the listed alarms into WhatsUp Event Alarm's main database.
- **Cancel**. Closes the dialog without importing your alarms and alarm groups.
- **OK**. Returns the Import Filters dialog back to the main filter listing view.

CHAPTER 5

Settings, Preferences, and Other Options

In This Chapter

Setting Preferences

The Preferences dialog allows you to set the default domain WhatsUp Event Analyst uses when listing computers, the maximum number of event log entries displayed per fetch/seek, regional date/time settings, email settings for reports, and chart settings for reports.

To open the dialog, click the **Options** menu, and then select the **WhatsUp Event Analyst Preferences** option.

General Tab

Default Domain. The domain entered here determines which domains WhatsUp Event Analyst uses to display computers for event log selection. If you have a multiple domain model with several trusting domains and a master domain, this domain should be the master domain so that all other domains are selectable. It also can be the the name of the domain hosting the OU that you manage, or the name of the workgroup containing servers and workstations that you manage.

Record Window. To improve speed, performance, and memory consumption, WhatsUp Event Analyst does not display the entire contents of an event log source in the Log View window all at once. Instead, it breaks up the entire log into sections and only displays the active section in the Log View dialog. By using the Record Window setting, you can control how large you want this section of log entries to be, in terms of contiguous log entries. The larger the window setting, the longer it takes WhatsUp Event Analyst to load those entries, but you are able to work with and sort more entries at a single time.

Default Chronological Order For Viewing Log Entries. This setting governs the default date sorting order for any log sources that WhatsUp Event Analyst opens. When installed, this setting is initially set to show the latest log entries, so that WhatsUp Event Analyst shows the most recent events first.

Resolve SID to Account Names When Reading Logs. If you do not need explicit user account name information when viewing event log entries, you can uncheck this setting. Doing so substantially reduces the time it takes to read, filter, export, and report on active or saved EVT log files. When unchecked, SID numbers are displayed in lieu of actual account names.

Note: This setting only applies to active computer logs and backup EVT files.

Disable Internal Web Browser When Researching Events. By default, WhatsUp Event Analyst uses an internal instance of Microsoft Internet Explorer in the Event Research Window when researching events online at eventlogs.com. If for any reason the internal web browser does not initialize, or if your default browser is something other than Microsoft Internet Explorer, you may check this option to have WhatsUp Event Analyst use your own web browser to research these events.

Place Filter Name in Report Filenames When a Filter Is Used. To better distinguish between reports of the same type, you can instruct WhatsUp Event Analyst to place the name of the filter applied to the log source when the report is created. The filter name then appears in square brackets (e.g. [FilterName]) after the name of the report in the filename of the generated HTML/CSV files.

Ping Computers Before Connecting. If this setting is checked, WhatsUp Event Analyst attempts to ping any computers to see if they are currently running before trying to open live or active event logs on those computers. This can prevent lengthy network timeouts from happening if you attempt to connect to a computer that is not currently running.

Note: By default, Microsoft Vista workstations have ICMP responses disabled via their firewall settings. Therefore, if you want to use this setting with Vista workstations, set a Windows Firewall group policy to allow ICMP responses.

Timeout in Milliseconds. If you have enabled the Ping/ICMP test feature mentioned above, use this setting to determine how many milliseconds must pass without an ICMP response from a target system to consider it a non-response. For slower networks, or if you are connecting to computers across a WAN, it may be necessary to increase this setting.

Regional/Locale Tab

Date Format Used for Display and Data Conversion. This option controls how WhatsUp Event Archiver constructs dates before displaying them in the Log View window or inserting them into either a text file or an ODBC database. The default setting is for WhatsUp Event Analyst to use the Regional System Settings which are specified in the Regional Settings section of the Control Panel. For example, U.S. dates are formatted mm/dd/yy, but European dates are often formatted dd/mm/yy. Alternatively, you can set WhatsUp Event Analyst to use the U.S. format when performing these conversions. The settings you choose affect how dates are output to files and input into ODBC databases. Therefore, you should consult the *International Issues* (on page 10) section of this help file to determine an appropriate strategy.

Report Charting Tab

Add Charts to WhatsUp Event Analyst Reports That Support Them. Some reports in WhatsUp Event Analyst support charts at the beginning of the report. Charting can be useful to pinpoint problem areas before reviewing the rest of the data in the report. If this global option is disabled, reports do not include charts when they are generated.

NOTES ON INCLUDING CHARTS IN REPORTS:

Some versions of Internet Explorer may display a blocked active content message when loading an WhatsUp Event Analyst report containing chart data. This is because our reports use client-side scripting to produce charting data. To show the chart, click the Information bar, and select Allow Blocked Content.

Also, some anti-spam and anti-virus software may block WhatsUp Event Analyst reports containing charts at the email server or at the email client. Again, this is due to the presence of client-side scripting (e.g. <SCRIPT> tags) used to display the charts. Add exceptions as needed to your email servers and/or email recipients so that WhatsUp Event Analyst reports can be relayed through your mail system.

Report Emailing Tab

SMTP Server. If you plan on having WhatsUp Event Analyst email scheduled reports to select individuals after they are created, enter in the fully-qualified domain name (e.g. mailserver.acme.com) or IP address (e.g. 10.34.23.1) of the mail server in this field. Make sure you setup your SMTP server to allow relay from the machine(s) running WhatsUp Event Analyst.

Sender Address. By default, WhatsUp Event Analyst sends emailed reports from EventAnalystService@donotreply.eventanalyst.com. If security settings mandate that you use an address with your domain name in order to relay messages, you may enter in a different address here as appropriate.

Custom Report Subject Line. If you are creating many reports of the same type that use different servers as their log source, or use different filters to control the data sent to each report, you may want to differentiate between reports in the subject line of the email containing them. To do so, create a custom report subject line template using the following escape sequences:

%1 represents the Report Name

%2 represents the Report Source

%3 represents the Filter Name

%4 represents the Log Type

For instance, setting a custom subject line of "%1 from %2, Filter: %3" might appear like so when an email arrives with a User Account Management report attached:

User Account Management from MYCOMPUTER, Filter: Special Admins

Send link to report (via share) instead of attachment. When this option is checked, WhatsUp Event Analyst creates a shared folder on the local machine that maps to the <WhatsUp Event Analyst Installation Directory>\Reports\Scheduled subfolder called EAREPORTS$. Then, when scheduled reports are created, if an email address is supplied, WhatsUp Event Analyst sends an email with links to the reports via the EAREPORTS$ share like so:

\\LOCALMACHINE\EAREPORTS$\Event_Analyst_Report…htm

\\LOCALMACHINE\EAREPORTS$\Event_Analyst_Report…csv

Also, you can supply a different UNC share folder path to create the reports in when creating a scheduled report. If you do so, the WhatsUp Event Analyst Service sends links to that share via email after the reports are created.

Zip compress scheduled reports before emailing them. If this option is enabled, WhatsUp Event Analyst sends scheduled reports as zipped attachments, as opposed to HTML attachments. This often can be useful when your reports are large or your email security settings block HTML files.

Delete zipped reports from disk after emailing them. When this option is selected, the zip files created for emailing purposes Are deleted from disk after the email is sent to the intended recipient.

Microsoft Vista and Server 2008/2012 Settings

Change Information Events to Success Audits and Failure Audits as Appropriate. When checked, WhatsUp Event Analyst changes the Level field in a security EVTX log file from "Information" to "Success Audit" or "Failure Audit" when displaying or converting log entries. This feature is useful when analyzing Microsoft Vista and/or Microsoft Windows Server 2008/2012 security events alongside events from older operating systems in a central database.

