



IPSWITCH

WhatsUp Event Alarm
v10.x
User Guide

CHAPTER 1 WhatsUp Event Alarm Help And Users Guide

WhatsUp Event Alarm Overview and Architecture	1
Deployment Scenarios.....	2
WhatsUp Event Alarm Concepts.....	4
Monitoring Strategies	5
Tips and Tricks.....	6
WhatsUp Event Alarm	6
WhatsUp Event Archiver	7
Initial Setup	8
Using the License Manager	8
WhatsUp Event Alarm's Feature Areas.....	11
Legal Information and License Agreement.....	12
Troubleshooting / Contacting Technical Support	16

CHAPTER 2 Using WhatsUp Event Alarm Menu Options

Using the File Menu	20
Using the Edit Menu.....	21
Using the View Menu.....	21
Using the Tools Menu	21
Using the Options Menu.....	22
Using the Help Menu.....	23

CHAPTER 3 Setting Up Monitoring for Multiple Computers

Using the Rapid Configuration Tool.....	24
Setting-up Monitoring for Multiple Computers at Once (Step 1).....	26
Setting-up Monitoring for Multiple Computers at Once (Step 2).....	27
Setting-up Monitoring for Multiple Computers at Once (Step 3).....	28
Setting-up Monitoring for Multiple Computers at Once (Step 4).....	28
Setting-up Monitoring for Multiple Computers at Once (Step 5).....	29
Setting-up Monitoring for Multiple Computers at Once (Step 6).....	29

CHAPTER 4 Changing Monitoring on Multiple Computers

Adjusting Settings for Currently Monitored Logs (Step 1).....	30
Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 2).....	31
Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 3).....	32
Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 4).....	33
Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 5).....	34

Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 6).....	35
---	----

CHAPTER 5 Monitoring Windows Event Logs

Defining Custom Alarms.....	36
Defining Custom Syslog Alarms.....	38
Defining Alarm Bundles	39
Defining Notifications.....	40
Defining Custom Notifications.....	44
Monitoring Custom Event Logs.....	45
Watching Logs.....	46
Deleting Monitored Logs.....	49

CHAPTER 6 Adjusting Audit Policies on Workstations and Servers

Adjusting Audit Policies	50
Unifying Audit Policies (Step 1)	51
Unifying Audit Policies (Step 2)	51
Unifying Audit Policies (Step 3)	51

CHAPTER 7 Adjusting Log Retention and Size Settings on Computers

Adjusting Log Retention and Log Size Settings.....	53
Unify Log Settings (Step 1).....	54
Unify Log Settings (Step 2).....	54
Unify Log Settings (Step 3).....	55
Unify Log Settings (Step 4).....	55

CHAPTER 8 Monitoring Syslog Devices

Changes in Syslog Support Between WhatsUp Log Management v9 to WhatsUp Log Management v10	56
Syslog Support in WhatsUp Event Alarm.....	58
Adding a New Syslog Device	61

CHAPTER 9 Sharing Defined Alarms Among Multiple WhatsUP Event Alarm Installations

Exporting Alarms.....	63
Importing Alarms	64

CHAPTER 10 Creating Database Tables for Storage of Detected Events

Creating Tables.....	65
Creating Tables on Other ODBC Servers	66

Setting Up Databases and Making Connections.....	67
--	----

CHAPTER 11 Configuring and Tuning WhatsUp Event Alarm

Setting Preferences	68
Enabling Flood Control.....	72
Setting the Default Domain / Workgroup	73
Installation Requirements	73
Before You Begin.....	75
Microsoft Vista / Windows Server 2008 Requirements and Recommendations	85
Other Recommendations	88
Rapid Configuration Chooser Dialog	92
Rapid Configuration Chooser Dialog	93
Service Account Dialog.....	93
Build Priority Dialog	95
WhatsUp Event Alarm Log Entries Viewer Dialog.....	97
Custom Domain Manager Dialog.....	97
Computer Name Retrieval Dialog.....	99

CHAPTER 1

WhatsUp Event Alarm Help And Users Guide

In This Chapter

WhatsUp Event Alarm Overview and Architecture.....	1
Deployment Scenarios.....	2
WhatsUp Event Alarm Concepts.....	4
Monitoring Strategies.....	5
Tips and Tricks.....	6
Initial Setup.....	8
Using the License Manager.....	8
WhatsUp Event Alarm's Feature Areas.....	11
Legal Information and License Agreement.....	12
Troubleshooting / Contacting Technical Support.....	16

WhatsUp Event Alarm Overview and Architecture

What Does WhatsUp Event Alarm Do?

WhatsUp Event Alarm continuously monitors new event log entries as they are generated on servers and workstations throughout your network. Specifically, you can associate one or more alarms (an alarm being defined as a combination of event log fields (e.g. Source, Type Of Event, EventID) to monitor for) with one or several of the event logs the WhatsUp Event Alarm Service is watching. When an alarm is "tripped" (e.g. a new event log record is recorded that matches the criteria of an alarm), the WhatsUp Event Alarm Service sends one or more alerts (notifications) to you in real time informing you immediately about the incident. Notification options include email message, network popups, pager alerts, forwarding events to a syslog server, inserting entries into a database, and a listener console that captures targeted UDP datagrams and broadcast NetBIOS messages that contain event information.

Unlike many other server monitoring tools in the market, WhatsUp Event Alarm does not require client services to be installed on all of the servers whose logs you want to watch. Because the WhatsUp Event Alarm Service typically runs under a domain administrator account, it can monitor event logs over the network and send out notifications from one or more listening points on your network. Also, Because you can watch over several computers from a single WhatsUp Event Alarm installation, it is easy to change monitoring settings for all computers from the central WhatsUp Event Alarm Control Panel running on one computer.

For added flexibility, install and run WhatsUp Event Alarm on single, non-domain workstations or servers, such as those that exist inside a demilitarized zone. In addition, you

can install multiple instances of WhatsUp Event Alarm to different computers on your network, such as one installation per WAN (Wide Area Network) site if you have a distributed network, and wish to minimize scanning latency and/or the use of WAN bandwidth.

How Does WhatsUp Event Alarm Work?

The WhatsUp Event Alarm program can be subdivided into 4 major parts:

- § **The Log Monitoring Database.** This database stores all of the information about what logs to monitor, and their associated alarms and notification methods. After you place a log in the monitoring database, the WhatsUp Event Alarm Service immediately begins scanning on a regular basis for new event log entries.
- § **The WhatsUp Event Alarm Service.** This is the true 24/7, 365 day engine of the WhatsUp Event Alarm product. Running all the time, even without user interaction, it uses the Log Monitoring Database to continuously scan for new event log entries on remote computers, sending out notifications when alarms are tripped. For maximum performance, it can delegate log scanning and notification work out to companion processes, which is directly configurable by the network administrator.
- § **The WhatsUp Event Alarm Control Panel.** This is the centralized GUI administration console that you use to manage the event logs you are watching with the WhatsUp Event Alarm Service. In many ways, it is a graphical representation of the Log Monitoring Database. However, it also contains many other useful features, such as allowing you to adjust audit policies on computers, and event log settings like file sizes and retention policies. To read more about its interface, visit the WhatsUp Event Alarm's Main Interface help topic.

Deployment Scenarios

Well-connected Local Area Networks

Deploying WhatsUp Event Alarm in a Local Area Network environment is one of the easiest ways to configure and use the solution. If all machines whose logs will be monitored reside in the same domain (or trusting domains) and are well connected by 100Mbit or greater Ethernet links, choose one high-capacity server or workstation to run the WhatsUp Event Alarm solution. If you have more than 50 servers whose logs must be monitored, or if you do a great deal of auditing (e.g. more than 10 megs of security events per day on domain controllers), you may wish to set up multiple installations of WhatsUp Event Alarm for better load balancing. For example, Installation A of WhatsUp Event Alarm could be configured to monitor only your domain controllers with high levels of auditing activity, and Installation B could monitor your member servers and workstations.

If you have a well-connected LAN with non-trusting domains or a series of workgroups, set up, at minimum, a WhatsUp Event Alarm system in each separate domain/workgroup.

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

Deployment of WhatsUp Event Alarm in a WAN environment or DMZ setting is more complex but manageable. If you have a domain environment at each remote end of the WAN, or if the domain spans multiple WAN links, set up one WhatsUp Event Alarm system at each end of the WAN link. Doing so reduces traffic flowing across the often bandwidth-limited or high-

latency WAN link. When notifications need to flow from the remote WAN site to the central network, instruct WhatsUp Event Alarm to use TCP/IP-friendly notification methods, such as SMTP email, syslog messages, and ODBC database connections.

Demilitarized zones often do not allow typical Microsoft networking connections between machines, and if that proves true on your network, you should install WhatsUp Event Alarm on each machine residing in the DMZ. To simplify the rollout of WhatsUp Event Alarm on these individual systems, consider using WhatsUp Event Alarm's ability to export and import alarm definitions to and from text files. You can create an export file with the most frequently needed alarms, and then import that file into each system after installation. Also, consider creating rapid configuration templates that can be used on more than one system to quickly configure different WhatsUp Event Alarm systems to use a similar monitoring strategy.

After the software is installed to each machine, configure the machines to send notifications back into the protected network using TCP/IP-friendly notifications like SMTP email, syslog packets, and ODBC database connections. You may need to adjust certain firewall settings in order for data to flow inward as described.

WhatsUp Event Alarm Concepts

Alarms

Specify the criteria in a detected event that triggers a notification. (E.g. Source = Security, Event ID = 529).

Are defined and managed under the Edit Menu->Define Alarms menu option.

Can fire any time a matching event is detected, or can be contrained to only fire when X number of occurrences happen in X number of seconds (e.g. a threshold alarm).

Ignore Events

Defined exactly the same way as an alarm (e.g. Edit Menu->Define Alarms) but are used differently.

When an alarm is associated with a computer log as an ignore event, any event detected on the computer log that matches the ignore event is discarded.

Alarm Bundles

Housekeeping measure used to group related alarms alongside one another.

Are defined and managed under the Edit Menu->Define Alarm Bundles area.

Can be associated with computer logs alongside or in lieu of individual alarms.

Make it easier to centrally adjust what is monitored on various computer logs without having to adjust each computer log individually. Adjusting alarm membership in an alarm bundle effects the monitoring profile on all computers logs that use that alarm bundle.

Notifications

Specify how the administrator will be notified when an alarm is triggered.

Are defined and managed under the Edit Menu->Define Notifications area.

Can be associated only with a specific alarm (e.g. a **specific notification**) or can be associated with a log on a computer (e.g. a **general notification**).

Specific notifications are performed when their corresponding alarm is detected on a monitored computer log.

General notifications are performed when any alarm is detected on the monitored computer log to which they are bound.

Monitored Computer Event Logs

Are associated with one or more alarms, ignore events, alarm bundles, and notifications.

Represent the particular Windows Event Log on a computer being monitored.

Their monitoring profile can be modified individually by selecting either **Watch a New Log** or **Edit the Selected Log** from the File Menu.

Their monitoring profile can be modified alongside other logs at the same time by selecting **Rapid Configuration Setup, Setup Monitoring for Multiple Computers at Once,** or **Adjust Settings for Currently Monitored Logs** from the Tools Menu.

Must be associated with alarm(s) and notification(s) to be monitored correctly by Event Alarm.

Monitoring Strategies

Different organizations have different requirements for how they monitor log information over time. The following section outlines a few more common collection practices, and how to implement them with WhatsUp Event Alarm.

Just show me warnings and errors

Many administrators want a simple tool that informs them when less-than-desirable things start happening on their servers. Warnings and errors from applications and hardware are of paramount importance to them. WhatsUp Event Alarm can meet this need with ease.

- 1 From the WhatsUp Event Alarm Control Panel, click the **Tools** menu, and then select *Rapid Configuration Setup* (on page 92).
- 2 Select the domain or workgroup of the computers you need to monitor.
- 3 Select the computers and log types you want to monitor for errors and warnings.
- 4 Define a notification or several notifications that inform you when warning or error events occur. In a large network with a high volume of events, you may want to use syslog messages as a notification method, and route them to the names or IP address(es) of machines running the WhatsUp Event Alarm Listener Console. Alternatively, you can use database insertions as a notification method, and then periodically review the collected events using Dorian Software's WhatsUp Event Analyst tool, or another database querying utility.
- 5 From the Rapid Configuration screen, set WhatsUp Event Alarm to send out notifications when **errors are detected on systems** and when **warnings are detected on systems**.

I am only concerned about a small, specific group of events

In some cases, administrators may only be concerned with very specific events, like when a certain job completes on their network, or when a business-critical server application goes down. In situations like these, it is best to send the notification via email or pager immediately when the event is detected. If certain events should be used to notify specific individuals, separate notifications should be created for each party, and then should be attached as specific notifications to the alarm they act upon. For example, if you must trap for a specific type of Microsoft Exchange Server error, you may want that alarm to only notify the Exchange administrator via email.

After you have created the appropriate custom alarms and notifications, place these alarms into an alarm bundle, and then start the process of associating that alarm bundle with event logs on computers on your network. You can use one of the Step-By-Step Wizards (under the Tools menu) for that purpose.

I need to know when certain security related activities happen on servers in my network, especially on my domain controllers

WhatsUp Event Alarm ships with many predefined alarms in each of the major Microsoft Windows auditing categories. Some examples of these auditing categories include:

- § Account Logons and Logoffs
- § Active Directory Object Modifications

- § File, Registry, and Object Auditing
- § User, Group, and Computer Management

Using the Rapid Configuration Tool from the Tools menu, you can quickly check off certain types of security activities you need to know about, such as user/group/computer account creation, group membership changes, logon failures, and others.

If you want to be more specific with your monitoring, you can modify some of WhatsUp Event Alarm's existing alarms to meet your needs. For example, to meet HIPAA requirements, you might need to track all changes to a file or group of files in a directory. To do so, you could modify the Successful Object Open and Failed Object Open alarms to include the directory name or file name you are interested in, and then bundle all related alarms into an alarm bundle you define.

I want to run a central console on my desktop allowing events of interest to stream into view

WhatsUp Event Alarm provides this centralized, streaming view by way of the WhatsUp Event Alarm Listener Console. The WhatsUp Event Alarm Listener Console receives incoming NetBIOS broadcast messages or UDP datagrams sent as syslog messages, both of which are generated by WhatsUp Event Alarm when an alarm is detected. In general, UDP datagrams sent as syslog messages are the recommended notification method here, as they can be targeted and offer more features in the WhatsUp Event Alarm Listener Console.

To learn more about setting up the WhatsUp Event Alarm Listener Console on administrator workstations, refer to its online help documentation.

Tips and Tricks

If you have a huge domain consisting of several hundred servers, you will most likely want to try some of the following techniques to optimize performance.

WhatsUp Event Alarm

- 1 Install WhatsUp Event Alarm on more than one server.** By installing the program on more than one server, you can make different servers monitor different sets of computers on your network. For example, you can have 10 monitoring servers, each monitoring 15 computers each. This reduces the processor and memory load on each WhatsUp Event Alarm server. In addition, if you have very high activity servers on your network, such as email servers or domain controllers (Active Directory servers) logging many events per minute. In those situations, it may be best to dedicate an WhatsUp Event Alarm installation to monitoring those critical servers and use another WhatsUp Event Alarm installation to monitor the remaining logs on a network segment.

If you are configuring WhatsUp Event Alarm to receive a high volume of syslog messages from other devices on your network, it may also be a good idea to install additional WhatsUp Event Alarm servers. In this way, you can break up the devices which forward syslog messages to use different WhatsUp Event Alarm servers, and reduce the overhead on any one WhatsUp Event Alarm server.

If you plan to use WhatsUp Event Alarm in a WAN environment, it is recommended that you install an WhatsUp Event Alarm Server locally at each remote end of the WAN to improve monitoring performance and reduce notification latency.

- 2 **Optimize performance settings in the Preferences dialog.** WhatsUp Event Alarm is designed for networks of all sizes by providing adjustable settings for resource usage (e.g. CPU, memory, etc.) For example, if you have a large set of available memory on your monitoring server, you may want to make multiple scanning processes for WhatsUp Event Alarm to use when looking for alarm triggers on remote logs. You may also want to consider enabling Turbo Scanning Mode. While this can generate more memory and processor overhead, it allows WhatsUp Event Alarm to scale to higher volume servers on networks.
- 3 **Do not go overboard on setting alarms.** It is best to only select alarms that reflect critical situations on particular computers (e.g. a bad login, low disk space, fault-tolerant disk error, etc). The more alarms you attach to a log, the longer it takes WhatsUp Event Alarm to scan through new entries that occur on that event log. In general, if you need to "cast a wider net" for a larger range of possible events, set fewer but broader alarms. For instance, instead of creating 10 alarms each scanning for a particular EventID, create an alarm that is associated with a certain type of event (e.g. error) and source (e.g. Microsoft Exchange Server).

WhatsUp Event Archiver

- 1 **Install WhatsUp Event Archiver on more than one server.** By installing the program on more than one server, you can make different servers manage different sets of computers on your network. For example, you could have 7 archiving servers, each managing 100 computers to better optimize your network traffic according to topology: where you have switches as opposed to hubs on the LAN. Plus, this reduces the processor and memory load on each WhatsUp Event Archiver server.
- 2 **Avoid scheduling archiving times too close to one another.** If you elect to collect your logs daily, weekly, or monthly, ensure you space out the collection times. Even a few minutes in between logs can make a noticeable difference. You can also schedule logs to archive when they approach their size limits. Because logs on different computers grow at different rates, this guarantees that the archiving process is spread out across a wide range of times.
- 3 **Collect the logs as EVT/EVTX files as opposed to converting them to text files, Access, or ODBC databases.** It takes extra processor overhead to convert saved log files into other formats, such as Access or ODBC databases. Collecting them in their native EVT/EVTX format reduces work for the WhatsUp Event Archiver Service. However, if you spread out the collection times well enough as mentioned in Tip 2, converting into different data formats should present no problems.
- 4 **Match platforms.** If you plan on converting event log entries into text files, Access databases, or ODBC databases, install WhatsUp Event Archiver on the platform (e.g., Windows 2003) that matches the majority of your servers and workstations. If you match

platforms, WhatsUp Event Archiver can take advantage of caching which can increase data conversion speed and reduce network bandwidth.

- 5 **Compress data.** If you are collecting logs in EVT or text formats, you may want to compress the files after each archive. Compressing log files can shrink them down to 5% of their original size and will greatly reduce the amount of storage needed on the final destination file server.
- 6 **Use the Working Directory.** WhatsUp Event Archiver allows you to first transport archived EVT/EVTX files to a temporary working directory local to the machine running WhatsUp Event Archiver. This greatly speeds up the time needed for log processing, such as MD5 hash calculation, zipping, and conversion into other formats, and also saves bandwidth. You can control the size of files transported to this directory, as well as the location of the directory here.

Did you know that you can consolidate event log entries from untrusting domains into a single database? If you have a Microsoft SQL Server on a TCP/IP based LAN, you can set the SQL Server up so that it uses standard authentication (as opposed to Windows authentication). After defining a username and password for the SQL server, you can make WhatsUp Event Archiver servers from different domains send all of their log entries to that central server. Read more about how to work with ODBC databases in the Log Registration Options dialog section of this help file.

Visit the *Ipswitch Support* (<http://www.whatsupgold.com/support/library/index.aspx>) website to find additional information and upgrades for this product.

Initial Setup

The links below open topics about setting up WhatsUp Event Alarm for the first time.

Installation Requirements (on page 73)

Manually Creating Firewall Exceptions

Before You Begin (on page 75)

Microsoft Vista / Windows Server 2008 Requirements and Recommendations (on page 85)

Other Recommendations (on page 88)

Configuring the WhatsUp Event Alarm Service Account (on page 93)

Using the License Manager

When you install WhatsUp Event Alarm, it automatically runs in 30-day evaluation mode, and it allows you to monitor event logs from 50 different computers at once. To shift the product into registered mode after purchasing licenses from Ipswitch or a reseller, you must use the License Manager dialog located under the Help menu. When registering the product for the first time, select the **Register WhatsUp Event Alarm** option from the **Help** menu. If you are

adding licenses to a WhatsUp Event Alarm system that has already been registered, use the **Upgrade WhatsUp Event Alarm Licenses** option.

Before your purchase:

When you are evaluating WhatsUp Event Alarm for the first 30 days, you can use it to monitor logs on 50 different Windows computers. Registering and purchasing licenses is simple, and is handled by the License Manager dialog found under the Help menu. Whenever you need to add more product licenses, generate an encrypted key that you send to Ipswitch, Inc. After receiving the request, we will issue you a license upgrade key. If you would also like to use WhatsUp Event Alarm to monitor logs on Windows XP, Windows Vista, or Windows 7 workstations, we have special discounted license rates for workstations.

Visit the *Ipswitch Support Site* (<http://www.whatsupgold.com/support/index.aspx>) to make a purchase with a credit card, a purchase order, or to find resellers in your area.



Note: WhatsUp Event Alarm licensing is determined by the total number of computers you monitor logs on, not by the computers actually doing the monitoring.

After your purchase, but before your registration:

- 1 Shortly after processing your order, you will receive an email with instructions on how to activate your software over the Internet. This email contains your service number. Enter this service number, along with your name, organization, and email address in the **User Information** section of the License Manager. If you have multiple monitoring stations to configure (see below), repeat this step at each station.
- 2 Determine how many monitoring stations (i.e. separate WhatsUp Event Alarm installations) you want to set up. A monitoring station is a spare (but reliable) Microsoft Windows XP/2003/Vista/7/2008/2012 workstation or server where WhatsUp Event Alarm is installed. If you have a well-connected domain (10 MBit or greater LAN), we recommend only monitoring a maximum of 25 to 50 servers per monitoring station. The actual number may vary depending on how much auditing data your servers produce. We recommend setting up collection stations in evaluation mode **FIRST** to check load balancing before registering the software.



<Note 1> If you have standalone servers in a demilitarized zone or other isolated network, you can install WhatsUp Event Alarm to each standalone machine, configuring it to only monitor itself.



<Note 2> If you have WAN network links, it is best to set up a WhatsUp Event Alarm monitoring server at each of the remote ends, as to minimize traffic WAN traffic and not unduly delay notifications.

After all the different monitoring stations are configured appropriately, you can license each monitoring station independently by going to the **Help > Register WhatsUp Event Alarm** menu option, and preparing an Internet registration at that station.

In general, it is best to configure the stations first (since the products are fully functional during the first 30 days), and then register after the configuration.

Below is a hypothetical example of how your registration might look after configuring your monitoring stations:

Monitoring Station 1: 25 servers in domain / LAN

Monitoring Station 2: 1 server in a DMZ / Firewalled LAN

Monitoring Station 3: 1 server in a DMZ / Firewalled LAN

Monitoring Station 4: 5 servers in a domain / WAN remote end

In this scenario, we have 32 servers whose logs are being monitored, spread out over 4 monitoring stations. This means that you would submit a separate registration, one for each monitoring station, specifying the number of servers you will be watching at that station (e.g. 25 at Station 1, 1 at Station 2, 1 at Station 3, and 5 at Station 4).

The Ipswitch Fulfillment Team will respond with an unlocking code for each monitoring station once they receive your request.

After station configuration:

- 1 Indicate how many servers and workstations whose logs you want to monitor in the Request Licenses section of the License Manager.
- 2 If you are connected directly to the Internet, click the **Send request via the Web** button. Your license request is transmitted directly to Ipswitch, Inc. via the web.
- 3 If you are not directly connected to the Internet, click the **Export this request to an HTML file** button. An HTML file is generated at the location on disk you specify. Transport the HTML file via your network, or via removable media, to a machine with Internet access. Open the HTML file on your Internet-connected machine, and follow the instructions to request licenses via the web.



Note: If you need to activate the software inside a classified network, call Ipswitch at 781-676-5700 in order to activate the software over the phone.

- 4 After you receive an activation email, paste your response key into the Response Key field. After entering this key, click the **Unlock/Add Licenses** button. If the key is validated successfully, WhatsUp Event Alarm is registered with the number of licenses you requested.
- 5 Restart the WhatsUp Event Alarm Control Panel.
- 6 Repeat steps 4-8 for each monitoring station that needs licenses.

If you need to add licenses at a later date:

If, after registering WhatsUp Event Alarm, you discover you need more licenses, you can repeat the steps above to get a license upgrade response key, and increase the number of licensed computers.



Note: Only enter the number of licenses you want to add to the existing total to create a new license limit. The response you receive from Ipswitch will increase your number of licenses to the desired total.



Note: If you reset your request, you must send in a new request to Ipswitch. As a general rule, do not reset your request unless told to do so by a member of the Ipswitch fulfillment team.

WhatsUp Event Alarm's Feature Areas

WhatsUp Event Alarm's Main Interface (The Control Panel)

In order to make the administration of the WhatsUp Event Alarm system as simple as possible, WhatsUp Event Alarm ships with a GUI console called the WhatsUp Event Alarm Control Panel. From the control panel, you can add new logs to be monitored, edit the alarms and notifications for existing logs, and delete logs from the system. In addition, the WhatsUp Event Alarm Control Panel comes with a *rapid configuration tool* (on page 24) and step-by-step wizards that can help you *setup monitoring for multiple computers at once* (on page 26), adjust settings for currently monitored logs, *unify the audit policies* (on page 51) across Windows computers in your domains, and *unify the event log settings* (on page 54) (such as log size and retention intervals) across multiple machines.

Here are the 6 components of the WhatsUp Event Alarm Control Panel:

WhatsUp Event Alarm Control Panel Menu

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

File (on page 20)

Edit (on page 21)

View (on page 21)

Tools (on page 21)

Options (on page 22)

Help (on page 23)

Note: By right-mouse clicking on any log in the Event Logs Watched by WhatsUp Event Alarm List, you can pull up a context menu that mimics the commands of the File menu.

Toolbar

The toolbar serves as a quick access mechanism to many of the commands present in the six Control Panel menus. If you hover over any toolbar button, descriptive text will appear indicating what menu option the button controls.

Domain Chooser

The domain chooser appears as a pull-down list in the upper right hand corner of the control panel. The list contains the primary domain you chose when you installed the software, as well as any other domains that trust the primary domain. Selecting a new domain causes the Event Logs Watched by WhatsUp Event Alarm list to refresh, listing only the computers and logs registered in that specific domain.

Event Logs Watched by WhatsUp Event Alarm Tab

This listing shows you at a glance the event logs (and their corresponding computers) being monitored by the WhatsUp Event Alarm service. It also displays the last time any log was checked and the time it took to scan it for entries. You can sort this list by heading by clicking on any of the column headers.

Status Bar

This bar at the bottom of the Control Panel always indicates the number of event logs / syslogs being watched in a given domain, and the status of the WhatsUp Event Alarm Service.

Legal Information and License Agreement

Legal Information Including Patent and Trademark Notices

WhatsUp Event Alarm is Copyright © 2001-2015 Ipswitch, Inc. All Rights Reserved.

WhatsUp Event Alarm 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 Server 2012®, 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 Alarm 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., 83 Hartwell Avenue, 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

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.

Using WhatsUp Event Alarm Menu Options

In This Chapter

Using the File Menu.....	20
Using the Edit Menu.....	21
Using the View Menu.....	21
Using the Tools Menu.....	21
Using the Options Menu.....	22
Using the Help Menu.....	23

Using the File Menu

Use the File menu to manage log addition, editing, and deletion, audit policy access, general event log setting access, and a shortcut to the Microsoft Event Viewer.

File menu options

- § **Watch a New Log.** Opens the Log Watching Options dialog used to set WhatsUp Event Alarm to watch a new event log with specific alarm(s) (criteria) and alerting notifications.
- § **Edit the Selected Log.** Opens the Log Watching Options dialog used to reconfigure the alarms and notifications on the existing log highlighted in the Registered Log Listing.
- § **Delete the Selected Log(s).** Removes all selected logs in the Registered Log Listing from the WhatsUp Event Alarm monitoring database.
- § **Add a New Syslog Device.** Opens the Syslog Device Monitored dialog used to set WhatsUp Event Alarm to listen for syslog messages from computers and devices across your network, redirecting those messages into the Application log on the computer where WhatsUp Event Alarm is installed.
- § **Edit a Syslog Device.** Opens the Syslog Device Monitored dialog used to adjust the device name and IP address of the device that WhatsUp Event Alarm receives syslog messages from.
- § **Delete Syslog Device(s).** Removes all syslog devices selected from the WhatsUp Event Alarm monitoring database.
- § **Audit Policy.** Opens the Audit Policy dialog used to change the audit policies on the selected computer.
- § **Log Settings.** Opens the Log Settings dialog used to to change items like the event log size and method of retention for the selected computer and log.

- § **Event Viewer.** Opens the Microsoft Event Viewer and sets the focus to the selected computer.

Using the Edit Menu

Use the Edit menu to define events you want to monitor (e.g. alarms), group those events together (e.g. alarm bundles), define the way you want to be notified when the events happen (e.g. notifications), and export/import alarms to/from different WhatsUp Event Alarm installations.

Edit menu options

- § **Define Alarms.** Opens the Define Alarms dialog used to add, edit, and delete alarms scanning the information inside event logs.
- § **Define Alarm Bundles.** Opens the Define Alarm Bundles dialog used to create logical groupings of the alarms associated with different event logs.
- § **Define Notifications.** Opens the Define Notifications dialog used to add, edit, delete, and test notifications to alert you and others when particular event log alarms are triggered.
- § **Custom Notifications.** Opens the Custom Notifications dialog used to create custom notification formatting for email and popup messages.
- § **Export Alarms.** Opens the Export Alarms dialog used to save certain alarms and alarm groupings to a flat file. This is useful when you need to transfer alarm sets from one machine to another.
- § **Import Alarms.** Opens the Import Alarms dialog used to import certain alarms and alarm groupings from an alarm export file created by another WhatsUp Event Alarm installation.

Using the View Menu

Use the View menu to manually refresh your screen. F5 is the keyboard shortcut for the refresh operation.

Using the Tools Menu

The Tools menu contains several items designed to help you automate the process of monitoring event logs on your servers. In addition, you can use this menu to create WhatsUp Event Alarm compatible tables in Access, SQL, or other ODBC databases. You can open the WhatsUp Event Alarm Log Entries dialog to view events logged by the WhatsUp Event Alarm Service during its monitoring operations.

Tools menu options

- § **Rapid Configuration Setup.** Starts the *Rapid Configuration Tool* (on page 24), which is the easiest way to setup a monitoring strategy for multiple machines on your network.
- § **Step-By-Step Wizards.** Use the step-by-step wizards to automate the process of monitoring logs with WhatsUp Event Alarm, unify your audit policies, and unify your log settings across a domain. The wizards offer greater flexibility than the Rapid Configuration Tool mentioned above.
- § *Setup Monitoring for Multiple Computers at Once* (on page 26). Opens a series of dialogs you can use to monitor event logs from many different servers at once. You can select a certain number of computers, and then apply a uniform set of ignore events, alarms, and notifications to all of them.
- § **Adjust Settings for Currently Monitored Logs.** Opens a series of dialogs you can use to adjust the settings of logs already monitored by WhatsUp Event Alarm. Use this wizard to adjust your monitoring strategy as needed.
- § *Unify Audit Policies* (on page 51). Use this wizard to apply a uniform set of audit policies to multiple computers at once.
- § *Unify Log Settings* (on page 54). Instead of using the Microsoft Event Viewer to set event log settings (such as log size and retention) on each computer individually, you can use this wizard to automatically unify these settings on multiple computers at once.
- § **Database Helpers.** WhatsUp Event Alarm has a specific table format defined for storing event log entries. You can use the following menu items to create WhatsUp Event Alarm tables automatically in the databases you specify.
- § **Create Access Table(s).** Opens a dialog used to create WhatsUp Event Alarm-compatible tables in Microsoft Access databases.
- § **Create Microsoft SQL Server Table(s).** Opens a dialog used to create WhatsUp Event Alarm-compatible tables in Microsoft SQL Server.
- § *Creating Tables on Other ODBC Servers* (on page 66). Open a help topic that shows you how to create WhatsUp Event Alarm-compatible tables in other ODBC databases not natively supported by WhatsUp Event Alarm.
- § *View WhatsUp Event Alarm Log Entries* (on page 97). Opens the WhatsUp Event Alarm Log Entries dialog so you can view the events logged by the WhatsUp Event Alarm Service when monitoring your computers' event logs.

Using the Options Menu

Use the Options menu to configure WhatsUp Event Alarm default operating behaviors and settings, manage the WhatsUp Event Alarm Service and control how computer account information is obtained in the program.