Place User Information From the Description Field Into the User Field as Appropriate. Microsoft Vista does not record information about the user performing the action or affected by the action in the User field or the Security log. This option makes WhatsUp Event Analyst automatically extract the most appropriate user from the Description field of each record and place it in the User field when viewing or converting EVTX security log files

Append Keyword and Opcode Fields to the Category Field. To maintain a common number of fields between EVT and EVTX files that are output into text files and database tables, WhatsUp Event Analyst can append the Keyword and Opcode fields to the Task/Category field in an EVTX log record when displaying it or converting it into a new format. The consolidated Task/Category field also contains the Keyword and Opcode fields, appearing like so:

Task/Category:Keyword:Opcode

Global Settings - Setting the Service Account

The Service Account tab configures the WhatsUp Log Management Services to run under a specific user account.

To open the tab, click the **Organization > settings > Global Settings**, and then select the **Service Account** tab.

If WhatsUp Log Management is installed on a computer participating in a domain, and if you are scheduling reports against EVT/EVTX files as opposed to database sources, this account must have domain admin rights, or at minimum, a domain user account with local administrative rights on ALL member servers and workstations being accessed (e.g. an OU Admin account), since it is responsible for reading event logs on domain computers across the network. If you are running WhatsUp Log Management on 1.) a computer not participating in a domain, 2.) are simply reporting against database tables containing log data collected by WhatsUp Event Archiver or WhatsUp Event Alarm, or 3.) are monitoring several machines in a workgroup with a common administrative account and password, select a local account on that same machine which is a member of the local Administrators group.

Setting Up the WhatsUp Event Analyst Service with the Service Account dialog:

I want to choose a domain account from a domain. WhatsUp Event Analyst attempts to populate the Account Name listing with all of the user accounts present in the primary domain where you are running WhatsUp Event Analyst.

I want to choose a local account from this computer. WhatsUp Event Analyst attempts to populate the Account Name listing with all of the user accounts present on the computer where WhatsUp Event Analyst is installed. This option is disabled if WhatsUp Event Analyst is running on a domain controller/active directory server.

Account Name. In this field, choose the name of the user account you want the WhatsUp Event Analyst service to run under. If for any reason WhatsUp Event Analyst cannot automatically populate this list with account names, you can type in an account name. Ensure that the account name is in a fully-qualified format (e.g. DOMAINNAME\AccountName). For example, if you create an account named EAService in the IPSWITCH domain, you would type in IPSWITCH\EAService.

Again, ensure that this user account is in the local Administrators group on each member server/workstation in the domain, if analyzing logs from multiple computers in a domain(s). The easiest way to do this is to make sure it is a member of the Domain Admins group, or an OU Admins group that you have created for a specific OU.

Alternatively, if you are only planning to analyze logs from the local computer, or are planning to analyze logs from other workgroup machines that have a common administrator account, make the service account a local administrator. The WhatsUp Event Analyst Service will not run properly under a LocalSystem context.

Make sure you select an account that is not subject to routine password expiration. If the WhatsUp Event Analyst Service account password expires, the service stops working and archiving jobs do not be completed.

If you are only analyzing and reporting on log data held in a central database, administrator rights across different systems on the network are not needed. You may choose a domain account that is a local Administrator on the WhatsUp Event Analyst system, and that has appropriate rights assigned to the central database

Password. Type in the password of the account you listed in the Account Name field.

Confirm Password. Retype the password for verification.

OK. WhatsUp Event Analyst reconfigures the WhatsUp Event Analyst Service to run under the account you specified. In addition, it adds the Log on as a service and Act as part of the operating system user rights to the account at the local and domain level to ensure proper operation.

Cancel. Aborts the account reconfiguration and leaves the current WhatsUp Event Analyst Service account unchanged.

Setting Up the WhatsUp Event Analyst Service Account Manually

If for any reason you cannot set the WhatsUp Event Analyst Service account from within the Service Account dialog, you can perform this process manually by accessing **Control Panel > Services Applet** (on NT 4.0 systems) or **Control Panel > Administrative Tools > Services** (on 2000/XP/2003/Vista/2008/Win 7 systems).

Before assigning your service account to the WhatsUp Event Analyst Service, verify the following:

1 That the service account is a local administrator (e.g. in the local Administrators group) on every member server and workstation you plan on accessing (note that this is not necessary if you are only working with log data from a central database). The easiest way to accomplish this is to make it a member of the Domain Admins group, or an OU Admin group for a given organizational unit. If you plan to analyze logs directly from domain controllers, only Domain Admins can perform this action.

2 That the service account holds the following user rights (either explicitly or through group membership). You may need to adjust domain-wide or ou-wide group policies to accomplish this.

- Log on as a service
- Act as part of the operating system
- Manage auditing and security log

3 That the service account's password does not expire, due to account policies in your domain.

After you verify these aspects of your service account, assign it to the WhatsUp Event Analyst Service in the Services listing on the local machine. Also, set the WhatsUp Event Analyst Service startup type to Automatic, so it will load when the machine first starts up.

Managing Custom Domain to Computer Mappings

As networks grow and merge, domain and workgroup structures expand in size and complexity. In many cases, event logs must be viewed and reported against from multiple computers that reside in different domains, workgroups, or organizational units. WhatsUp Event Analyst helps resolve this potential problem by allowing network administrators to create custom domains: logical groups of related computers.

To manage custom domains, click the **Options** menu, and then select the **Manage Custom Domain to Computer Mappings** option.

For example, delegation of administration may require you to manage specific servers in three different organizational units of a larger domain. Or, in another scenario, you may have to report on logs from servers and workstations that reside in different workgroups. Using WhatsUp Event Analyst, you can map these individual computer names to a custom domain. Then, you can easily reference that custom domain to scheduled reports against all of these computers with WhatsUp Event Analyst's report scheduler.

Examples of Computer to Custom Domain Mappings:

Computer Name	**Custom Domain Name**
COMPUTER1	MYDOMAIN1
COMPUTER2	MYDOMAIN1
COMPUTER3	MYDOMAIN2
COMPUTER4	MYDOMAIN2

If the following computer and custom domain mappings were created as above, WhatsUp Event Analyst would display two additional domains in any dialog that allowed you to select computer names, specifically CUSTOM: MYDOMAIN1 and CUSTOM: MYDOMAIN2. When you changed focus to one of the custom domains, WhatsUp Event Analyst would show all computers in that custom domain.

In order to report against all types of logs successfully from computers in different domains/workgroups, the WhatsUp Event Analyst Service must run under an account whose user name and password is a.) common to all machines in the custom domain whose logs are collected, and b.) that has administrative rights on those systems.

Adding Computer Names or IP Addresses of Computers To a Custom Domain

Computer / IP Address. Type the name of the computer or its IP address in this field.

Custom Domain Name. Type the name of the custom domain you want associated with this computer or IP address.

Create Mapping. When you click this button, the computer name entered above is associated with the custom domain, and appears in the list below.

Removing Computer Names or IP Addresses of Computers From a Custom Domain

Remove Computer(s). Removes all the selected computers in the list above, effectively disassociating them from the custom domain.

OK. Saves computer to custom domain mappings.

Cancel. Cancels the operation without saving the changes.

Retrieving Computer Names

When attempting to open an active computer event log, WhatsUp Event Analyst presents you with a list of computers to choose from. You can control how WhatsUp Event Analyst prepares this list of computers in certain dialogs by setting the appropriate option in the Computer Name Retrieval dialog.

To open the dialog, click the **Options** menu, and then select the **Retrieve Computer Names From** option.

Computer Name Retrieval dialog options:

The Browse List. Choose this option if you are using WhatsUp Event Analyst to work with logs in a workgroup, not a domain. WhatsUp Event Analyst uses the master browser in the workgroup to list active computers currently online in the workgroup.