Options menu options:

- § *WhatsUp Event Alarm Preferences* (on page 68). Opens a dialog you can use to customize WhatsUp Event Alarm's default settings for communication (email and pager), and also optimize the behavior of the WhatsUp Event Alarm Service, such as CPU utilization, port number, etc.
- § *Set WhatsUp Event Alarm Service Account* (on page 93). Changes the user account the WhatsUp Event Alarm Service runs under.
- § **Start the WhatsUp Event Alarm Service.** If the WhatsUp Event Alarm Service is stopped, attempts to restart it.
- § **Stop the WhatsUp Event Alarm Service.** If the WhatsUp Event Alarm Service is running, attempts to stop it.
- § *Set Default Domain Or Workgroup* (on page 73). Changes the default domain the WhatsUp Event Alarm Control Panel uses to obtain computer account information, as well as to discover other trusting domains.
- § *Manage Custom Domain to Computer Mappings.* Opens the Custom Domain Manager dialog, which in turn allows you to create fictitious custom domains for the purpose of organizing related computers. This is very useful in situations where you must monitor the event logs on computers in a handful of organizational units or workgroups.
- § *Retrieve Computer Names From* (on page 99). Opens the Computer Name Retrieval dialog, allowing you to specify how WhatsUp Event Alarm attempts to lookup computer account information over the network in domains and/or workgroups.
- § *Manage Custom Logs* (on page 97). 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.

Using the Help Menu

The Help menu contains links to the Ipswitch Network Management homepage, this help file, and allows you to register WhatsUp Event Alarm and/or upgrade your total number of computer monitoring licenses. You can also check for upgrades to the WhatsUp Event Alarm product in the Help menu.

Help menu options

- § **Visit Ipswitch Network Management Online.** Attempts to connect to the Ipswitch, Inc. home page using your default browser.
- § **Register WhatsUp Event Alarm / Upgrade WhatsUp Event Alarm Licenses.** Opens the License Manager dialog used to initially register WhatsUp Event Alarm and later add more computer licenses to the product.
- § **How Many Licenses Am I Using?.** WhatsUp Event Alarm determines the number of licenses in use versus the number of licenses you have purchased and activated on this installation of WhatsUp Event Alarm.
- § **WhatsUp Event Alarm Help File.** Displays the help file you are currently viewing.
- § **About WhatsUp Event Alarm.** Displays the current WhatsUp Event Alarm version and splash screen.

CHAPTER 3

Setting Up Monitoring for Multiple Computers

In This Chapter

Using the Rapid Configuration Tool.....	24
Setting-up Monitoring for Multiple Computers at Once (Step 1)	26
Setting-up Monitoring for Multiple Computers at Once (Step 2)	27
Setting-up Monitoring for Multiple Computers at Once (Step 3)	28
Setting-up Monitoring for Multiple Computers at Once (Step 4)	28
Setting-up Monitoring for Multiple Computers at Once (Step 5)	29
Setting-up Monitoring for Multiple Computers at Once (Step 6)	29

Using the Rapid Configuration Tool

The Rapid Configuration tool in WhatsUp Event Alarm is one of the most efficient ways to establish a log monitoring strategy for multiple computers in your workgroup, domain, or organizational unit. An administrator can choose the computers, logs, notification methods, and events to monitor for in one area. After a rapid configuration is run, it is saved to disk and can be summoned again in the future to be applied to new systems, or to simply reset everything back to its initial monitoring profile.

Additionally, rapid configurations that are saved after being used to establish a monitoring strategy can be treated as templates in two of WhatsUp Event Alarm's step-by-step wizards: *Setup Monitoring for Multiple Computers at Once* (on page 26) and *Adjust Settings for Currently Monitored Logs* (on page 30).

Step 1 - Select Computers and Logs to Monitor

Type a name for the rapid configuration - **The name you supply here will be the name that this rapid configuration is saved as for reuse in the future.**

Place a check by all computers you wish to monitor using the same rapid configuration. You can control how WhatsUp Event Alarm retrieves this list of computers by using the *Computer Name Retrieval* (on page 99) dialog.

Similarly, place a check by all log types on those computers that you wish to monitor.

Step 2 - Create and Select Notification Methods

If this is your first time running WhatsUp Event Alarm, create some new notifications that define how WhatsUp Event Alarm notifies you when key events are detected. Clicking the **Create/Manage Notifications** button opens the *Define Notifications* (on page 40) dialog, allowing you to create new ways of being notified. After creating your notifications, close the Define Notifications dialog. Your notifications now display in the Rapid Configuration tool. Place a check by any that you wish to use in the current configuration.

Step 3 - Send Out Notifications When (Basic Selection Mode)

Many common critical actions (e.g. errors/warnings, certain security events) are already predefined in the Rapid Configuration tool. Checking any of these actions makes WhatsUp Event Alarm automatically find the alarms that correspond to these activities in its database and associate them with your computers and logs. If you desire a higher level of granularity when it comes to determining events that must be monitored, check **Turn on Advanced Selection Mode**. This allows you to select individual alarms by hand, as well as allow to create your own alarms.



Note: The individual alarms associated with one or more activities remain checked after you turn on Advanced Selection mode. This convenience allows you to define and select custom alarms directly alongside more common log activities.

Step 3 - Select Event Activity to Monitor With Alarms (Advanced Selection Mode)

In advanced selection mode, you can check all the individual events you want to monitor for on computer logs. Click the **Create/Manage Alarms** button to define your own custom alarms corresponding to events you want to track. Alarms categorized under the Security Log are listed on the left-side listing, and alarms that have been categorized under all other log types appear in the right-side listing. Place a check by any you wish to include in the rapid configuration.

Configure! Click this button when you are satisfied with the monitoring profile you have created. After your selections are validated, WhatsUp Event Alarm:

- § Removes the existing monitoring configuration in WhatsUp Event Alarm for the selected computers and logs
- § Groups the security log alarms you have selected into an alarm bundle (e.g. using the format RapidConfigName_SecurityAlarms)
- § Groups the other log alarms you have selected into an alarm bundle (e.g. using the format RapidConfigName_OtherAlarms)
- § Associates the security log alarm bundle with all of the security logs on the computers you have selected for monitoring
- § Associates the other logs alarm bundle with all of the other logs on the computers you have selected for monitoring
- § Associates the notification methods with the monitored servers
- § Stops and restarts the WhatsUp Event Alarm Service so your new configuration takes immediate affect Saves your rapid configuration to disk for future editing or reuse



Note: Deselecting a computer or computers during a modification and re-execution of a Rapid Configuration profile does not remove the deselected computers from monitoring. To remove computers/logs from monitoring, you must delete them directly from the File menu.

If, in the future, you want to adjust what events WhatsUp Event Alarm monitors, you can add or remove alarms from either the Security Alarms alarm bundle or the Other Alarms alarm bundle using the Define Alarm Bundles Dialog found under the Edit menu. If you want to set up exclusionary alarms (e.g. "ignore events"), you may run the Adjust Settings for Currently Monitored Logs wizard, choosing a previous Rapid Configuration as a template and then adding Ignore Events in Step 3 of the wizard. Likewise, if you want to apply an existing rapid configuration to new servers that appear on your network, you may run the *Setup Monitoring for Multiple Computers at Once* (on page 26) wizard, and select a previous Rapid Configuration as a template in Step 1.

If you want certain events to only generate one particular notification, regardless of the computer being monitored, use the Specific Notification feature in the Define Alarms dialog.

Cancel. Closes the Rapid Configuration tool without saving changes.

Transferring Rapid Configurations From One WhatsUp Event Alarm Installation to Another

Rapid configurations are saved as .INI files in the RapidConfigs subfolder located underneath the WhatsUp Event Alarm Installation Directory (e.g. C:\Program Files\WhatsUp Event Alarm). To make rapid configurations available for use on an installation of WhatsUp Event Alarm on another machine, you may copy the corresponding .INI files from one RapidConfigs folder to another. Likewise, to remove a rapid configuration template, remove the corresponding .INI file in this folder.

Setting-up Monitoring for Multiple Computers at Once (Step 1)

The event logs from each computer chosen are added to the log monitoring database, and WhatsUp Event Alarm compares new events in these logs to the alarms you specify in Step 4. You can select multiple computers by holding down CTRL or SHIFT while selecting items with your mouse.

Select the servers and workstations you want to monitor with the WhatsUp Event Alarm Service. The event logs from each computer chosen are added to the log monitoring database. Moving computers into the right-side column targets them for monitoring. Moving computers to the left-side column excludes them from monitoring. When you are satisfied with your selections, click **Submit**.

Determine what alarms you want to re-categorize as ignore events so that these events are dropped if detected on the computer logs you are monitoring. Ignore events are useful in preventing certain types of events from producing notifications in WhatsUp Event Alarm.

To make an alarm serve as an event to ignore, drag it from the left side (Available Alarms column) of the dialog to the right side (Events To Ignore Column). If you have bundled up a group of alarms that you want to ignore, drag that alarm bundle from the left side (Available Alarm Bundles column) to the right side (Events To Ignore Column). Click the **Add** button to move selected alarms or alarm bundles from the left-side to the right side.

To stop using an alarm as an event to ignore, select it in the right side list, and then click **Remove**.

Determine what alarms you want to watch for on the computers and event logs you have selected.

To associate an alarm with this monitoring profile, drag it from the left side (Available Alarms column) to the right side (Associated Alarms Column). If you have bundled up a group of alarms that you want to use, drag that alarm bundle from the left side (Available Alarm Bundles column) to the right side (Associated Alarms Column). Click the **Add** button to move selected alarms or alarm bundles from the left side to the right-side.

To stop monitoring for an alarm or bundle of alarms, select it in the right side list, and then click **Remove**.

Determine which notifications you want to use to alert you when alarms are tripped on your servers.

To associate a notification with the monitoring profile, drag it from the left side (Available Notifications column) of the page to the right side (Associated Notifications Column). Click the **Add** button to move selected notifications from the left side to the right side.

To stop using a particular notification in this monitoring profile, select the notification in the right side list, and then click **Remove**.

Setting-up Monitoring for Multiple Computers at Once (Step 2)

In Step 2, select the servers and workstations you want to monitor with the WhatsUp Event Alarm Service. The event logs from each computer chosen are added to the log monitoring database, and WhatsUp Event Alarm compares new events in these logs to the alarms you specify in Step 4. You can select multiple computers by holding down CTRL or SHIFT while selecting items with your mouse. Moving computers into the right-side column targets them for monitoring. Moving computers to the left-side column excludes them from monitoring. When you are satisfied with your selections, click **Next** to continue.

Setting-up Monitoring for Multiple Computers at Once (Step 3)

In Step 3, determine what alarms you want to re-categorize as ignore events so that these events are dropped if detected on the computer logs you are monitoring. Ignore events are useful in preventing certain types of events from producing notifications in WhatsUp Event Alarm.

To make an alarm serve as an event to ignore, drag it from the left side (Available Alarms column) of the dialog to the right side (Events To Ignore Column). If you have bundled up a group of alarms that you want to ignore, drag that alarm bundle from the left side (Available Alarm Bundles column) to the right side (Events To Ignore Column). Click the **Add** button to move selected alarms or alarm bundles from the left-side to the right side.

To stop using an alarm as an event to ignore, select it in the right side list, and then click **Remove Ignore Event(s)**.



Note: To create new ignore events or modify the criteria for existing ignore events, Click the **Edit** menu, and then select **Define Alarms**.

Setting-up Monitoring for Multiple Computers at Once (Step 4)

In Step 4, determine what alarms you want to watch for on the computers and event logs you have selected.

To associate an alarm with this monitoring profile, drag it from the left side (Available Alarms column) of the dialog to the right side (Associated Alarms Column). If you have bundled up a group of alarms that you want to use, drag that alarm bundle from the left side (Available Alarm Bundles column) to the right hand side (Associated Alarms Column). Click the **Add** button to move selected alarms or alarm bundles from the left side to the right-side.

To stop monitoring for an alarm or bundle of alarms, select it in the right side list, and then click **Remove Alarm(s)**.



Note: To create new alarms or modify the criteria for existing alarms, click the **Edit** menu and then select **Define Alarms**.

Setting-up Monitoring for Multiple Computers at Once (Step 5)

Determine which notifications you want to use to alert you when alarms are tripped on your servers.

To associate a notification with the monitoring profile, drag it from the left side (Available Notifications column) of the dialog to the right side (Associated Notifications Column). Click the **Add** button to move selected notifications from the left side to the right side.

To stop using a particular notification in this monitoring profile, select the notification in the right side list, and then click **Remove Notification(s)**.



Note: To create new notifications or modify the criteria for existing notifications, click the **Edit** menu, and then select **Define Notifications**.

Setting-up Monitoring for Multiple Computers at Once (Step 6)

In Step 6, WhatsUp Event Alarm attempts to add the event logs on all of the computers you selected in Step 2 to the WhatsUp Event Alarm Service's log monitoring database. When finished, WhatsUp Event Alarm displays all successes and failures, ordered by individual computer. Double click a computer name to find out more about what caused a success or failure. When you are finished previewing the results, click **Exit** to return to the WhatsUp Event Alarm Control Panel.

The icon legend in the Results pane is as follows:



- Indicates an error occurred.



- Indicates a warning condition; the log on this computer may need additional attention.



- Indicates the operation was successful.

CHAPTER 4

Changing Monitoring on Multiple Computers

In This Chapter

Adjusting Settings for Currently Monitored Logs (Step 1)	30
Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 2)	31
Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 3)	32
Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 4)	33
Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 5)	34
Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 6)	35

Adjusting Settings for Currently Monitored Logs (Step 1)

Before adjusting the ignore events, alarms, and notifications on your currently monitored computers, select the type of log you want to modify on these currently monitored computers. The DNS Server, Directory Service, and File Replication Service logs are only available for adjustment on certain Windows servers. If none of your computers currently utilize these logs, choose a different log type before continuing.

Select the servers and workstations already being watched by WhatsUp Event Alarm whose logs' monitoring profile should be adjusted. You can select multiple computers by holding down CTRL or SHIFT while highlighting items with your mouse. Moving computers into the right column targets them for adjustment; moving computers back to the left column excludes them from adjustment.

Determine what alarms you want to re-categorize as ignore events so that these events are dropped if detected on the computer logs you are monitoring. Ignore events are useful in preventing certain types of events from producing notifications in WhatsUp Event Alarm.

To make an alarm serve as an event to ignore, drag it from the left side (Available Alarms column) to the right side (Events To Ignore Column). If you have bundled a group of alarms that you want to ignore, drag the alarm bundle from the left side (Available Alarm Bundles column) to the right side (Events To Ignore Column). Click the **Add** button to move selected alarms or alarm bundles from the left side to the right side. To stop using an alarm as an event to ignore, select it in the right side list, and then click **Remove**.

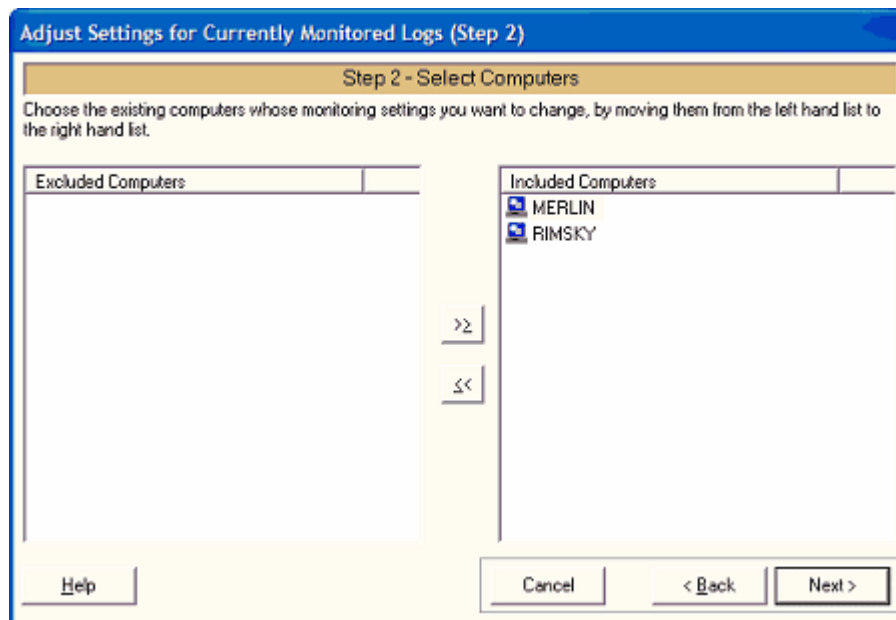
Determine what alarms you want to watch for on the computers and event logs you have selected for adjustment.