The AD Server / Domain Controller. Choose this option if you are using WhatsUp Event Analyst to analyze logs from a domain or multiple domains. When selected, WhatsUp Event Analyst always enumerates all computer accounts directly from the domain controller / Active Directory server. This can take time on very large domains.

The Following OU in Active Directory. If you are only working with logs on servers in a particular organizational unit in your Active Directory, select this option. Once selected, use the **...** button to select the Organizational Unit from which you want to retrieve computer accounts.

Managing Log Settings

WhatsUp Event Analyst allows the administrator to adjust log retention and log size settings on individual servers and workstations. This is useful when organizations do not use Group Policy to control log retention and size settings, or are managing computers in one or more workgroups instead.

Note: If you are running a Microsoft Windows 2003 or 2008 domain and have Group Policies enabled, you should use the Group Policy Editor to manage your log size and retention settings for related groups of computers.

Note: Adjusting log settings on Microsoft Vista computers is not yet supported. In the interim, use the Local Security Policy tool and/or Group Policy Editor to adjust these settings on Microsoft Vista computers.

Use the Log Settings dialog to set individual event log file sizes and retention properties.

To open the dialog, click the **File** menu, and then select the **Log Settings** option.

Log Settings dialog field descriptions:

Log Type. Use this list to choose an individual event log from the computer to modify settings on.

File Size. Type a new size into the text box, or use the up/down arrows to adjust the file size. Due to the architecture of the Microsoft Event Log subsystem, your size entry is rounded to the nearest 64 kilobyte increment.

Event Log Retention. When an event log becomes full, there are three actions a Microsoft Windows operating system can take. One is to start overwriting all events, beginning with the oldest and working forward. This is a relatively low security setting, because once events are overwritten, they cannot be recovered. A slightly more secure setting is to only allow events to be overwritten if they are a certain number of days old or older. The optimal setting from a security standpoint is to prevent the event log system from overwriting any events.

Viewing Log Entries

During the process of creating scheduled reports, WhatsUp Event Analyst logs all successful and failed operations to the local Windows Application Event Log. As a convenience to the administrator, WhatsUp Event Analyst provides a viewer for these events, where administrators can filter out certain types of activity (e.g. errors, warnings), as well as export diagnostic information to an HTML file.

When launched, the WhatsUp Event Analyst Log Entries dialog loads all WhatsUp Event Analyst Service events from the Windows event log. You can filter out certain types of activity by un-checking **Show Error Events**, **Show Warning Events**, and **Show Information Events**.

To copy the highlighted event to the Windows clipboard, click **Copy to Clipboard**.

To refresh all WhatsUp Event Analyst Service log entries from the local Application event log, click **Refresh Log Entries**.

To export all displayed log entries to an HTML file for further review or to send to Ipswitch Support, click **Export to HTML**.

Note: Only WhatsUp Event Analyst Service events currently present in the active Application Event Log are displayed. Older events may already be archived into saved EVT/EVTX files, and if so, you must load those older files in the Microsoft Event Viewer to view their contents.

CHAPTER 6

Exporting

In This Chapter

Exporting to Comma-Delimited Text

You can export WhatsUp Event Analyst log source information to either an HTML file or a comma-delimited text file.

To export to an HTML file, click the **Export** menu, and then select the **Export to HTML** option.

To export to a comma-delimited text file, click the **Export** menu, and then select the **Export to Comma-Delimited Text** option.

Export to Text dialog field descriptions:

Source. Indicates the source supplying the event log entries for export into the file.

Choose File. If exporting to a comma-delimited file, this should be the path to the text file that will be created. If exporting to HTML, enter a path to an HTML file that will be created.

Browse (...). When exporting to text, this button allows you to browse and create a new text file. When exporting to HTML, you can browse and create a new HTML file.

Progress Bar. Indicates the export progress into the selected file.

Export. Starts the export process.

Exporting to a Database

You can export WhatsUp Event Analyst log source information to either an Ipswitch compatible event log table in an Access database or an ODBC database.

To export to an Access database, click the **Export** menu, and then select the **Export to Access** option.

To export to an ODBC database, click the **Export** menu, and then select the **Export to ODBC** option.

Export to Access dialog and Export to ODBC dialog field descriptions:

Source. Indicates the source supplying the event log entries for export into the database.

Choose Database. If exporting to Access, this should be the file path to the Access .MDB file. If exporting to ODBC, enter a fully qualified ODBC connection string here.

Browse (...). When exporting to Access, this button allow you to browse and select an existing Access database, or create a new one. When exporting to ODBC, this launches the ODBC connection manager, where you can select a predefined ODBC connection or define a new one. When setting up a new ODBC data source, you must use a File DSN to connect to your database server, not a system DSN. For more information on how to create a valid File DSN, review the *Setting Up Databases and Making Connections* (on page 31) help topic.

Choose Table. After a database is selected, WhatsUp Event Analyst populates this list with all available tables in the database. Select an existing WhatsUp Event Archiver/WhatsUp Event Analyst/WhatsUp Event Alarm compatible table or type in a new name if you want WhatsUp Event Analyst to create a new table.

Progress Bar. Indicates the export progress into the selected database table.

Export. Starts the export process.

Cancel. Closes the dialog, and if necessary, abandons the current exporting process.

Exporting to ODBC

The Export to ODBC dialog is used to convert an existing event log source to an Ipswitch compatible event log table in an ODBC database.

To open the dialog, click the **Export** menu, and then select the **Export to ODBC** option.

Export to ODBC dialog field descriptions:

Source. Indicates the source supplying the event log entries for export into the database.

Choose Database. If exporting to Access, this should be the file path to the Access .MDB file. If exporting to ODBC, enter a fully qualified ODBC connection string here.

Browse (...). When exporting to Access, this button allow you to browse and select an existing Access database, or create a new one. When exporting to ODBC, this launches the ODBC connection manager, where you can select a predefined ODBC connection or define a new one. When setting up a new ODBC data source, you must use a File DSN to connect to your database server, not a system DSN. For more information on how to create a valid File DSN, review the *Setting Up Databases and Making Connections* (on page 31) help topic.

Choose Table. After a database is selected, WhatsUp Event Analyst populates this list with all available tables in the database. Select an existing WhatsUp Event Archiver/WhatsUp Event Analyst/WhatsUp Event Alarm compatible table or type in a new name if you want WhatsUp Event Analyst to create a new table.

Progress Bar. Indicates the export progress into the selected database table.

Export. Starts the export process.

Cancel. Closes the dialog, and if necessary, abandons the current exporting process.

CHAPTER 7

Working with Reports

In This Chapter

Managing Reports

WhatsUp Event Analyst reports display in a tree structure that sorts reports by compliance regulation category, providing visibility to reports most relevant to your organization. Within the tree structure, top nodes are named according to category and the subnodes are named according to the name of the associated report.

Reporting categories include

§ HIPAA
§ Sarbanes-Oxley
§ PCI DSS
§ FISMA
§ FERPA
§ NERC CIP
§ MiFID
§ Gramm-Leach Bliley
§ Syslog (Cisco)
§ All reports
§ Custom reports

Note: Report taxonomies are only suggestions; consult with auditors and/or your organizational leadership for approval of their compliance requirements.

Reporting Issues

WhatsUp Event Analyst has the ability to generate three types of event log reports: detailed, pre-built, and custom reports. All reports are generated in HTML for easy viewing across a wide variety of platforms. In addition, pre-built and custom reports are also generated in CSV (comma-delimited) format, for further manipulation in spreadsheet programs and/or direct import into custom databases. This help section is dedicated to explaining all of these report types in further detail, and provide you with some suggestions on how to best implement them.

Detail Reports

In order to generate a detail report, apply a filter to an active log source, and then print the log from the *File Menu* (on page 20) by selecting the **Print Log Entries to HTML** menu option. Here are some examples of detail reports you can create using filters.

User Activity Report. Create and store a filter which only displays log records for an individual account. When you print the report, you can quickly ascertain all activity (successes and failures) for a given user over a given time frame.

Auditing Category Report. WhatsUp Event Analyst ships with predefined filters in most of the major auditing categories. Choose an audit category filter, apply it, and then print the log.

Error Report. Create and store a filter that only displays log records where the type of event is an error. This can help you pinpoint application or hardware failures.

Pre-Built Reports

Pre-built reports are created by selecting a particular report module from the *Reports Menu* (on page 23). You can create reports on demand (e.g. Run a Report Now) or schedule them for later generation (e.g. Schedule a Report For The Active Log Source / Schedule a Report For Any Log Source). When invoked, the module asks for any necessary information, and then builds the report. When the report is built, click the **View HTML** button to view the report in HTML format (Note: a default browser must be installed on your computer to view the report. We recommend viewing the report in Microsoft Internet Explorer version 4.0 or later). Likewise, click the **View CSV** button to view the comma-delimited report data in a spreadsheet program or Notepad. An example of a pre-built report module is the Top 10 Most Frequently Occurring Events report, which is useful in determining concentrations of greatest log activity in a filtered or non-filtered log source. As of this writing, WhatsUp Event Analyst has over 35 pre-built reports.

Custom Reports

Custom reports are very similar to detail reports, in that they rely primarily on filters to limit their information, but also allow the user to apply a custom grouping and sort order to the report fields. In order to build a custom report, the following steps must be taken:

1. Create a custom report layout with the Custom Reports Designer dialog
2. Attach a filter to a log source (this can either be an active log source that you are currently viewing in WhatsUp Event Analyst, or a log source you are scheduling a report against).

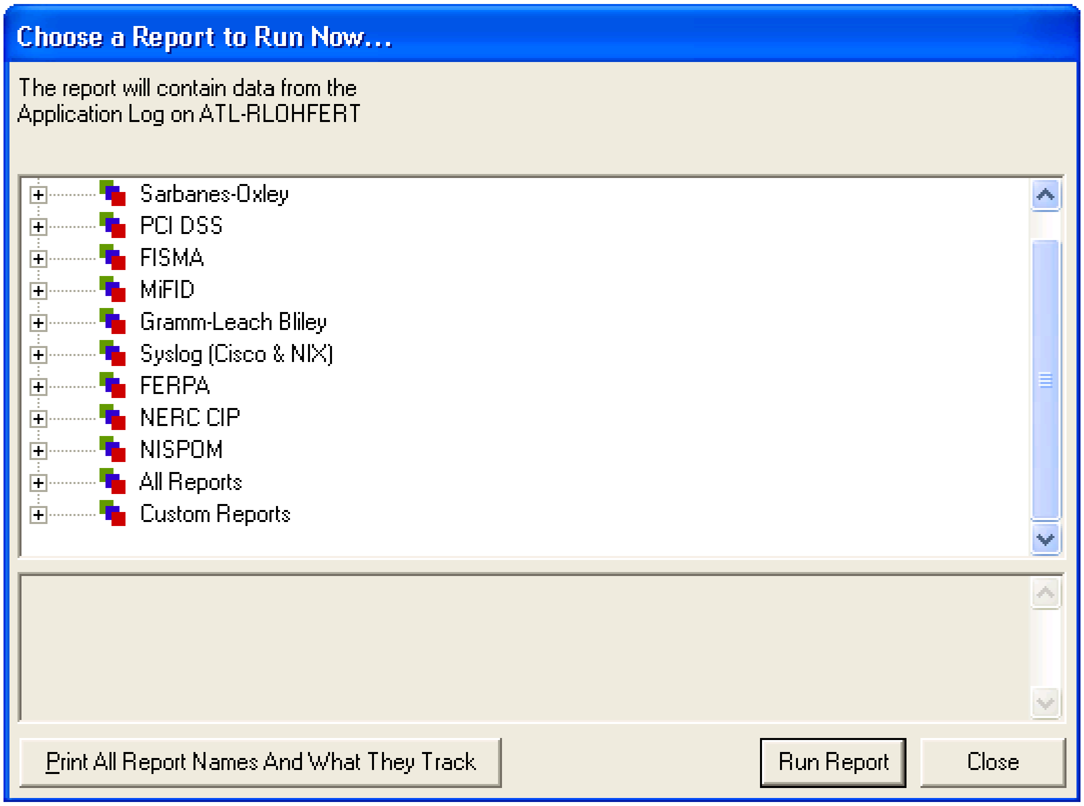
3 Invoke the custom report either immediately with the Report Chooser dialog or schedule it in the Report Scheduling Configuration dialog. All custom reports are prefaced with Custom Report in both dialogs to differentiate them from pre-built reports.

All scheduled reports log a success or failure event in the Application log where WhatsUp Event Analyst is installed. Use the WhatsUp Event Analyst Log Entries dialog to determine whether scheduled reports are being generated as they should.

Choosing a Report to Run Now

Use the Choose a Report to Run Now dialog to select a pre-built or custom report module you want to run against an event log source (e.g. the topmost Log View window). When invoked, the module processes events from the log source in question, and then gives you the option to view the resulting report in two formats. All reports are generated as HTML and CSV files, and they are stored in the working directory of WhatsUp Event Analyst Installation Folder>\Reports\Manual. You can save the report in a different location using your web browser or spreadsheet program.

Note: Taxonomies for compliance report (HIPPA, Sarbanes-Oxley, PCI DSS, FERPA, NERC CIP, FISMA, MiFID, Gramm-Leach Bliley) are suggestions; consult with your auditors and executives for approval of compliance plans.



Choose a Report to Run Now...

The report will contain data from the Application Log on ATL-RLOHFERT

- Sarbanes-Oxley
- PCI DSS
- FISMA
- MiFID
- Gramm-Leach Bliley
- Syslog (Cisco & NIX)
- FERPA
- NERC CIP
- NISPOM
- All Reports
- Custom Reports

The Choose a Report to Run Now dialog is accessible in one of two ways: either directly by clicking the **Build Report** button when opening a log source, or by selecting the **Run a Report Now** option from the *Reports menu* (on page 23) when events are currently being viewed inside WhatsUp Event Analyst in a *Log View Window* (on page 48). In the latter case, when the **Run a Report Now** menu option is selected, it takes as its log source focus the top-most *Log View Window* (on page 48) currently opened in WhatsUp Event Analyst.

To find out more about what any given report does, click the report name in the list. A full description of the report appears below the report listing, or clicking the **Print All Report Names and What They Track** button to export all report information to a text file. To build the report, click the **Run Report** button. To close this dialog, click the **Close** button.

Using the Report Scheduler

The Report Scheduler allows you to manage all scheduled reports that the WhatsUp Event Analyst Service is responsible for producing on a regular basis. From here, you can schedule a new report, edit an existing report's settings, clone a report, or delete a report from the scheduling database. The list of scheduled reports displays all reports scheduled for generation with the WhatsUp Event Analyst Service. Includes the report name, the log type, the time, and the interval.

New. Opens the Report Scheduling page, where a new report can be selected and scheduled.

Clone. Opens the Report Scheduling page, and copies the currently selected report's properties, allowing you to quickly schedule another report similar to the original.

Edit. Opens the Report Scheduling page, where an existing report's scheduling properties can be adjusted.