To associate an alarm with this monitoring profile, drag it from the left side (Available Alarms column) to the right side (Associated Alarms Column). If you have bundled a group of alarms that you want to use, drag that alarm bundle from the left side (Available Alarm Bundles column) to the right side (Associated Alarms Column). Click the **Add** button to move selected alarms or alarm bundles from the left side to the right side. To stop monitoring for an alarm or bundle of alarms, select it in the right side list, and then click **Remove**.

Determine which notifications you want to use to alert you when alarms are tripped on your servers.

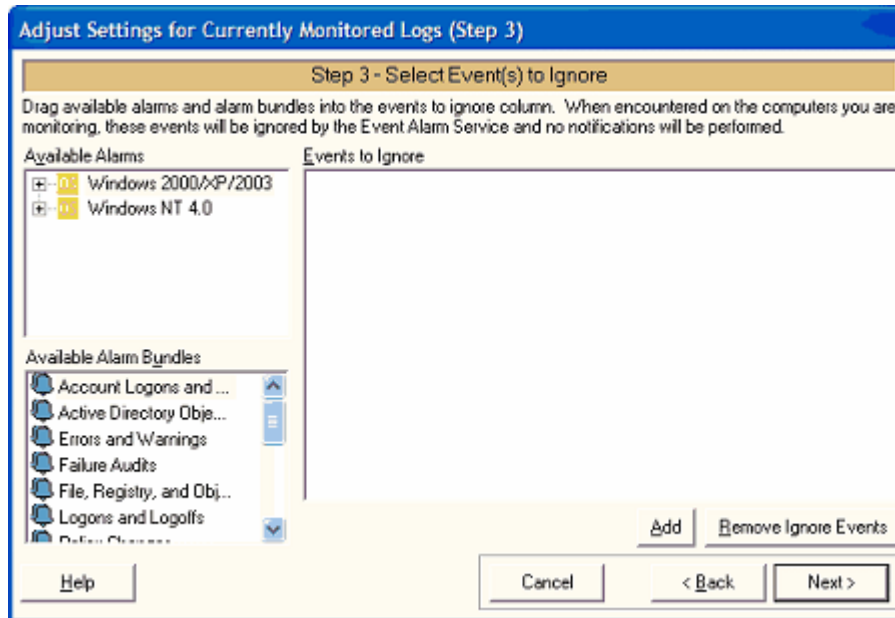
To associate a notification with this monitoring profile, drag it from the left side (Available Notifications column) to the right side (Associated Notifications Column). Click the **Add** button to move selected notifications from the left side to the right side. To stop using a particular notification in this monitoring profile, select the notification in the right side list, and then click **Remove**.

Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 2)



In Step 2, select the servers and workstations already being watched by WhatsUp Event Alarm whose logs' monitoring profile should be adjusted. You can select multiple computers by holding down CTRL or SHIFT while highlighting items with your mouse. Moving computers into the right column targets them for adjustment; moving computers back to the left column excludes them from adjustment. When you are satisfied with your selections, click **Next** to continue.

Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 3)



In Step 3, you determine what alarms you want to re-categorize as ignore events so that these events are dropped if detected on the computer logs you are monitoring. Ignore events are useful in preventing certain types of events from producing notifications in WhatsUp Event Alarm.

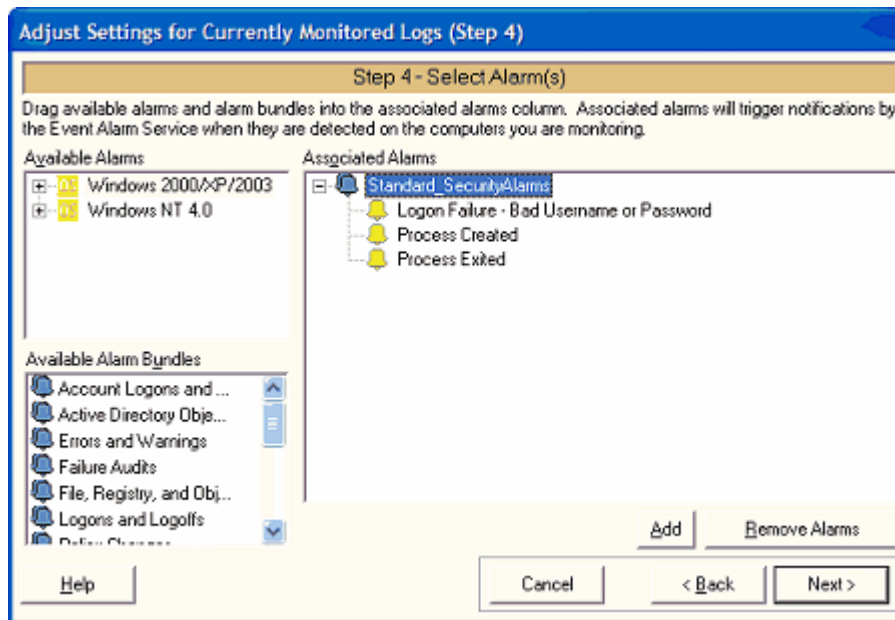
To make an alarm serve as an event to ignore, drag it from the left side (Available Alarms column) of the dialog to the right side (Events To Ignore Column). If you have bundled a group of alarms that you want to ignore, drag the alarm bundle from the left side (Available Alarm Bundles column) to the right side (Events To Ignore Column). Click the **Add** button to move selected alarms or alarm bundles from the left side to the right side.

To stop using an alarm as an event to ignore, select it in the right side list, and then click **Remove Ignore Event(s)**.



Note: To create new ignore events or modify the criteria for existing ignore events, click the **Edit** menu, and then select **Define Alarms**.

Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 4)



In Step 4, you determine what alarms you want to watch for on the computers and event logs you have selected for adjustment.

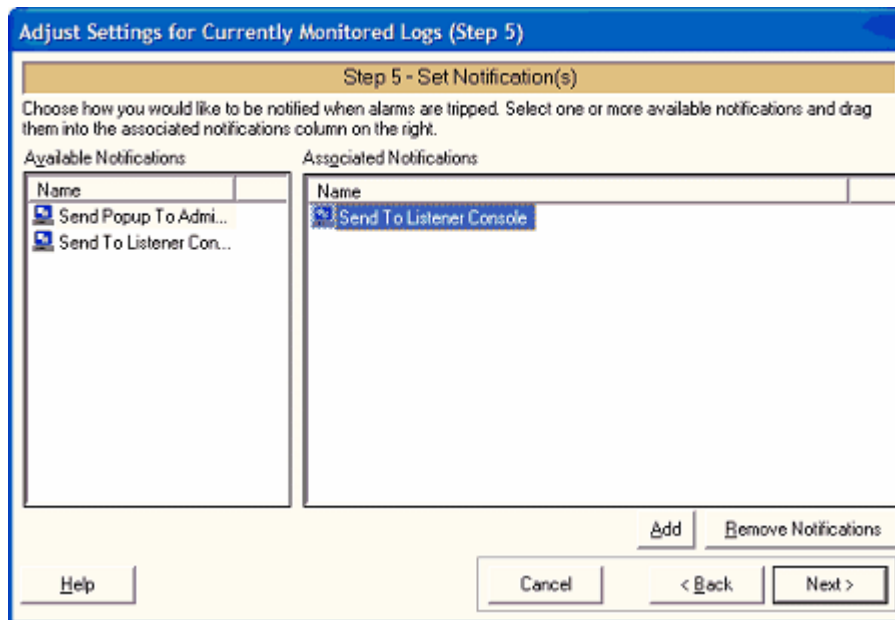
To associate an alarm with this monitoring profile, drag it from the left side (Available Alarms column) of the dialog to the right side (Associated Alarms Column). If you have bundled a group of alarms that you want to use, drag that alarm bundle from the left side (Available Alarm Bundles column) to the right side (Associated Alarms Column). Click the **Add** button to move selected alarms or alarm bundles from the left side to the right side.

To stop monitoring for an alarm or bundle of alarms, select it in the right side list, and then click **Remove Alarm(s)**.



Note: To create new alarms or modify the criteria for existing alarms, click the **Edit** menu, and then select **Define Alarms**.

Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 5)



Now its time to determine which notifications you want to use to alert you when alarms are tripped on your servers.

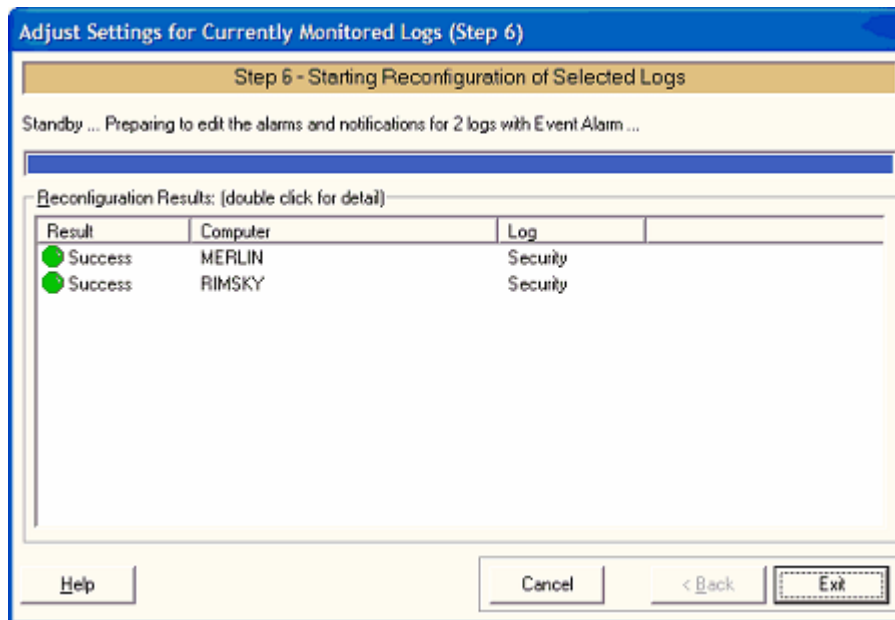
To associate a notification with this monitoring profile, drag it from the left side (Available Notifications column) of the dialog to the right side (Associated Notifications Column). Click the **Add** button to move selected notifications from the left side to the right side.

To stop using a particular notification in this monitoring profile, select the notification in the right side list, and then click **Remove Notification(s)**.






Note: To create new notifications or modify the criteria for existing notifications, click the **Edit** menu, and then select *Define Notifications* (on page 40).

Adjusting Settings for Currently Monitored Logs or Syslog Devices (Step 6)



In Step 6, WhatsUp Event Alarm attempts adjusting the monitoring properties of the specific event log on all of the computers you selected. When finished, WhatsUp Event Alarm displays all successes and failures, ordered by individual computer. Double-click a computer name to find out more details about what caused a success or failure when adjusting the log in the monitoring database. When you finish previewing the results, click the **Exit** button to return to the WhatsUp Event Alarm Control Panel.

The icon legend in the Results pane is as follows:

-  - Indicates an error occurred.
-  - Indicates a warning condition; the log on this computer may need additional attention.
-  - Indicates the operation was successful.

Monitoring Windows Event Logs

In This Chapter

Defining Custom Alarms	36
Defining Custom Syslog Alarms.....	38
Defining Alarm Bundles.....	39
Defining Notifications.....	40
Defining Custom Notifications	44
Monitoring Custom Event Logs	45
Watching Logs.....	46
Deleting Monitored Logs	49

Defining Custom Alarms

WhatsUp Event Alarm makes it easy to quickly add and save your own custom event log alarms (criteria) for watching specific event logs on your network. In addition, you can define alarms that serve as ignore events, in case there are certain types of events that you do not want to receive notifications for. Although WhatsUp Event Alarm ships with many predefined alarms, you can add your own as necessary.

To define custom alarms

- 1 From the WhatsUp Event Alarm control panel, click the **Edit** menu, and then select **Define Alarms**. The Define Alarms dialog appears.
- 2 Select the operating system associated with the type of alarm you want to define, and then click **Add** or click **Add Syslog** to define a syslog alarm.
- 3 The Define Alarms dialog changes to display the fields needed to define the alarm.
- 4 Complete the following fields:



Note: Only complete the fields you want WhatsUp Event Alarm to compare against new events when scanning event logs. Leave blank all fields that should be ignored. For example, do not enter None or N/A in the Category field.

Alarm Properties

- § **Source.** Type the registered application, hardware, or OS subsystem name associated with the events you want to filter. This field supports substring matching, so if you enter Log here, both the EventLog and NETLOGON sources are considered matches.

- § **Category.** Limits events by category. This field supports substring matching, so if you enter Logon here, both the Account Logon and Logon/Logoff categories are considered matches. In most cases, it is not necessary to filter by category.
- § **User.** Limits events by user account. This field supports substring matching, so if you enter IUSER here, both the IUSER_WEB1 and IUSER_WEB2 users are considered matches.
- § **Computer.** Limits events by computer. This field supports substring matching, so if you enter DMZ here, both the DMZ_SERVER1 and DMZ_SERVER2 computers are considered matches. In most cases, it is not necessary to filter by computer.
- § **Event ID.** Limits events by source-specific event number(ID).
- § **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**.
- § **Insert Tab.** Inserts "<TAB>" at the current position in the Description field. <TAB> represents an actual tab character at that point in the description string you are defining (e.g. Logon Type:<TAB>3)
- § **Insert CRLF.** Inserts "<CRLF>" at the current position in the Description field. <CRLF> represents an actual carriage return line feed sequence at that point in the description string.
- § **Type.** To scan by type, check only those types you want included in the alarm definition. If you do not want to scan by type, leave all check boxes blank.

Threshold and Notifications Properties



Note: You can require that WhatsUp Event Alarm only sends a notification if the alarm is tripped multiple times within a certain interval. This is useful for detecting things like intrusion attempts, imminent hardware failure, etc, without generating an abundance of false alarms.



Note: Leave these fields blank if you want to be notified every time an event matches the above criteria. The Threshold Limit must be 2 matching events or greater if you choose to set it up.

- § **Threshold Limit.** Specifies how many times an alarm must be tripped before notification is sent.
 - § **Threshold Timeout.** Specifies the maximum interval or window (in seconds) that related events must occur within before being discarded.
 - § **Specific Notifications.** If this field is set to a notification other than <NONE>, whenever this alarm is triggered on a monitored event log **ONLY** this notification fires. No other notifications associated with that computer and event log are fired. By setting a specific notification, you can have a one-to-one relationship between an alarm and a notification. This is useful if you only want a certain party to be notified when certain types of events occur.
- 5 Click **Save** to save your changes.

Alarm Explorer view field and button descriptions

- § **Add, Edit, and Delete WhatsUp Event Alarms.** This tree view control allows you to drill down and search for alarms by operating system, log type, and category. Double click to expand any item.
- § **Comment.** When an alarm is selected, the comment field displays a detailed description about its purpose.
- § **Add Syslog.** Sets up the dialog to receive a new syslog alarm definition from the information you provide.
- § **Add.** Sets up the dialog to receive a new alarm definition from the information you provide.
- § **Edit.** Loads the alarm definition of the selected alarm and allows you to modify its fields.
- § **Delete.** Deletes the selected alarm or category; a category can only be deleted if it has no child alarms.
- § **Close.** Closes the dialog.

Defining Custom Syslog Alarms

WhatsUp Event Alarm makes it easy to quickly add and save your own custom syslog alarms for watching on your network. Although WhatsUp Event Alarm ships with many predefined alarms, you can add your own as necessary.

To define custom syslog alarms

- 1 From the WhatsUp Event Alarm control panel, click the **Edit** menu, and then select **Define Alarms**. The Define Alarms dialog appears.
- 2 Select Syslog Devices, and then click **Add Syslog** to define a syslog alarm.
- 3 The Define Alarms dialog changes to display the fields needed to define the syslog alarm.
- 4 Complete the following fields:

Syslog Filter Properties

- § **Sender IP Address.** IP address for the alarm sender.
- § **Sender Hostname.** Hostname for the alarm sender.
- § **Priority (PRI) Value.** This number is included with every syslog message sent, regardless of who sent it and for what purpose. The number is always between 0 and 192 and is a combination of severity and facility.
- § **Facility.** This is derived from the Priority Code. You are only allowed to choose predefined values because they are predetermined by syslog standards.
- § **Severity Level.** This is derived from the Priority Code. You are only allowed to choose predefined values because they are predetermined by syslog standards.
- § **Header.** Syslog messages may include a header before the actual message itself; however, this is optional. The header should, but may not always, follow the RFC3164 standard. Therefore parsing is extended to allow for some variations of this format.