Delete. Deletes the currently selected report from the WhatsUp Event Analyst Service's scheduling database.

Configuring Scheduled Reports

Within this page and its tabs, select all options relevant to scheduling a summary or custom report with the WhatsUp Event Analyst service. Items on this page control which report is scheduled, the frequency it runs, the log source it uses as the basis of its data, and the output location for the HTML and CSV files generated.

To open the page, click **Analyst > Report Scheduler > New**.

Select Report tab:

Select the Report You Wish To Schedule. To select a report based on the report title, select the **Choose Report** radio button. Select the appropriate report from the list, then click **Submit**.

To select a report based on its category, select the **Choose Report by Category** radio button. Use the tree view to select the appropriate report, then click **Submit**.

Scheduling Options tab

Run This Report. When scheduling a report, you can either choose to create the report daily, weekly, or monthly. In addition to setting the day(s) the report runs, select the time when you want the report generated each day. It is best to schedule reports to run at off-peak times to minimize network traffic (e.g. after 12:00 midnight).

Database. Choose the database name containing the link to your database table or view.

Table. Select the table name associated with your selected database.

Log Type. Select the type of log that you want to report on.

Note: Some reports require a specific type of log (such as Security or System) to function correctly.

Output Directory. This field must contain a valid output folder where the HTML and CSV files are placed when they are created. By default, scheduled reports are written to the <WhatsUp Event Analyst Installation Folder>\Reports\Scheduled directory. You may want to create subfolders under this directory, such as one subfolder for each computer or log source, to properly organize your HTML reports. Alternatively, you can also have the reports created directly to a UNC share on a file server by supplying a UNC path in this field (e.g. \\FileServer\MyReports). Ensure the WhatsUp Event Analyst Service Account has full control access rights so it can create files in that share.

Email Recipients. If you want copies of a report sent to you or others via email after it is created, enter a comma-separated list of all email addresses in this field.

Note: If emailing reports, you must make sure to supply an SMTP server name in the Preferences page so that WhatsUp Event Analyst can relay the messages through your mail server.

Note: You can control how reports are sent in the Preferences page as well. Options include sending a link to the report, a zip file that contains all report files, or the uncompressed report files themselves.

Note: If used in conjunction with a custom report layout, advanced filters are a very powerful way to produce very specific reports on certain activities and/or trends on your network. Use the advanced filter to limit the scope of the data being reported on, and use the custom report sort definition to group and sort the filtered data into your desired format.

Report over all days / Only report over the last X days. If you schedule a recurring report (e.g. daily or weekly), you may find it useful to only report on data over the past day or few days. Setting this option creates a rolling schedule; as the reports run each day, the date range of data being reported on rolls with the schedule. This prevents reports containing duplicate data.

Note: If you select an advanced filter, this option is disabled. This is because advanced filters already have a way to limit data by recent dates, specifically, by using the relative date range option. For more information, please consult the *Advanced Filter Builder* (on page 38) dialog help topic.

Apply Filter tab

Use the Apply Filter tab to select and submit a filter. By attaching a filter, you can reduce the amount of data that WhatsUp Event Analyst reports on, producing smaller and more easily readable reports.

Select A Filter. Select either the **Basic Filter** radio button or the **Advanced Filter** radio button, and then select the appropriate filter. When finished, click **Submit**.

Designing Custom Reports

Use the Custom Reports Designer dialog to construct customized report layouts for filtered event log data. You can then pair these layouts with basic or advanced filters to produce reports targeting certain types of related log data.

To open the dialog, click the **Reports** menu, and then select the **Custom Reports Designer** option.

Note: For a detailed step-by-step tutorial on creating custom reports, please read the Custom Reporting in WhatsUp Event Analyst help file.

Custom Reports Designer dialog field and button descriptions:

Add. Opens the Custom Reports Editor, allowing you to create a new custom report design.

Edit. Opens the Custom Reports Editor, allowing you to edit an existing report design.

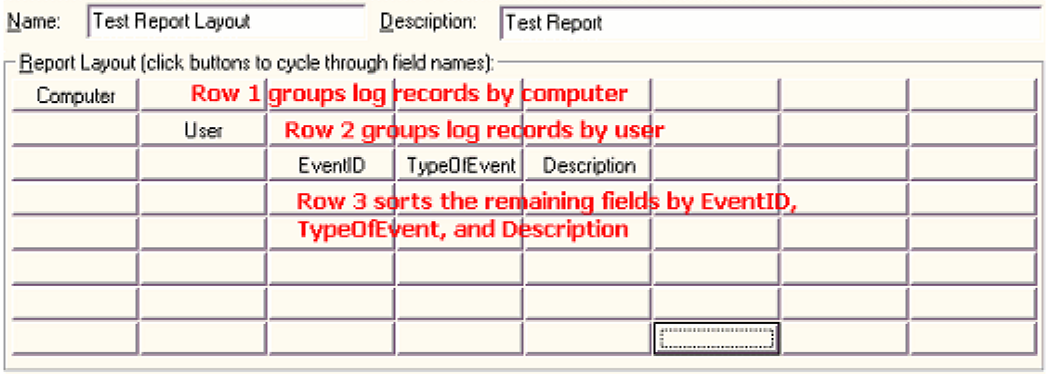
Delete. Deletes an existing custom report definition from WhatsUp Event Analyst's database.

Test. Tests the currently selected custom report layout against sample log data, and then allows you to view the created report. This aids in perfecting your reports layout.

Custom Reports Editor View

When you add or edit an existing custom report layout, the Custom Reports Designer dialog expands so you can change the grouping and sorting of fields in the layout. Specifically, an 8 x 8 grid displays. Clicking on any element of the grid allows you to place an available event log field at that position, change the event log field at that position, or clear the event log field at that position. You can think of each grid element as a toggle-button you can use to cycle through available event log fields.

Rows other than the last row are used to group records with a related field. Rows other than the last row cannot contain more than one element. If more than one row is used for grouping, each subsequent field must be offset by one column, as shown in the figure below. The first field in the final row must be offset by one column from the final grouping field, as shown below. The final row can contain more than one field, and the order of the fields (from left to right) in the final row determines the sort order.



Name: Test Report Layout Description: Test Report

Report Layout (click buttons to cycle through field names):

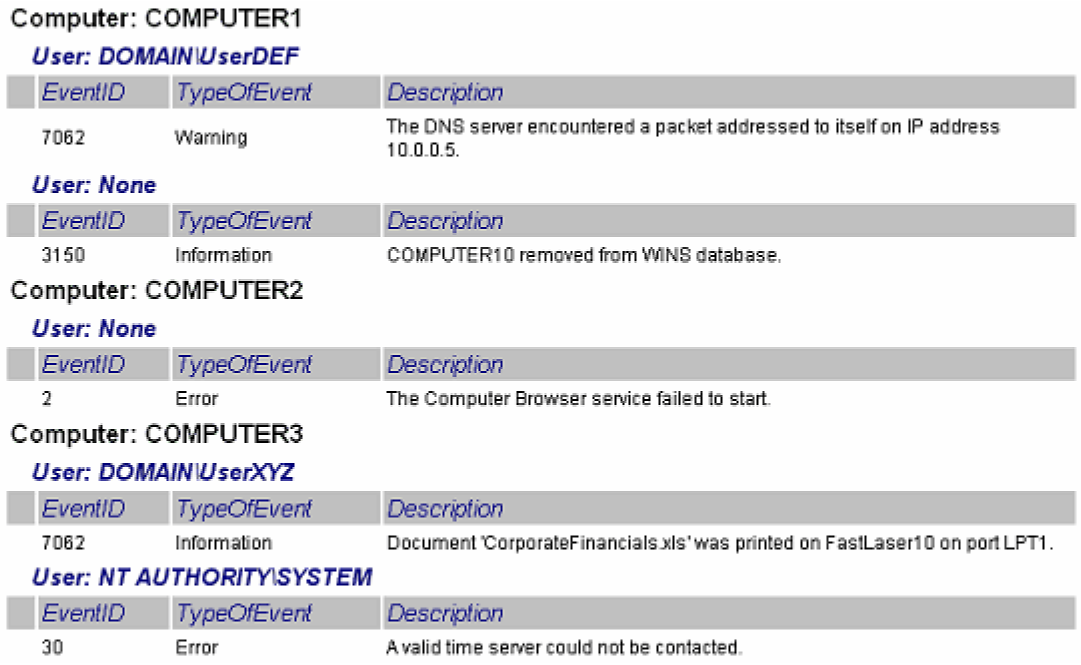
Computer							
	User						
		EventID	TypeOfEvent	Description			

Row 1 groups log records by computer

Row 2 groups log records by user

Row 3 sorts the remaining fields by EventID, TypeOfEvent, and Description

A sample report layout, where the first two rows contain grouping fields (e.g. Computer & User), and the final row contains the remaining fields in the report, ordered according to the desired sort priority.



Computer: COMPUTER1

User: DOMAIN\UserDEF

EventID	TypeOfEvent	Description
7062	Warning	The DNS server encountered a packet addressed to itself on IP address 10.0.0.5.

User: None

EventID	TypeOfEvent	Description
3150	Information	COMPUTER10 removed from WINS database.

Computer: COMPUTER2

User: None

EventID	TypeOfEvent	Description
2	Error	The Computer Browser service failed to start.

Computer: COMPUTER3

User: DOMAIN\UserXYZ

EventID	TypeOfEvent	Description
7062	Information	Document 'CorporateFinancials.xls' was printed on FastLaser10 on port LPT1.

User: NT AUTHORITY\SYSTEM

EventID	TypeOfEvent	Description
30	Error	A valid time server could not be contacted.

Data from an actual HTML report produced using the custom report layout designed in the previous figure.

You are not required to include all 8 event log fields in a custom report layout. Add only the ones you need to produce an understandable report.

If you need to make changes to an existing report layout, work backwards on the lowest row, from right to left, clearing grid elements, until you have reached the row you want to change. Alternatively, click the **Clear Grid** button to start over.

After you have created or modified a layout to your satisfaction, give it a name and description, and press the **Save** button to commit your changes.

Name. Enter the name for the custom report design you are creating.

Description. Enter a description of the custom report's purpose.

Help. Displays the custom reporting in the WhatsUp Event Analyst help file.

Clear Grid. Resets all of the fields on the grid, allowing you to start over and create a new layout.

Create Custom Field. Allows you to create a custom field definition to parse out a specific subvalue from a Windows Security Log event description.

Select Custom Field. Displays previously defined custom field definitions that you can make available to the current custom report design you are working on.

Save. Creates/updates the custom report definition in WhatsUp Event Analyst's database.

Cancel. Abandons changes made to the custom report definition.

Managing Friendly Event IDs

Use the Friendly Event ID Manager dialog to create friendly definitions for specific event identifiers (Event IDs) found in various log types.

To open the dialog, click the **Reports** menu, and then select the **Manage Friendly Event ID Definitions** option.

After a Friendly Event ID is defined, WhatsUp Event Analyst displays your friendly definition alongside the event identifier number in custom reports For example, a custom report previously grouped by Event ID now displays the friendly definitions alongside the Event IDs:

528 (Successful logon)

Event Record Data 1

Event Record Data 2

Event Record Data n…

538 (User logoff)

Event Record Data 1

Event Record Data 2

Event Record Data n…

Note: You can also use the Friendly Event ID Manager dialog to select one or more events when building an Advanced Filter inside WhatsUp Event Analyst.

Manage Mode

Add. Adds a new Friendly Event ID definition.

Edit. Allows you to edit an existing Friendly Event ID definition.

Delete. Deletes the currently selected definition.

Close.Closes the Friendly Event ID Manager.

Use Friendly Event IDs in custom reports to make them more descriptive. If this option is checked, matching friendly descriptions of certain Event IDs is placed in parentheses beside the Event ID numbers in custom reports. If this option is unchecked, no mapping is performed in custom reports.

Add/Edit Mode

Event ID. Enter the event identifier number for the event you want to associate with a friendly definition.

Source. Select the source with which this identifier is associated.

Log Type. Select the log type in which this event identifier is found.

Friendly Description. Enter descriptive text explaining the meaning/purpose of this event.

Save. Adds this definition to the Friendly Event ID database, or saves changes to an existing definition.

Cancel. Abandons an adding or editing operation.

Event ID Chooser Mode

OK. Returns the Event IDs you have chosen (e.g. checked) to the *Advanced Filter Builder* (on page 38) dialog.

Cancel. Closes the dialog without returning any Event IDs.

Viewing and Managing the Manual Reports Folder and the Scheduled Reports Folder

You can quickly access the Windows Explorer Manual Reports folder and the Scheduled Reports folder directly from WhatsUp Event Analyst. Access the folders to edit and manage them within Windows Explorer. To access the folders directly from Whatsup Event Analyst, click the **Reports** menu, and then select either the **View/Manage Manual Reports Folder** option or the **View/Manage Scheduled Reports Folder** option.

CHAPTER 8

Managing Syslog Reports

In This Chapter

Viewing the Cisco User Lockouts and Unlocks Report

The Cisco User Lockouts and Unlocks report displays user lockouts, due to authentication failures, and administrative unlocks of previously locked user accounts. This report targets the %AAA-5-USER_LOCKED and %AAA-5-USER_UNLOCKED Cisco IOS status messages, displaying by device/router all account lockouts by username. Unlocked accounts display by account name.

To view the Cisco User Lockouts and Unlocks report:

1 From the WhatsUp Event Analyst control panel, click the **Reports** menu, then select **Run a Report Now**. The Choose a Report to Run Now dialog opens.

2 Expand the Syslog (Cisco & NIX) tree, select the Cisco User Lockouts and Unlocks report, and then click **Run Report**. WhatsUp Event Analyst opens the selected report.

Cisco User Lockouts and Unlocks

Account Lockouts by Router/Device then Username

Router / Device Name	Date & Time	Username
CiscoRouter	[illegible]	[illegible]

Account Unlocks by Router/Device then Account Name

Router / Device Name	Date & Time	Account Name	Username
CiscoRouter	[illegible]	[illegible]	[illegible]

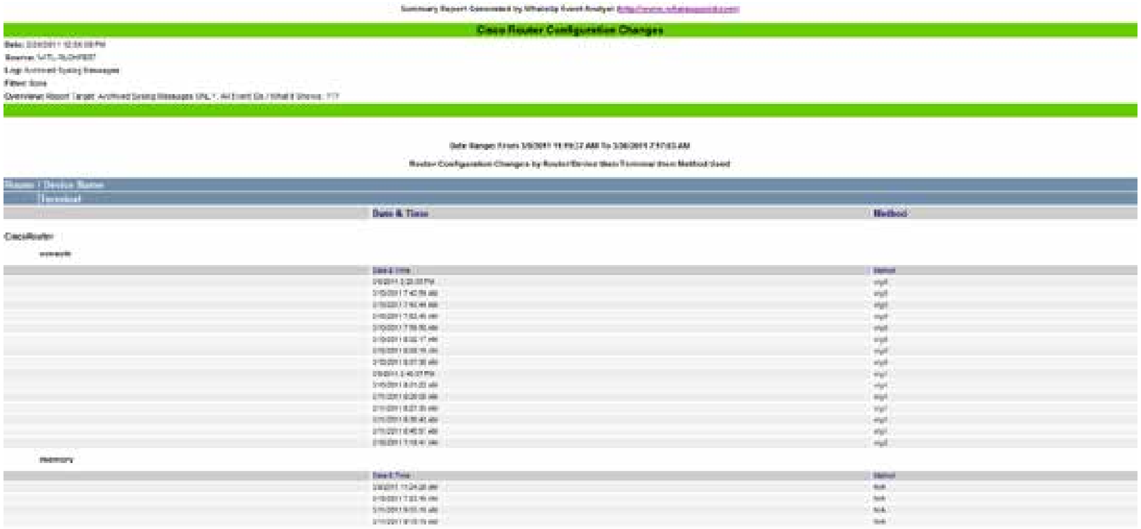
Viewing the Cisco Router Configuration Changes Report

The Cisco Router and Configuration Changes report displays all instances of user-initiated configuration changes on a Cisco device running IOS. Status messages referencing %SYS-5-CONGIG_1: are reported by devices and then sorted by the machine where the configuration change originated and the method used to change the configuration.