- § **Message.** The actual syslog message. Examples include status messages from a computer or security messages from a router.

Threshold and Notifications Properties



Note: You can require that WhatsUp Event Alarm only sends a notification if the alarm is tripped multiple times within a certain interval. This is useful for detecting things like intrusion attempts, imminent hardware failure, etc, without generating an abundance of false alarms.



Note: Leave these fields blank if you want to be notified every time an event matches the above criteria. The Threshold Limit must be 2 matching events or greater if you choose to set it up.

- § **Threshold Limit.** Specifies how many times an alarm must be tripped before notification is sent.
- § **Threshold Timeout.** Specifies the maximum interval or window (in seconds) that related events must occur within before being discarded.
- § **Specific Notifications.** If this field is set to a notification other than <NONE>, whenever this alarm is triggered on a monitored event log **ONLY** this notification fires. No other notifications associated with that computer and event log are fired. By setting a specific notification, you can have a one-to-one relationship between an alarm and a notification. This is useful if you only want a certain party to be notified when certain types of events occur.
- 5 Click **Save** to save your changes.

Defining Alarm Bundles

One of WhatsUp Event Alarm's most powerful features is its ability to define and maintain alarm bundles. Alarm bundles are logical sets of alarms that serve a common monitoring purpose. For example, an Account Management alarm bundle might contain password change alarms, group membership change alarms, etc.

When you associate an alarm bundle with one or more event logs, WhatsUp Event Alarm automatically scans incoming events in those logs to see if they match any of the alarms present in the bundle. Later, if you need to expand or reduce the number of alarms that monitor for particular activity on your servers, you can adjust the alarm bundle membership, as opposed to having to adjust all of the alarm mappings on all of the different servers' logs you are monitoring. This greatly reduces the time involved in changing the monitoring profile for multiple computers on your network.

You may also use alarm bundles to group ignore events. In most situations, organizations do not necessarily know what they want to ignore in their event logs until they deploy a monitoring solution. By creating alarm bundles for storing particular events you wish to ignore, you can continue to add additional events to that grouping as needed.

If you use the Rapid Configuration Tool to setup a monitoring strategy for your servers, it automatically places security alarms in a security alarm bundle and all other alarms in an other alarms bundle.

To define an alarm bundle, click the **Edit** menu, and then select **Define Alarm Bundles**.

When managing alarm bundles already defined

- § **Add.** Displays a list of alarms used to assemble a new alarm bundle.
- § **Edit.** Allows the user to add or remove alarms in an existing alarm bundle.
- § **Delete.** Removes the selected alarm bundle. This does not remove the individual alarms grouped in the alarm bundle, just the alarm bundle itself.

When adding or editing alarm groups

The easiest way to add alarms to an alarm bundle is to drag them from the left side column (Available Alarms) to the right side column (Alarms Associated With This Bundle). If you drag an entire alarm category from the left side to the right side, all alarms under that category are added. To remove one or more alarms from the bundle, highlight the alarms on the right side, and then click **Remove Alarm(s)**.

- § **Available Alarms.** displays all defined alarms available in WhatsUp Event Alarm, grouped by Operating System, Log Type, and Category.
- § **Alarms Associated With This Bundle.** displays all alarms currently in the selected alarm bundle.
- § **Add.** Associates the selected alarm in the left column with the current alarm bundle.
- § **Remove Alarm(s).** Removes the selected alarms from the current alarm bundle.
- § **Bundle Name.** Use this field to enter or edit the name of the alarm bundle you are creating or editing.
- § **Save.** Saves changes to the alarm bundle.
- § **Abandon.** Cancels the current add or edit operation on the alarm bundle.

Defining Notifications

WhatsUp Event Alarm provides many ways to alert an administrator when an alarm is tripped on a computer's event log. Notification options include:

- § Email notifications
- § Popup messages (utilizing the Messenger service on XP/2003 machines) to specific NetBIOS computer names and user names
- § Pager-based notifications that use a TAPI-compliant data modem and numeric codes
- § Forwarding events as syslog messages to a syslog host server, or to the WhatsUp Event Alarm Listener Console
- § NetBIOS broadcast notifications to all administrators running the WhatsUp Event Alarm Listener Console in the same domain
- § Placing each event that triggered an alarm into an Access or ODBC database.

To define notifications, click the **Edit** menu, then select **Define Notifications**.

Which Notification Method Should I Use?

The most robust notification method is email. WhatsUp Event Alarm is specially designed to be capable of generating hundreds of email messages per second using a multithreaded architecture. Email can be queued by SMTP servers pending delivery, and it is sent over a connection-oriented protocol (TCP/IP). Network popups are simple and convenient, but if too many are generated and sent to the same recipient, an XP/2003 desktop can only display a certain number (between 6-12) at a time before some messages are dropped. Network popups are also not necessarily connection-oriented, and therefore, delivery is not guaranteed. Syslog messages are also sent with a multithreaded architecture like email messages, but are not connection-oriented because they travel over the network as UDP packets. However, they are more easily routable than NetBIOS popup messages or broadcast notifications. Pager notifications should be reserved for the most critical events on the most critical logs. This is because a modem cannot communicate with multiple pagers at once, and at best, can only send out two to three notifications per minute. Because most pagers/cell phones now support text messaging with email addresses, email can often be used to deliver messages to wireless devices and is preferred over traditional numeric pager messages.

Every time specific notifications are sent out (e.g. email, network popup, syslog, or pager), the WhatsUp Event Alarm Service can be instructed to broadcast the same notification to all WhatsUp Event Alarm Listener Console clients listening in its primary domain. Multiple administrators can install and run the WhatsUp Event Alarm Listener Console application, and each one is informed via the broadcast message when an alarm has been tripped.



Note: You can control whether this feature is enabled in the WhatsUp Event Alarm Preferences dialog.

If you do not need to be informed immediately about a certain type of event on your network but would like to review the data that was detected on a regular basis, you can define a notification that places event log data into an Access or ODBC database. Then, you can retrieve that data via queries you define, or you can use Ipswitch's specialized analysis tool, WhatsUp Event Analyst (<http://www.eventanalyst.com>).

Note: You can combine notification types into a single defined notification in WhatsUp Event Alarm. For instance, you may want detected events sent to the WhatsUp Event Alarm Listener Console running on your desktop, but also placed into a SQL database. Check and configure both of these types when defining a single notification.

Are Undeliverable Notifications Queued? If WhatsUp Event Alarm cannot send a notification (e.g. inaccessible SMTP server), it queues the notification and attempts immediate redelivery (e.g. approximately a minute). If a second delivery attempt fails, it queues the message again and waits 20 minutes before retransmission. After a third failed attempt, it deletes the notification and places a warning event in the application log on the machine where WhatsUp Event Alarm is running.

Notification Chooser View

- § **Add, Edit, and Delete Event Notifications.** Select the notification you want to edit, delete, or test using this list view control.
- § **Add.** Sets up the dialog to receive a new notification definition from the information you provide.

- § **Edit.** Loads the definition of the selected notification and allows you to modify its notification methods.
- § **Delete.** Deletes the selected notification.
- § **Test.** Loads the selected notification and performs a test of all notification methods present in the notification definition. The successes/failures of the notification methods are noted in the resulting dialog. This is an excellent way to test whether notifications are sent out as expected.
- § **Close.** Closes the dialog.

Single Notification Add/Edit View

Check/uncheck (enable/disable) the particular notification methods on the various tabs you want to use in the notification you are defining. A single defined notification can utilize multiple notification methods as needed.

General Tab

- § **Notification Name.** Choose a name to remember this notification by for future use (e.g. when you associate it with a particular computer event log).
- § **Use Custom Notification Formatting for E-mail and Popup Messages.** Check this box and choose a custom notification from the list if you want to use a custom format for email and popup messages. Custom notifications are useful when you need to send e-mail messages to devices that have a limit on incoming character data (e.g. cell phones). See the *Defining Custom Notifications* (on page 44) help topic for more details.

E-Mail

E-mail Recipients. Type the email address(es) of the parties that will receive an email alert from WhatsUp Event Alarm. Separate multiple e-mail addresses with commas; do not put spaces in between the commas.

Pager

- § **Phone Number.** When defining a pager alert, type in the actual phone number (including area code, or dial-out extension as necessary) being dialed by the modem (e.g. *9, 18005555555)
- § **Pager String.** Enter an appropriate number of commas (which are interpreted as pauses as the pager service is preparing to receive a numeric message), and then the actual numeric message you want to accompany this notification (e.g. ,,,,,411 or ,,,,911).

Popup

Network Name. For a network popup message, enter the NetBIOS computer name where you want the message delivered. For the most consistent and reliable delivery, it is recommended that you use the computer name.



Note: If you enable network popups, ensure that the Messenger service is running on both the computer where WhatsUp Event Alarm is installed and the computer where network popups are sent. Starting with Microsoft Windows Vista and Windows Server 2008, network popups are no longer supported.

§ Syslog Servers and Listener Console Messages

- § **Syslog Server(s) or Listener Console(s).** Type the network name, IP address, or fully-qualified domain name of a central syslog host server or system running the WhatsUp Event Alarm Listener Console that should receive forwarded events. You can also use limited broadcast IP addresses so that any machine running the WhatsUp Event Alarm Listener Console on a certain subnet can receive these notifications (e.g. 192.168.1.255). To send to multiple systems, you can separate each network name/IP address/fully-qualified domain name with a comma (e.g. WKSTN2,10.32.2.31,ftp.mydomain.com). Do not place spaces in between the commas and the system names.
- § **UDP Port.** Choose a UDP port number that the syslog server(s) or listener console(s) above receive messages on. The default UDP port for syslog host servers is 514, and the default port for the WhatsUp Event Alarm Listener Console program is 6260. You can also type in your own port number if so desired.
- § **Priority Code.** Enter the numeric code of the priority you want to attach to outgoing syslog messages. The number is a combination of a syslog facility and level value. The numeric value is used only by syslog host servers; the WhatsUp Event Alarm Listener Console ignores it.



Note: If the Use RFC3164 formatting when sending syslog messages option is checked in the WhatsUp Event Alarm Preferences dialog, you must select a non-zero priority code above to ensure proper formatting. Conversely, if you are sending messages to the WhatsUp Event Alarm Listener Console, the Priority Code must be set to zero.

- § **Build Priority.** Opens the *Build Priority Dialog* (on page 95), and allows you to build a priority code by choosing a syslog facility and level. This information is only used by syslog host servers.

Database

- § **DB Connection.** Use the Browse (...) button to select either a Microsoft Access database (.mdb file) or ODBC data source where the event information contained in this alarm will be stored. If you choose Microsoft Access, you can browse to a directory where you want to create a new .MDB file, type in the new file name, and WhatsUp Event Alarm automatically creates the .MDB file on disk, even if Microsoft Access is not installed.
- § **Table Name.** Type a new table name or choose an existing WhatsUp Event Alarm-compatible database table where the event information contained in the triggering alarm will be stored. If you type in a new table name, WhatsUp Event Alarm attempts to automatically create it for you in the data source (Microsoft Access / Microsoft SQL Server only).
- § **Save.** Stores your new or updated notification in the WhatsUp Event Alarm database.
- § **Abandon.** Closes the dialog without saving changes.

Defining Custom Notifications

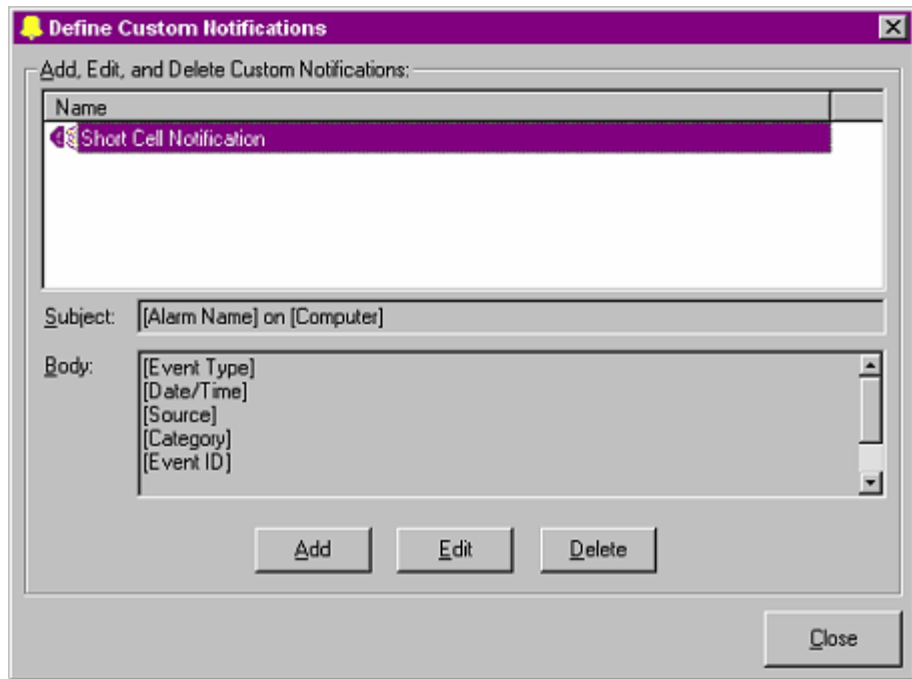
In some situations, you may want to customize the framing and the information contained in network popup and email notifications. The Custom Notifications dialog allows you to create a specific framework for both the subject and body of such notifications, including which parameters (e.g. the log type, date/time, Event ID, etc) to include in the message.

An example of a custom notification is one designed for email notifications sent to a cell phone. Many cell phone providers limit the amount of data displayed from an email message; therefore, a custom notification designed for a cell phone should only include certain parameters in an effort to conserve space.

Another example is the desire to send notifications as SMS messages to mobile devices. You can create a custom notification that places key fields in the Subject line of the notification, and then build a notification that uses that custom notification and sends an email message to an email-to-SMS gateway email server.

After one or more custom notifications are defined, you may attach a custom notification to a notification definition in the Define Notifications dialog.

To define custom notifications, click the **Edit** menu, then select **Custom Notifications**.



- § **Custom Notification List.** Displays a listing of all custom notifications currently maintained by WhatsUp Event Alarm. Select any notification from this list to display its subject and body framework in the fields below the list.
- § **Subject.** Displays the subject framework for the currently selected custom notification.
- § **Body.** Displays the body framework for the currently selected custom notification.

- § **Add.** Allows adding a new custom notification.
- § **Edit.** Allows editing the framework of an existing custom notification.
- § **Delete.** Deletes the currently selected custom notification.
- § **Close.** Closes the Custom Notification dialog.

The screenshot shows a Windows-style dialog box titled "Define Custom Notifications". It contains a "Custom Notification Details:" section with three input fields: "Name:" (containing "Short Cell Notification"), "Subject:" (containing "%0 on %8"), and "Body:" (containing a list of parameters: %2, %3, %4, %5, %6, %7, %9). Below these fields is a "Parameters:" section with a dropdown menu showing "%0 - Alarm Name" and an "Insert" button. At the bottom right are "Save" and "Abandon" buttons.

When adding or editing custom notifications

- § **Name.** Type a descriptive name for the custom notification you are defining.
- § **Subject.** Using the parameters listing below with the **Insert** button, construct a custom subject framework. You may intersperse the parameters you select with free form text.
- § **Body.** Using the parameters listing below with the **Insert** button, construct a custom body framework. You may intersperse the parameters you select with free form text.
- § **Parameters.** Represents critical components of the event and alarm that generated the notification. You may choose as many or as few as you like when building subject and body frameworks. WhatsUp Event Alarm replaces these parameter strings with the actual event and alarm data when it generates your notification.
- § **Insert.** Inserts the currently selected parameter into the subject or body fields (whichever has current focus) at the previous mouse position.
- § **Save.** Saves your newly created or recently edited custom notification.
- § **Abandon.** Cancels the current add or edit operation on the custom notification.

Monitoring Custom Event Logs

Traditionally, there are six standard Windows Event Logs present on Microsoft Windows server and workstation operating system; the Application, System, and Security logs appear

on all Windows operating systems, and the DNS Server, Directory Service, and File Replication Service logs can be found on server operating systems.