To view the Cisco Router Configuration Changes report:

1 From the WhatsUp Event Analyst control panel, click the **Reports** menu, then select **Run a Report Now**. The Choose a Report to Run Now dialog opens.

2 Expand the Syslog (Cisco & NIX) tree, select the Cisco Router Configuration Changes report, and then click **Run Report**. WhatsUp Event Analyst opens the selected report.



Cisco Router Configuration Changes

Router / Device Name

Terminal

Date & Time

Method

CiscoRouter

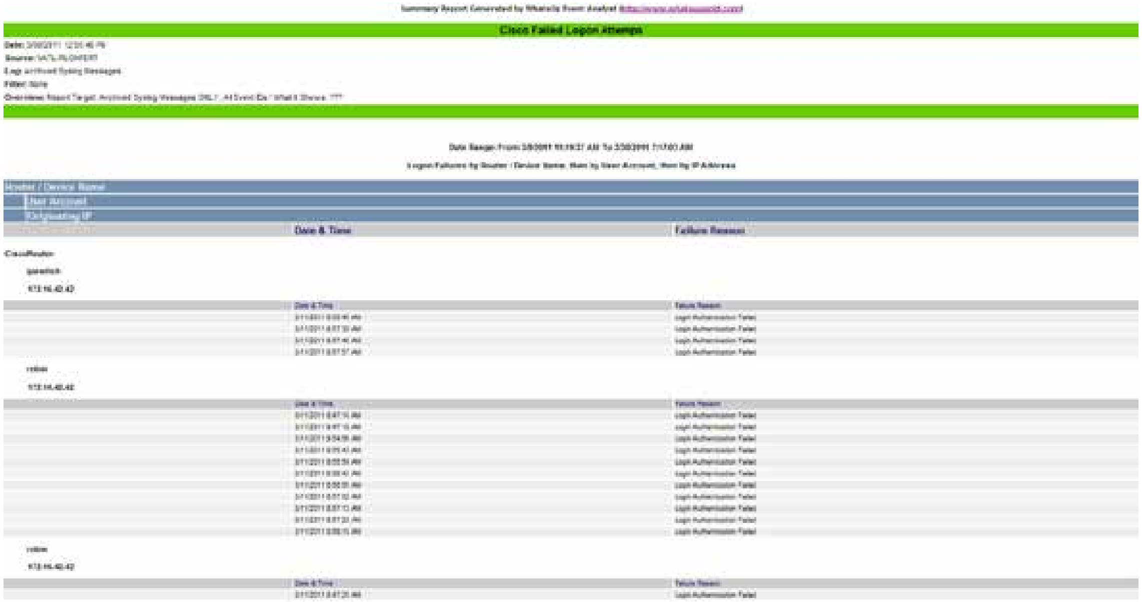
Viewing the Cisco Failed Logon Attempts Report

The Cisco Failed Logon Attempts report displays all logon failures from one or more Cisco devices. The %SEC_LOGIN-4-25 and %SEC_LOGIN-4-LOGIN_FAILED status messages are targeted, with a breakdown of logon failures by user account, by origination IP, and by failure reason.

To view the Cisco Failed Logon Attempts report:

1 From the WhatsUp Event Analyst control panel, click the **Reports** menu, then select **Run a Report Now**. The Choose a Report to Run Now dialog opens.

2 Expand the Syslog (Cisco & NIX) tree, select the Cisco Failed Logon Attempts report, and then click **Run Report**. WhatsUp Event Analyst opens the selected report.



Summary Report Generated by WhatsUp Event Analyst [illegible]

Cisco Failed Logon Attempts

Date: [illegible]
Source: [illegible]
Log: Archived Syslog Messages
Filter: None
Overview: [illegible]

Date Range: [illegible]

Logon Failures by Router / Device Name, then by User Account, then by IP Address

Router / Device Name
User Account
Originating IP

Date & Time	Failure Reason

CiscoRouter

[illegible]

[illegible]

Date & Time	Failure Reason
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed

[illegible]

[illegible]

Date & Time	Failure Reason
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed
[illegible]	Login Authentication Failed

[illegible]

[illegible]

Date & Time	Failure Reason
[illegible]	Login Authentication Failed

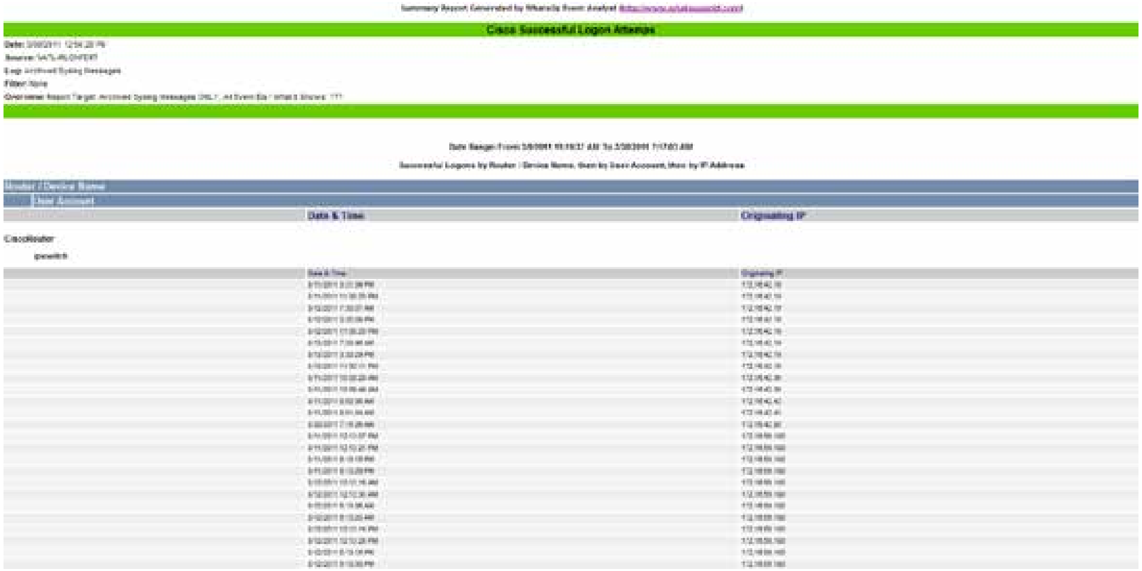
Viewing the Cisco Successful Logon Attempts Report

The Cisco Successful Logon Attempts report displays all successful logons for one ore more Cisco devices. The %SEC_LOGIN_SUCEESS: messages are targeted, with a breakdown of logon successes by user account and by originating IP.