However, various third-party applications are now creating their own custom Windows event logs for error tracking and reporting. WhatsUp Event Alarm gives you the option of defining these custom event logs so they can be collected alongside the standard logs mentioned above.

To define a custom event log for use within WhatsUp Event Alarm, select the **Manage Custom Logs** option from the **Options** menu. You can then browse to various computers to view the custom Windows event logs present on any given system. If you want to create a custom event log available for monitoring by WhatsUp Event Alarm, select it from the list and click the **Add Custom Log** button. Similarly, if you no longer wish to see a particular custom event log as available throughout WhatsUp Event Alarm, select it from the **Custom Event Logs Defined** list and click the **Remove Custom Log** button.

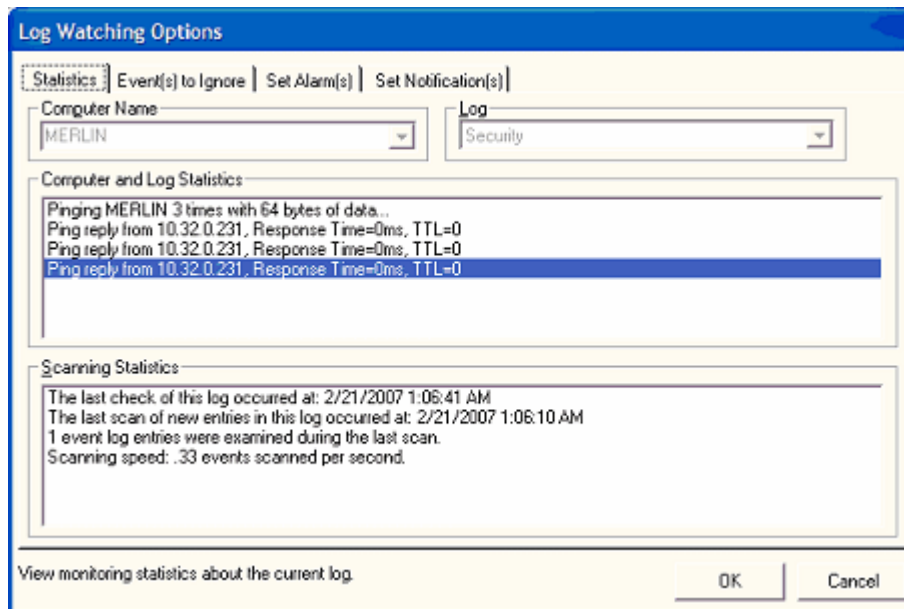
In some cases, you may not be able to enumerate custom logs on a remote machine (e.g. the Remote Registry Service may be disabled, for instance), so you can also choose to add a custom log manually by clicking the **Add Custom Log Manually** button. In the resulting dialog, specify both the **Custom 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 Vista and later operating systems, the internal name may be different, and you will need to determine the internal name by finding that logs subkey under the HKLM\System\CurrentControlSet\Services\EventLog section of that computer's registry.

Watching Logs

Use the Log Watching Options dialog to:

- § Begin monitoring a new computer event log for specific activity
- § Change alarms and notifications on a log you are already monitoring

- § View statistics on a log you are already monitoring.



To open the Log Watching Options dialog, click the **File** menu, and then click **Watch a New Log**.

Log Watching Options dialog field descriptions:

Choose Computer and Log Tab

- § **Computer name.** Choose a computer from the list. You can only select computers from the currently active domain in this list box. This field is disabled when you are editing an existing log.
- § **Log.** Choose Application, System, Security, DNS Server, Directory Service, or File Replication Service to determine which event log you want to monitor. This field is disabled when you are editing an existing log.

Statistics Tab

Double-click a log in the WhatsUp Event Alarm Control Panel, or select **Edit the Selected Log** from the **File** menu allows you to view recent statistics about monitoring operations against that log. Specifically, you can view:

- § Whether the computer responds to ICMP Echo (ping) requests
- § The operating system the computer is running
- § The number of log entries in that particular event log
- § The last time the log was checked for new entries
- § The last time the log was scanned because new entries were detected
- § The number of log entries traversed during the last scan
- § The scanning speed during the last scanning operation

Event(s) to Ignore Tab

By definition, events to ignore are simply defined alarms that serve a different purpose, namely, to ignore certain types of events present in your computer event logs. For example, you may be interested in being notified when logon failures occur in your security logs. But, there may be ongoing network issues where one user account (perhaps a service account) frequently generates logon failures. Because this represents a false positive, you should define an alarm with a logon failure Event ID, and the user account generating the false positive. Then, add this particular alarm to the Event(s) to Ignore list. By doing so, no notification is generated when this particular event is detected, but all other logon failures continue to generate notifications.

To make an alarm serve as an event to ignore, drag it from the left side (Available Alarms column) of the dialog to the right side (Events To Ignore Column). If you have bundled a group of alarms that you want to ignore, drag that alarm bundle from the left side (Available Alarm Bundles column) to the right side (Events To Ignore Column). Click the **Add** button to move selected alarms or alarm bundles from the left side to the right side.

To stop using an alarm as an event to ignore, select it in the right side list, and then click **Remove Ignore Event(s)**.

Set Alarm(s) Tab

These are the event criteria, that, when detected by WhatsUp Event Alarm, cause the WhatsUp Event Alarm Service to send out appropriate notifications.

To associate an alarm with a computer event log, drag it from the left side (Available Alarms column) of the dialog to the right side (Associated Alarms Column). If you have bundled a group of alarms that you want to use, drag that alarm bundle from the left side (Available Alarm Bundles column) to the right side (Associated Alarms Column). Click the **Add** button to move selected alarms or alarm bundles from the left side to the right side.

To stop monitoring for an alarm or bundle of alarms, select it in the right side list, and then click **Remove Alarm(s)**.



Note: To create new alarms or modify the criteria for existing alarms, click the **Edit** menu and then select **Define Alarms**.

Set Notifications Tab

When an alarm is tripped on a particular event log, WhatsUp Event Alarm checks to see what notifications are associated with that event log and sends alerts via the relevant notification methods.

Deleting Monitored Logs

If you need to stop monitoring one or more logs inside WhatsUp Event Alarm, select the log in the WhatsUp Event Alarm Control Panel, and then select the **Delete the Selected Log(s)** option from the **File** menu.

CHAPTER 6

Adjusting Audit Policies on Workstations and Servers

In This Chapter

Adjusting Audit Policies.....	50
Unifying Audit Policies (Step 1).....	51
Unifying Audit Policies (Step 2).....	51
Unifying Audit Policies (Step 3).....	51

Adjusting Audit Policies

WhatsUp Event Alarm allows the administrator to adjust audit policies on individual machines, and also provides the administrator with the ability to unify the audit policies of many workstations and servers at once by using a wizard. This can be useful when organizations do not use Group Policy to control audit settings, or are managing computers in one or more workgroups instead.

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 is automatically shifted to the domain that domain controller manages.



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 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 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).

- § **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.
- § **Object Access.** Audit attempts to access securable objects, such as files.
- § **Privilege Use.** Audit this to see when someone performs a user right.
- § **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 2000/XP/2003/Vista/2008).** Audit attempts to access the directory service.
- § **Logon Events (Windows 2000/XP/2003/Vista/7/2008/2012).** Audit this to see when someone has logged on or off your computer (either while physically at your computer or remotely).

Unifying Audit Policies (Step 1)

In Step 1, select the stand alone servers and workstations you want to unify audit policies on. You can group select computers by holding down CTRL or SHIFT while selecting items with your mouse. Use the >> button to move them to the right-side to include them in the unification process. Use the << button to move them to the left-side to exclude them from the unification process. When you are satisfied with your selections, click **Next** to continue.



Note: Domain controllers are purposefully not displayed in this list. If you want to adjust audit policies for an entire domain, choose the Primary Domain Controller in the WhatsUp Event Alarm Control Panel, and click the Audit Policy menu option from the File menu.



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.

Unifying Audit Policies (Step 2)

In Step 2, choose whether you want to enable auditing on the machines you selected in Step 1, and if enabled, which categories you wish to audit.

Unifying Audit Policies (Step 3)

In Step 3, WhatsUp Event Alarm attempts to unify the audit policies on all of the computers you selected in Step 1. When finished, WhatsUp Event Alarm displays the successes and failures, ordered by individual computer. Double click a computer name to find out more

about what caused a success or failure. Click **Exit** when you are ready to return to the WhatsUp Event Alarm Control Panel.

The icon legend in the Results pane is as follows:



- Indicates an error occurred.



- Indicates the operation was successful.

CHAPTER 7

Adjusting Log Retention and Size Settings on Computers

In This Chapter

Adjusting Log Retention and Log Size Settings	53
Unify Log Settings (Step 1)	54
Unify Log Settings (Step 2)	54
Unify Log Settings (Step 3)	55
Unify Log Settings (Step 4)	55

Adjusting Log Retention and Log Size Settings

WhatsUp Event Alarm allows the administrator to adjust log retention and log size settings on individual machines, and also provides the administrator with the ability to unify the log retention settings and log sizes of many workstations and servers at once by using a wizard. This can be 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.

Use the Log Settings dialog to set individual machine event log file sizes and retention properties. To open the Log Settings dialog, select a computer in the WhatsUp Event Alarm Control Panel, and choose the **Log Settings on \COMPUTERNAME** option from the **File** menu.

Log Settings dialog box descriptions:

- § **Log Type.** Use this list to choose an individual event log from the computer on which you want to modify settings.
- § **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 the Microsoft Windows operating system can take. One is to begin overwriting all events from the oldest and working forward. This is a relatively low security setting, since 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. WhatsUp Event Alarm's sister application, WhatsUp Event Archiver, empowers you to choose this last option because it can automatically archive the logs when they are nearing their maximum size.

Unify Log Settings (Step 1)

It is important to choose appropriate log retention and size settings for different types of servers. Log retention settings, which determine when events are overwritten in an event log, if ever, play an important role in security. If your retention policy is too liberal, critical log entries may be overwritten by the EventLog service, never to be seen again. Also, you must choose a log size that is big enough to accommodate the levels of auditing happening on a machine, but that is not so big as to make periodic analysis too time consuming.

To streamline the chore of standardizing log file sizes and retention settings, WhatsUp Event Alarm allows administrators to push similar retention settings and log sizes to member servers and workstations in a domain in one operation. To unify these settings on your member servers and workstations, invoke the Unify Log Settings Wizard, located in the Tools menu under Step-By-Step Wizards.

Choose a domain and one or more event log types that receive the same log settings, such as a uniform file size and retention policy. The DNS Server, Directory Service, and File Replication Service logs are only available on certain Windows servers. If you select them in addition to the Application, System, and Security logs, ensure that you limit your computer selection to only Windows servers in Step 2. At the completion of this wizard, WhatsUp Event Alarm applies the log settings you choose to the logs on the computers you select in Step 2. When you are finished, click **Next** to continue.



Note: If you are running a Microsoft Windows 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.

Unify Log Settings (Step 2)

In Step 2, select the servers and workstations whose log settings you would like to unify. You can group select computers by holding down CTRL or SHIFT while selecting items with your mouse. Use the >> button to move them to the right side includes them in the unification process. Use the << button to move them to the left side excludes them from the unification process. When you are satisfied with your selections, click **Next** to continue.


Unify Log Settings (Step 3)

After you have selected the computers and event logs that you want to unify log settings on, use this step to define the settings you want to apply to all of them. For more information about these settings, refer to the Log Settings Dialog help topic.

Unify Log Settings (Step 4)

In Step 4, WhatsUp Event Alarm attempts to unify the log settings on all of the logs and computers you selected in Steps 1 and 2. When finished, WhatsUp Event Alarm displays the successes and failures, ordered by individual computer. Double click a computer name to find out more detail about what caused a success or failure. Click **Exit** when you are ready to return to the WhatsUp Event Alarm Control Panel.

The icon legend in the Results pane is as follows:

 Indicates an error occurred.

 Indicates the operation was successful.

CHAPTER 8

Monitoring Syslog Devices

In This Chapter

Changes in Syslog Support Between WhatsUp Log Management v9 to WhatsUp Log Management v10.....	56
Syslog Support in WhatsUp Event Alarm	58
Adding a New Syslog Device.....	61

Changes in Syslog Support Between WhatsUp Log Management v9 to WhatsUp Log Management v10

WhatsUp Log Management v10 introduces many new features related to the receipt and processing of Syslog messages. Below are the most significant changes made to the product between the two versions:

- § The Syslog Listener Service now has extended capabilities. In v9, it was a component of WhatsUp Event Alarm, and it placed incoming Syslog messages in the local Windows Application Event Log. Now, it has the ability to process Syslog messages in different ways, depending on which Syslog handlers you enable in the WhatsUp Log Management Suite Service Manager.
- § If you enable the Syslog Event Archiver handler, the Syslog Listener Service redirects incoming Syslog messages into the new, custom Archived Syslog Messages event log on the local machine. You can optionally save/clear/export this special custom log on a regular basis in the WhatsUp Event Archiver application. This is the best mechanism for consolidating all of your Syslog messages into a single log file and/or central database on a regular basis.
- § If you enable the Syslog Monitor handler, the Syslog Listener Service passes incoming Syslog messages directly to the WhatsUp Event Alarm Scanning Engine. To specify rules/criteria to evaluate against incoming Syslog messages, from the WhatsUp Event Alarm application, click the **Edit** menu, and then select **Define Alarms**. Choose **Add Syslog** to define one or more Syslog-specific alarms. From the Authorized Syslog Devices tab, add one or more Syslog devices you want monitored, and associate the above alarm(s) with the log, allowing notifications to fire when specified types of Syslog messages are received.



Note: Pre-version 10, to trigger Syslog-based alarms in WhatsUp Event Alarm, you had to define Windows-based alarms for incoming Syslog messages and monitor the local Application event log. This is no longer necessary. Define the appropriate Syslog alarms and associate them directly with each Syslog device as needed in the WhatsUp Event Alarm Scanning Engine.

- § The Syslog Listener Service can now receive Syslog messages over IPv4 and IPv6 networks. It can also receive connectionless messages using UDP or connected-based messages sent via TCP. You can control the ports used by each protocol and transmission mechanism in the WhatsUp Log Management Suite Service Manager. From the Service Manager, click the **Options** menu in the Service Manager, and then select **Configure Syslog Ports**.
- § If you have recently upgraded your version of WhatsUp Event Alarm, and in your previous version you were monitoring incoming Syslog messages, complete the following tasks to resume Syslog monitoring:
- § Redefine your previous Syslog alarms (formerly written as special criteria placed in the Windows Event Log) into new Syslog-specific alarms. (e.g. **Edit** menu > **Define Alarms** > **Add Syslog**).
- § Double-click each device in the **Authorized Syslog Devices Being Monitored** tab, and select the alarm(s) and notification(s) you want to fire when certain types of Syslog messages arrive from each device. Click **OK** to save your changes.

- § Just as WhatsUp Event Alarm has special Syslog-specific alarms used to monitor Syslog messages as they arrive from different devices, WhatsUp Event Analyst allows you to define Syslog-specific filters (both Basic and Advanced). You can use these filters to build queries and reports against Syslog messages consolidated in the local Archived Syslog Messages EVT(X) log, or the Archived Syslog Messages database table link, if you are storing your Syslog messages in Microsoft SQL. Furthermore, you can target certain Syslog-specific fields when building custom reports in WhatsUp Event Analyst. For more information, refer to the Custom Reporting Guide and Tutorial help file in the WhatsUp Event Analyst Programs Group.



Syslog Support in WhatsUp Event Alarm

WhatsUp Event Alarm is designed to work with syslog messages in two different ways:

- § WhatsUp Event Alarm can send Windows events that trip alarms to a central syslog server (where that central syslog server can perform further actions or analysis, such as a Linux machine with a Perl script for handling syslog files.) Alternatively, these notifications can be sent to one or more local workstations running the WhatsUp Event Alarm Listener Console, which prioritizes incoming syslog messages in different views for the benefit of the administrator.
- § WhatsUp Event Alarm can also receive syslog messages from other syslog devices (e.g. routers, Unix machines) throughout your network, and pass them directly to its internal rules engine for evaluation and notification generation.