To view the Cisco Successful Logon Attempts report:

1 From the WhatsUp Event Analyst control panel, click the **Reports** menu, then select **Run a Report Now**. The Choose a Report to Run Now dialog opens.

2 Expand the Syslog (Cisco & NIX) tree, select the Cisco Successful Logon Attempts report, and then click **Run Report**. WhatsUp Event Analyst opens the selected report.



Summary Report Generated by WhatsUp Event Analyst [illegible]

Cisco Successful Logon Attempts

Date: [illegible]
Source: [illegible]
Log: Archived Syslog Messages
Filter: None
Overview: Report Target: Archived Syslog Messages ONLY, All Event IDs / What It Shows: ???

Date Range: From [illegible] To [illegible]

Successful Logons by Router / Device Name, then by User Account, then by IP Address

Router / Device Name
User Account

Date & Time	Originating IP
[illegible]	[illegible]

CiscoRouter
ipswitch

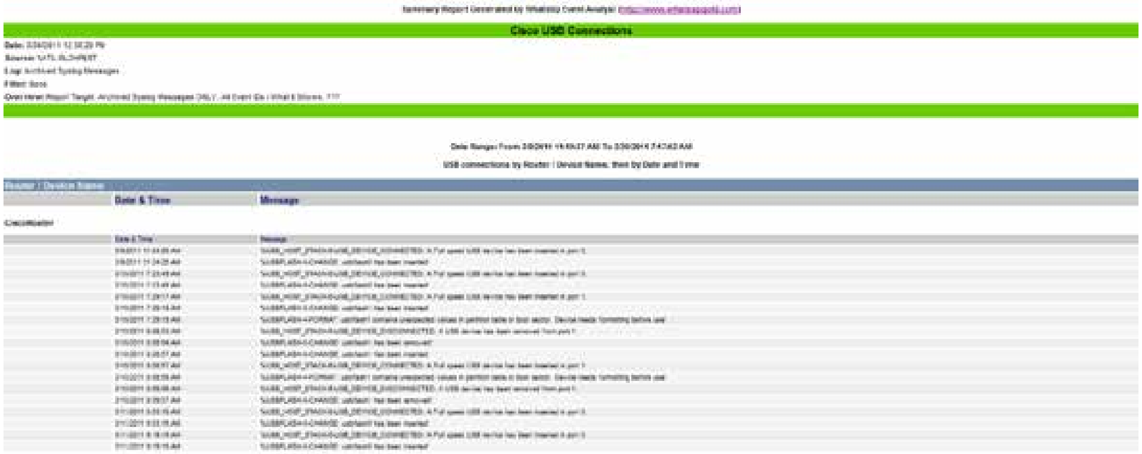
Viewing the Cisco USB Connections Report

The Cisco USB Connections report displays all status messages from one or more Cisco devices referencing any status message beginning with %USB, allowing the viewer to determine if a router reconfiguration or data file backup has been attempted with a USB device.

To view the Cisco USB Connections report:

1 From the WhatsUp Event Analyst control panel, click the **Reports** menu, then select **Run a Report Now**. The Choose a Report to Run Now dialog opens.

2 Expand the Syslog (Cisco & NIX) tree, select the Cisco USB Connections report, and then click **Run Report**. WhatsUp Event Analyst opens the selected report.



Summary Report Generated by WhatsUp Event Analyst [illegible]

Cisco USB Connections

Date: [illegible]
Source: [illegible]
Log: Archived Syslog Messages
Filter: None
Overview: Report Target: Archived Syslog Messages ONLY, All Event IDs / What It Shows: ???

Date Range: From [illegible] To [illegible]

USB connections by Router / Device Name, then by Date and Time

Router / Device Name

CiscoRouter

Date & Time	Message
[illegible]	[illegible]

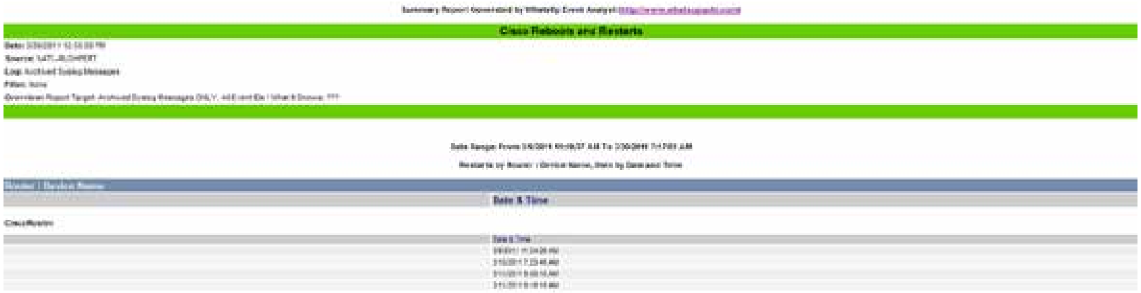
Viewing the Cisco Reboots and Restarts Report

The Cisco Reboots and Restarts report displays all Cisco device restarts by targeting the %SYS-5-RESTART status message. All reboots and restarts are sorted by router or device.

To view the Cisco Reboots and Restarts report:

1 From the WhatsUp Event Analyst control panel, click the **Reports** menu, then select **Run a Report Now**. The Choose a Report to Run Now dialog opens.

2 Expand the Syslog (Cisco & NIX) tree, select the Cisco Reboots and Restarts report, and then click **Run Report**. WhatsUp Event Analyst opens the selected report.



Cisco Reboots and Restarts

Router | Device Name

Date & Time

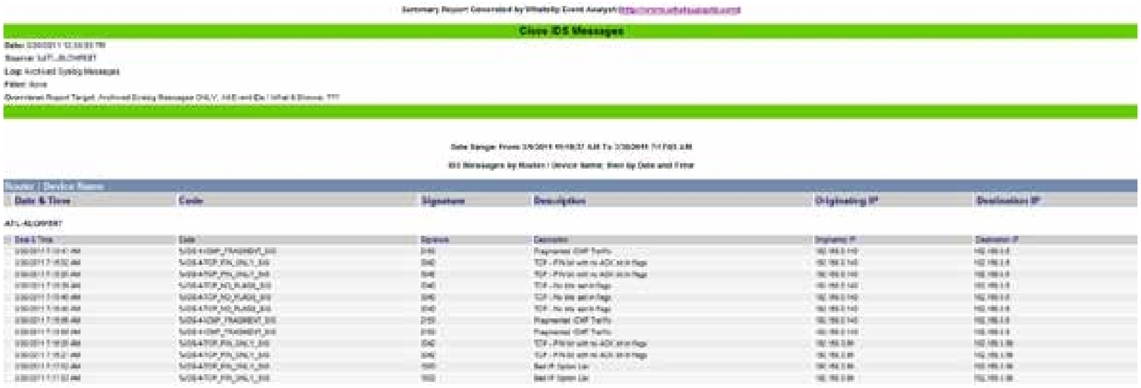
Viewing the Cisco IDS Messages Report

The Cisco IDS Messages report displays all status messages from one or more Cisco devices referencing a status message beginning with %IDS, allowing the viewer to determine if any attempted intrusions or unauthorized network probing is taking place as detected.

To view the Cisco IDS Messages report:

1 From the WhatsUp Event Analyst control panel, click the **Reports** menu, then select **Run a Report Now**. The Choose a Report to Run Now dialog opens.

2 Expand the Syslog (Cisco & NIX) tree, select the Cisco IDS Messages report, and then click **Run Report**. WhatsUp Event Analyst opens the selected report.



Cisco IDS Messages

Router | Device Name

Date & Time	Code	Signature	Description	Originating IP	Destination IP