Setting up Outbound WhatsUp Event Alarm Syslog Notifications:

Use the Define Notifications icon in Alarm Settings (Organize > settings > Alarm Settings > Define Notifications > New > Syslog tab) to create a new syslog notification or edit an existing syslog notification. This allows WhatsUp Event Alarm to send alerts to a central syslog server or group of machines running the WhatsUp Event Alarm Listener Console for further processing. Within this tab, you can specify the following items:

- § The host names or network addresses of the syslog servers or WhatsUp Event Alarm Listener Console workstations that receive WhatsUp Event Alarm's alerts
- § The port that the syslog daemon(s) or WhatsUp Event Alarm Listener Console(s) is listening on (e.g. 514) for incoming messages
- § The priority number you want to attach to any syslog messages originating from WhatsUp Event Alarm. For more information on configuring these types of notifications, see the Defining Notification Methods section.

Message Format of Syslog Notifications Sent By WhatsUp Event Alarm:

If the Use RFC3164 formatting when sending syslog messages option is selected in the *WhatsUp Event Alarm Preferences* (on page 68) dialog, the syslog message are structured as follows:

<Priority Number> Timestamp Hostname WhatsUp Event Alarm Notification Engine - Alarm (Process Created) tripped. Event details follow: Log Type,Date/Time,Source,Type of Event,Category,EventID,Username,Computer,Description

Here's a specific example of a syslog notification sent by WhatsUp Event Alarm with RFC3164 formatting:

<13> May 03 2008 03:01:25 EVENTALARMSERVER WhatsUp Event Alarm Notification Engine - Alarm (Process Created) tripped. Event details follow: Security Log,5/1/2002 3:00:48 AM,Security,Success Audit,Detailed Tracking ,592,NT AUTHORITY\SYSTEM,CARNEGIE,A new process has been created:

New Process ID: 2155349568

Image File Name: NTVDM.EXE

Creator Process ID: 2156614400

User Name: SYSTEM

Domain: NT AUTHORITY

Logon ID: (0x0,0x3E7)

If the Use RFC3164 formatting when sending syslog messages option is not selected in the *WhatsUp Event Alarm Preferences* (on page 68) dialog, the syslog message is structured as follows:

<Priority Number> WhatsUp Event Alarm Notification Engine - Alarm (Process Created) tripped. Event details follow: Log Type,Date/Time,Source,Type of Event,Category,EventID,Username,Computer,Description

Here's a specific example of a syslog notification sent by WhatsUp Event Alarm without RFC3164 formatting:

<13> WhatsUp Event Alarm Notification Engine - Alarm (Process Created) tripped. Event details follow: Security Log,5/1/2002 3:00:48 AM,Security,Success Audit,Detailed Tracking ,592,NT AUTHORITY\SYSTEM,CARNEGIE,A new process has been created:

New Process ID: 2155349568

Image File Name: NTVDM.EXE

Creator Process ID: 2156614400

User Name: SYSTEM

Domain: NT AUTHORITY

Logon ID: (0x0,0x3E7)

The use of the comma-delimited text format is intentional, so that syslog server administrators can write programs and/or scripts to parse out key parameters from these messages.

Maximum Syslog Notification Message Length:

By definition, syslog messages can only be 1024 bytes or smaller when sent by UDP to a syslog server. Therefore, any part of the message (e.g. the description field) that is larger than 1024 bytes is truncated.



Note: If you plan to transmit syslog messages across routers, ensure that router does not inadvertently fragment UDP datagrams, as this may prevent proper transmission of the syslog messages.

How Do I Create Alarms to Correspond to Certain Syslog Messages Received by WhatsUp Event Alarm?:

All valid syslog messages received by WhatsUp Event Alarm are redirected into the local Application event log on the machine where it is installed. Therefore, you should create a custom alarm in WhatsUp Event Alarm under the Edit menu, Define Alarms area. To only generate notifications for messages with a certain priority, enter the Facility and Level (e.g. Kernel.Emergency, Debug.Information, Local2.Warning) in the Category field of the alarm. To only generate notifications for messages from a certain host, place the name of your syslog device (as you defined it originally in the Syslog Device Dialog) or the IP address of the host in the description field and click the Contains radio button. To only generate notifications for messages containing certain text, place the text after the description field and click the Contains radio button.

Associate this newly created alarm with the Application log on the machine where WhatsUp Event Alarm is installed, and WhatsUp Event Alarm begins sending notifications to you if any received syslog messages meet the criteria of the custom alarm(s) you have defined.

How Do I Configure Network Devices to Forward Syslog Messages to WhatsUp Event Alarm?:

Most Unix-type operating systems have a configuration file (conf file) used by the syslog daemon to control its operation. On several such operating systems, it is located at the following path: /etc/syslog.conf, although the path may vary. Within this configuration file, you can instruct the syslog daemon to forward messages with a certain facility or level to a different network host. In this case, that host would be the IP address of the Windows XP/2003/Vista/7/2008/2012 computer running WhatsUp Event Alarm. An example entry might look something like this:

```
*.emergency @10.32.4.1
```

This will forward all syslog messages with an emergency level to the WhatsUp Event Alarm server at 10.32.4.1

```
auth.* @10.32.4.5
```

This will forward all syslog messages from the security (auth) facility to the WhatsUp Event Alarm server at 10.32.4.5

```
*.* @10.32.4.2
```

This forwards all syslog messages from any level or facility to the WhatsUp Event Alarm server at 10.32.4.2

In the case of routers and switches, you may need to either adjust a configuration menu or upload a configuration file to make it redirect certain syslog messages to an WhatsUp Event Alarm server.

Consult your operating system's / router's / switch's documentation (or syslogd man pages) for further information on setting up syslog message forwarding.

Adding a New Syslog Device

WhatsUp Event Alarm allows you to add syslog devices on your network that you want to monitor.

To add a new syslog device

- 1 Click **Organize > devices > New > Syslog**. The New Syslog Device page appears.
- 2 Complete the following fields:

§ Device Information

- § **Name**. Type the name of the syslog device you want to monitor.
- § **Business Unit**. Select the appropriate business unit from the drop down list.
- § **Site**. Select the appropriate site from the drop down list.
- § **Network address**. Select and enter information for the fully qualified domain name, Internet Protocol Version 4 or Internet Protocol Version 6.

§ **IP Address:** Type the IP address associated with the Syslog device you want to monitor.

3 Click **Save** to add the device to the device list.

CHAPTER 9

Sharing Defined Alarms Among Multiple WhatsUP Event Alarm Installations

In This Chapter

Exporting Alarms.....	63
Importing Alarms.....	64

Exporting Alarms

If you are running multiple installations of WhatsUp Event Alarm throughout your network, and you need to transfer large numbers of custom alarms and alarm bundles between installations, use the Import and Export Alarm dialogs inside WhatsUp Event Alarm to accomplish this task.

Use the Export Alarms dialog to transfer sets of alarms or alarm bundles from one WhatsUp Event Alarm installation to another. After you export alarms and alarm bundles to a file, you can always import them from the *Import Alarms* (on page 64) dialog.

Export Alarms dialog field descriptions:

- § **File to Export Alarms and Alarm Bundles Into.** Click the Browse (...) button to select a file that will receive the exported alarms and alarm bundles. Navigate to the directory where you want to save the exported file, and type in a new file name. WhatsUp Event Alarm creates the file and exports the alarms when you click **OK**.
- § To prepare an alarm for export, drag it from the left side (Available Alarms Column) of the dialog to the right side (Alarms And Bundles For Export Column). If you have bundled a group of alarms that you want to export, drag that alarm bundle from the left side (Available Alarm Bundles Column) to the right side (Alarms And Bundles For Export Column). Click the **Add** button to move selected alarms or alarm bundles from the left side to the right side.
- § To not export an alarm or alarm bundle, select it in the right side list, and then click **Remove Alarm(s)**.
- § **OK.** Exports all of the items in the Alarms and Alarm bundles to Export tree to the file you selected.
- § **Cancel.** Closes the dialog without exporting your alarms/alarm bundles.

Importing Alarms

Use the Import Alarms dialog to import sets of alarms or alarm bundles exported by another WhatsUp Event Alarm installation into the local WhatsUp Event Alarm system. This can be very useful if you need to set up a uniform set of alarms across multiple WhatsUp Event Alarm installations. If you want to export alarms and alarm bundles to a file for use on another system, you may do so from the *Export Alarms* (on page 63) dialog.

Import Alarms and Alarm Bundles field and button descriptions:

- § **Import Alarms and Alarm Groups from File.** Click the Browse (...) button to choose a file containing exported alarms and alarm groups from a different WhatsUp Event Alarm installation. After you select this file, the alarms and alarm groups housed in that file are displayed in the Alarms to Import listing.
- § **View.** Displays more detailed information about the alarm or alarm group you have selected in the Alarms to Import listing.
- § **Remove.** Removes the selected alarm or alarm group out of the Alarms to Import listing. Deleted alarms 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 Alarms dialog back to the main alarm listing view.

CHAPTER 10

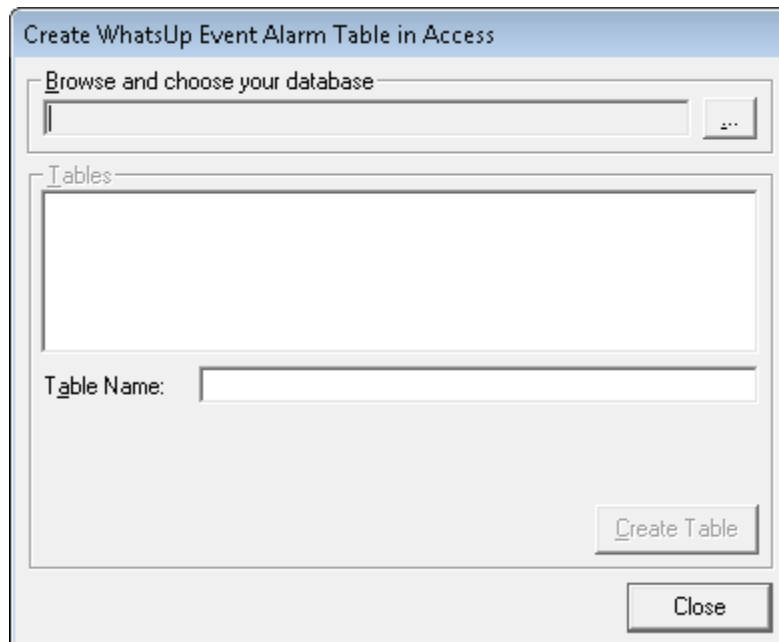
Creating Database Tables for Storage of Detected Events

In This Chapter

Creating Tables	65
Creating Tables on Other ODBC Servers.....	66
Setting Up Databases and Making Connections.....	67

Creating Tables

You can use the Create Table dialog to create WhatsUp Event Alarm compatible tables in Microsoft Access and Microsoft SQL Server databases. After creating the tables, you can instruct WhatsUp Event Alarm to place event log entries into these tables when alarms are tripped, providing you with the history of events that triggered alarms. Use the *Define Notifications* (on page 40) dialog to set up database insertions when alarms are triggered.



- § **Browse and choose your database.** Click the (...) button to either find or create a Microsoft Access .MDB database file, or find/create an ODBC data source link to a Microsoft SQL.

- § **Tables.** After you connect to a database, WhatsUp Event Alarm automatically populates this list with all of the tables in that database. To create a new table, type the table name below the list, and then click **Add**.
- § **Table Name.** The name of the table you want to create.
- § **Close.** Closes this dialog.

Creating Tables on Other ODBC Servers

Although WhatsUp Event Alarm was designed to place event log data into Microsoft Access and Microsoft SQL Server databases, it can import this data into other ODBC databases as well. The key to importing event log data into other databases is using a WhatsUp Event Alarm compatible table format. To create a WhatsUp Event Alarm compatible table, you must adhere to the following field names and field data types. Print this help topic and consult with your database administrator to create the following table structure. If your database server supports SQL CREATE TABLE statements, here is a sample script to generate such a table:

```
CREATE TABLE [NewTest] ([RecordNum] [bigint] IDENTITY (1, 1) NOT NULL ,
[DateAndTime] [datetime] NOT NULL , [Source] [varchar] (100) NOT NULL ,
[TypeOfEvent] [varchar] (50) NOT NULL , [Category] [varchar] (100) NOT
NULL , [EventID] [int] NOT NULL , [AccountInfo] [varchar] (150) NOT NULL
, [Computer] [varchar] (100) NOT NULL , [Description] [text] NOT NULL ,
[LogType] [int] NOT NULL);
```

Field Name	Field Data Format	Comments
RecordNum	8-byte integer	Autonumber (IDENTITY) field
DateAndTime	8-byte date/time	
Source	100-byte string	
TypeOfEvent	50-byte string	
Category	100-byte string	
EventID	4-byte integer	
AccountInfo	150-byte string	
Computer	100-byte string	
Description	Long string	Text field
LogType	4-byte integer	

In this table, every field is self-explanatory except for the LogType field. This integer indicates the particular log file the event record came from, and works as follows:

1 Application Log

2 System Log

3 Security Log

4 DNS Server Log

5 Directory Service Log

6 File Replication Service Log

Setting Up Databases and Making Connections

In order to prepare a new ODBC-compliant database to receive selected event log entries from WhatsUp Event Alarm, create (or have your database administrator create) a new database on your database server with default settings, and establish an initial size for the database that can be expanded later (e.g., 5 gigabytes). It is recommended that you use Microsoft SQL Server 2005, 2008, or 2012 as your database server back end, as these platforms have been tested and work well with WhatsUp Event Alarm. 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 should be a standard security login as opposed to an Windows integrated login. If you do opt to use integrated Windows security, ensure that the WhatsUp Event Alarm Service account has full read and write permissions to the database by using the SQL Server Enterprise Manager tool.

After the database and login is created, use the ODBC connection manager that can be opened from several of WhatsUp Event Alarm's dialogs to create a connection string to the database. It is important that this connection is set up as a File DSN as opposed to 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. Choose your previously created File DSN by name whenever WhatsUp Event Alarm opens the ODBC connection manager dialog.

Configuring and Tuning WhatsUp Event Alarm

In This Chapter

Setting Preferences.....	68
Enabling Flood Control.....	72
Setting the Default Domain / Workgroup.....	73
Installation Requirements.....	73
Before You Begin.....	75
Microsoft Vista / Windows Server 2008 Requirements and Recommendations	85
Other Recommendations.....	88
Rapid Configuration Chooser Dialog.....	92
Service Account Dialog.....	93
Build Priority Dialog.....	95
WhatsUp Event Alarm Log Entries Viewer Dialog.....	97
Custom Domain Manager Dialog.....	97
Computer Name Retrieval Dialog.....	99

Setting Preferences

The WhatsUp Event Alarm Preferences page, available from the Organize page, allows you to optimize the operating behavior of the WhatsUp Event Alarm Service, manage flood control and notification times, and establish communication devices for the purpose of sending notifications. Many of these settings, when changed, do not take effect immediately - the WhatsUp Event Alarm Service should be stopped and restarted if you want the program to begin using new settings.

Below is an explanation of all the fields in the WhatsUp Event Alarm Preferences page.

Performance Tuning tab

This tab allows you to optimize the performance of the WhatsUp Event Alarm Service as it monitors event logs from multiple computers on your network. In general, if you want more immediate notification capabilities (e.g. receiving notification within seconds of a new event log entry being recorded), you must increase the resource burden (CPU, memory, and network traffic) on the WhatsUp Event Alarm Server. Conversely, if notifications need not be

immediate, then you can reduce the resource burden on the server and make it scan log entries more infrequently.

- § **Processor Utilization.** This slider establishes a baseline number of milliseconds for how long the WhatsUp Event Alarm Service rests between each new scan of event logs stored in its log monitoring database. The default setting is 2000ms, or 2 seconds per run through all of the server logs being monitored. In addition, the service also rests for 1/4 this value in between log entries (e.g. .5 seconds in this case). For example, if you are monitoring 20 event logs, WhatsUp Event Alarm visits each log in a round robin fashion to scan for new entries. $20 \times .5 \text{ seconds} = 10 \text{ seconds}$ plus 2 seconds at the end of the run, representing a minimum interval of 12 seconds before a log is revisited again for a scan of new event log entries. On a larger network generating many event log entries, it may be necessary to reduce this interval and increase the number of scanning processes. Conversely, on a smaller network, you may be able to increase the interval and only use a single scanning process, if new events are logged infrequently on your servers.
- § **Enable Turbo Scanning Mode.** If you turn this option on, the WhatsUp Event Alarm Service does not yield any processor time during the intervals when it is actively scanning new events that have occurred on computer logs. Typically, this results in CPU utilization of 5 to 15% of total processor time per log scanning process used. Therefore, the more dedicated event log scanning processes you instruct WhatsUp Event Alarm to use (see below), the more total CPU time is consumed. Enabling Turbo Scanning Mode is often useful if you are trying to scan many computers' event logs from one WhatsUp Event Alarm installation, especially if several of the servers audit many events per minute (e.g. Domain Controllers).
- § **Dedicated Event Log Scanning Processes.** This setting controls how many event logs to scanned at once with the WhatsUp Event Alarm Service. Typically, the busier the network, the more event log scanning processes you use to keep up with the volume. E.g. if a few servers are generating hundreds of events per minute, you want to use multiple processes so that scanning the new entries in the busier servers do not unnecessarily delay the other logs needing scanned on the network. A good rule of thumb is to add an additional scanning process for 1000 log entries / minute produced by your network. If the servers you monitor are producing a total of 4000 log entries / minute, use between 4 and 6 scanning processes.

Each additional scanning process you create uses an additional 5 to 8 MBs of system memory, on top of the 10MB working minimum for the WhatsUp Event Alarm Service and notification engine. Ensure you have enough RAM available on your monitoring server to support additional processes.

Enabling the Turbo Scanning Mode above may actually reduce the number of scanning processes you need to use, since Turbo Scanning Mode does make each scanning process more efficient. We recommend that you experiment with these settings to see which configuration works the best in your environment.

- § **Old Record Scanning Limit.** This limit determines how many old entries prior to the most current event log entry the WhatsUp Event Alarm Service can scan during each pass through an event log. Because the WhatsUp Event Alarm service maintains a history of the last event log record it scans on each log, it can determine how many entries have been added since its last scan. It scans either the total number of new event log records added to a log, or the old record scanning limit, whichever is smaller. On busier networks, you may wish to set this to a higher number, so that no records are missed between scans.
- § **Event Log Access Caching.** WhatsUp Event Alarm can maintain open connections to the event logs it is responsible for monitoring. If persistent access is enabled, authentications is reduced on monitored machines and scanning speed improves. However, in some network environments, maintaining persistent access may cause problems (e.g. over WAN links, using WhatsUp Event Alarm alongside software that breaks open file handles, etc). Therefore, consider disabling this option if scanning operations prove unreliable.
- § **ICMP Echo (Ping) Testing / System Offline Notification.** To avoid the lengthy network timeouts that can occur when WhatsUp Event Alarm attempts to scan logs on machines that are offline, you can instruct WhatsUp Event Alarm to use ICMP Echo testing when monitoring computer logs. If enabled, WhatsUp Event Alarm attempts to ping each computer before scanning it. You can also control the timeout in milliseconds that WhatsUp Event Alarm waits for a response from the computer. If your network has a high latency, consider increasing this number. You can instruct WhatsUp Event Alarm to perform a certain notification when computers no longer respond to pings, and also when they come back online (e.g. start responding to pings again).

Flood Control / Notification Times tab

This tab allows you to restrict the sending of notifications to certain times, and to enable flood control options in the event that one or more computers on your network start raising a very high level of alarms per second.

Flood Control Enable/Disable. Enabling flood control makes the WhatsUp Event Alarm Service automatically stop sending notifications about events on a particular computer if a certain number of alarms are generated in a short period of time. For example, a program on an application server may start flooding the Application log with errors. If flood control is enabled and the cutoff number of alarms are detected within a specified period of time, the WhatsUp Event Alarm Service sends a notification indicating that a flood of events is detected, and then stops sending notifications related to that alarm on that computer until the flood expiration interval is reached.

- § **X identical alarms from the same computer in Y seconds is considered a flood.** From here you determine how many identical alarms, when detected on the same computer within a given time frame, is considered a flood. It is recommended that you do not set either value too low, or valid notification messages may be prematurely halted from a computer experiencing issues.
- § **Keep a computer in flood mode so that no similar alarms are sent for X minutes.** The value entered for X represents the time in minutes before a flood expires for a given alarm on a given computer. No new notifications related to that alarm are sent until this time period ends.

- § **Flood control will restrict transmission of the following notification types.** In general, some notification methods prove more problematic in the event of a notification flood than others. By default, WhatsUp Event Alarm only applies flood control techniques to notifications that arrive via email, network popup, or pager. Database insertions are not typically governed by flood control, because they are non-interactive by nature. Syslog messages/WhatsUp Event Alarm Listener Console messages are not typically governed by flood control, because floods of messages can be consolidated and suppressed directly by the user in the event of a flood.
- § **Notification Times.** In certain scenarios, administrators may only care to receive notifications about alarms during certain times in the day (e.g. during work hours/after work hours). Turning on notification time restrictions allows you to prevent WhatsUp Event Alarm from sending out notifications during certain times on certain days. To disable notifications during certain hours, click the appropriate block in the grid to toggle it to a red "N." Likewise, to enable notifications during other hours, click the appropriate block in the grid to toggle it to a green "Y." To select a certain hour on all days, click one of the column blocks at the top of the grid. To select all hours on a specific day, click one of the column blocks to the left of the grid.

Communication Info tab

Use this tab to set key communication properties, such as an outbound SMTP server for email notifications and a TAPI-compliant modem for pager-based notifications.

- § **Enable email notifications in WhatsUp Event Alarm.** Check this box if you plan to send email notifications with WhatsUp Event Alarm. You need to enter in your SMTP server name, port, and sender address.
- § **SMTP Server for email relay.** This should be a high-availability email server internal to your organization. When WhatsUp Event Alarm prepares an email notification, it relays the message through this SMTP server.
- § **Port.** The port number used by the SMTP Server above to accept new messages for relay. Some organizations restrict internal mail traffic to a non-standard SMTP port (e.g. something other than port 25), so if that is the case in your organization, you can change the port number used here.
- § **Sender address used.** Use this field to supply an originating email address for all email notifications. A good candidate for this email address is a person who frequently needs to be made aware of particular alarms when they are tripped. When an email notification is sent out, this address is used as the originating or reply-to address of the message. Also, this address receives any undeliverable reports if a mail message cannot be relayed.
- § **Select TAPI-Compliant Data Modem.** WhatsUp Event Alarm automatically detects all TAPI-compliant data modems installed on the server where it is running, and displays them in this list. Select the modem you wish to use from the list. If no such modems are available on the machine, this option is grayed out and pager notifications are not generated.
- § **Modem Disconnect Timeout.** Some data modems do not know how to disconnect after the receiving pager hangs up. Therefore, this timeout indicates the number of seconds the modem can remain off-hook to dial and transmit a numeric message. When this timer has elapsed, the modem is automatically put back on-hook until it is needed for another pager notification.

- § **Broadcast (NetBIOS) Notifications.** If enabled, WhatsUp Event Alarm automatically sends out a NetBIOS-style broadcast notification to all clients running the WhatsUp Event Alarm Listener Console in the domain. Uncheck this option if you do not want these notifications sent.
- § **Note:** If you change this setting, you must stop and restart the WhatsUp Event Alarm Service before it takes effect.
- § **Use RFC3164 formatting when sending syslog messages.** When checked, WhatsUp Event Alarm adds an RFC3164 compliant header to the syslog messages it sends as notifications (e.g. the header contains a timestamp and hostname as well as the priority code). For more information on how this works, please review the Syslog Support in WhatsUp Event Alarm help topic.

Vista and Newer tab

Use this tab to govern how WhatsUp Event Alarm refines Microsoft Vista and Microsoft Windows Server 2008 logs when it scans for new events.

- § **For system logs, change information events to Success Audits and Failure Audits as appropriate.** When checked, WhatsUp Event Alarm converts the Level field in a security EVT file from "Information" to "Success Audit" or "Failure Audit" in the text file or database table, depending on the nature of the event. This feature is useful if you are analyzing Microsoft Vista and/or Microsoft Windows Server 2008 security events alongside events from older operating systems in a central database.
- § **For system logs, place User info from the Description field in the User field as appropriate.** Microsoft Windows Vista and Windows Server 2008 do 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 Alarm extract the most appropriate user from the Description field of each EVT record and place it in the User field for the purpose of alarm detection and notification construction.
- § **For system events, append keywords and opcodes to the Category field (e.g. Category: Keyword: Opcode).** To maintain a common number of fields between EVT and EVT files that are output into text files and database tables, WhatsUp Event Alarm can append the Keyword and Opcode fields to the Task/Category field in an EVT record when sending a notification. The consolidated Task/Category field also contains the Keyword and Opcode fields, appearing like so:
Task/Category:Keyword:Opcode.

Enabling Flood Control

Enabling flood control makes the WhatsUp Event Alarm Service automatically stop sending notifications about events on a particular computer if a certain number of alarms are generated in a short period of time. For example, a program on an application server may start flooding the Application log with errors. If flood control is enabled and the cutoff number of alarms are detected within a specified period of time, the WhatsUp Event Alarm Service sends a notification indicating that a flood of events is detected, and then stops sending notifications related to that alarm on that computer until the flood expiration interval is reached.

Setting the Default Domain / Workgroup

The default domain governs the primary (master) Windows domain the WhatsUp Event Alarm Control Panel works with. Alternatively, this can specify a workgroup, if WhatsUp Event Alarm is installed on a computer not participating in a domain. If you choose a top-level domain that is trusted by other domains, the trusting domains appear in the domain chooser list box by default.

Installation Requirements

Operating System:

- § 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 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.

SMTP Server (optional):

If you wish to send email notifications with WhatsUp Event Alarm, specify an internal SMTP server for mail relay during setup. Ipswitch recommends the Virtual SMTP server component that ships free with IIS on most Windows workstations and servers.

TAPI-Compliant Data Modem (optional):

If you wish to send numeric pager notifications with WhatsUp Event Alarm, a data modem must be present on the machine where it is installed.

Microsoft Access (optional)

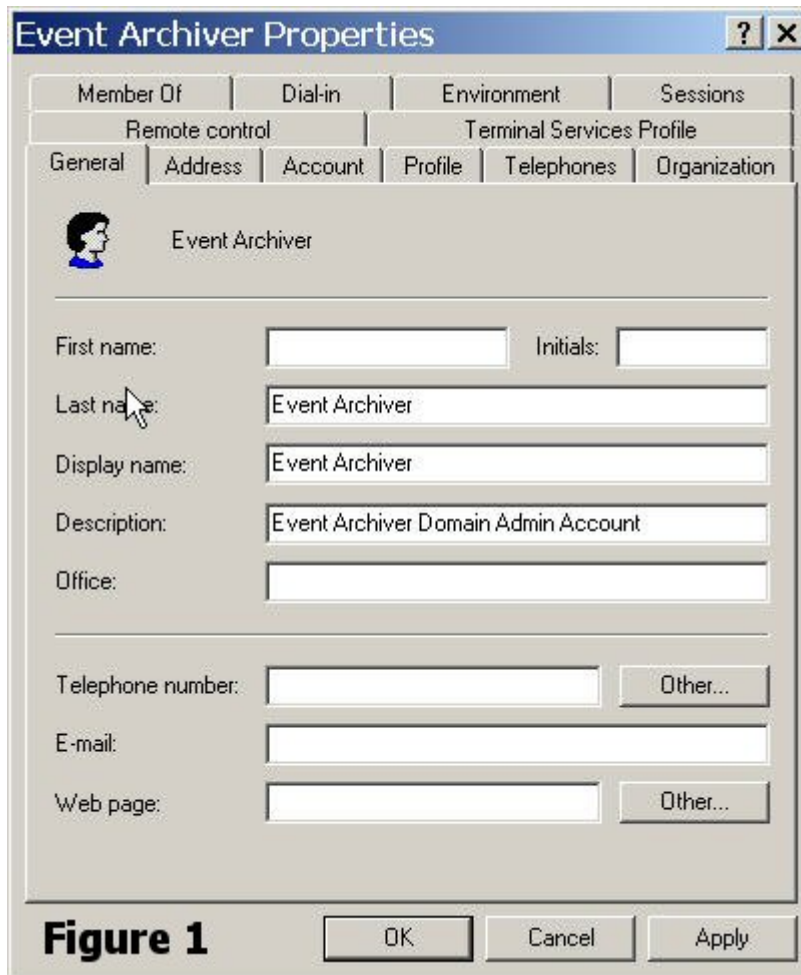
WhatsUp Event Alarm can place event log entries that trip alarms into Microsoft Access database tables, so you will need Microsoft Access installed if you wish to view these tables directly. Alternatively, you can review the contents of these databases with Ipswitch's WhatsUp Event Analyst program.

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

WhatsUp Event Alarm can also place event log entries into ODBC server database tables. Microsoft SQL Server is the recommended database server for LANs generating a great deal of event log activity. For best performance, it is recommended that you install WhatsUp Event Alarm to a different machine than the ODBC database server, although in smaller environments, the database can be located on the same system as WhatsUp Event Alarm.

Before You Begin

- 1 Ensure you are logged in with local administrator rights on the machine where you are installing the product. In addition, if the product will be used to monitor logs in a domain or OU, ensure you have domain administrator or OU admin rights as well. Check these settings in Active Directory Users and Computers. Otherwise, you will be unable to properly configure the software.




The screenshot shows the 'Event Archiver Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a question mark and a close button. Below the title bar are several tabs: 'Member Of', 'Dial-in', 'Environment', 'Sessions', 'Remote control', and 'Terminal Services Profile'. The 'General' tab is active, showing fields for 'First name', 'Last name', 'Display name', 'Description', 'Office', 'Telephone number', 'E-mail', and 'Web page'. The 'Last name' field is populated with 'Event Archiver', and the 'Description' field is populated with 'Event Archiver Domain Admin Account'. There are 'Other...' buttons next to the 'Telephone number' and 'Web page' fields. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Event Archiver Properties

Member Of | Dial-in | Environment | Sessions

Remote control | Terminal Services Profile

General | Address | Account | Profile | Telephones | Organization

 Event Archiver

First name: Initials:

Last name:

Display name:

Description:

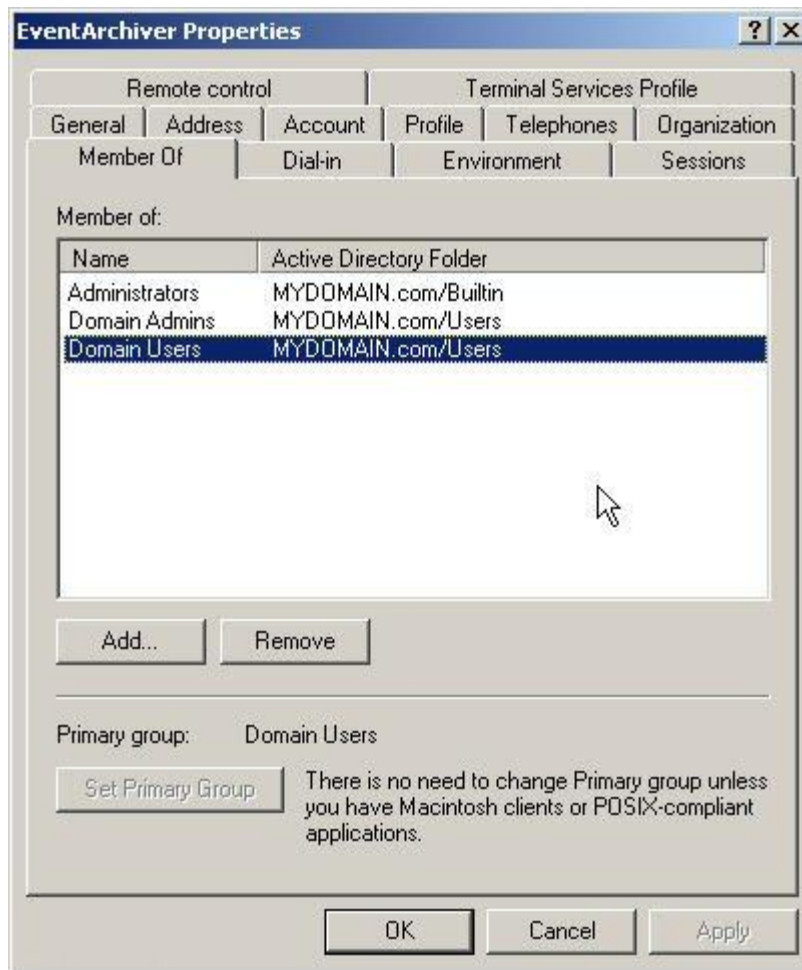
Office:

Telephone number: Other...

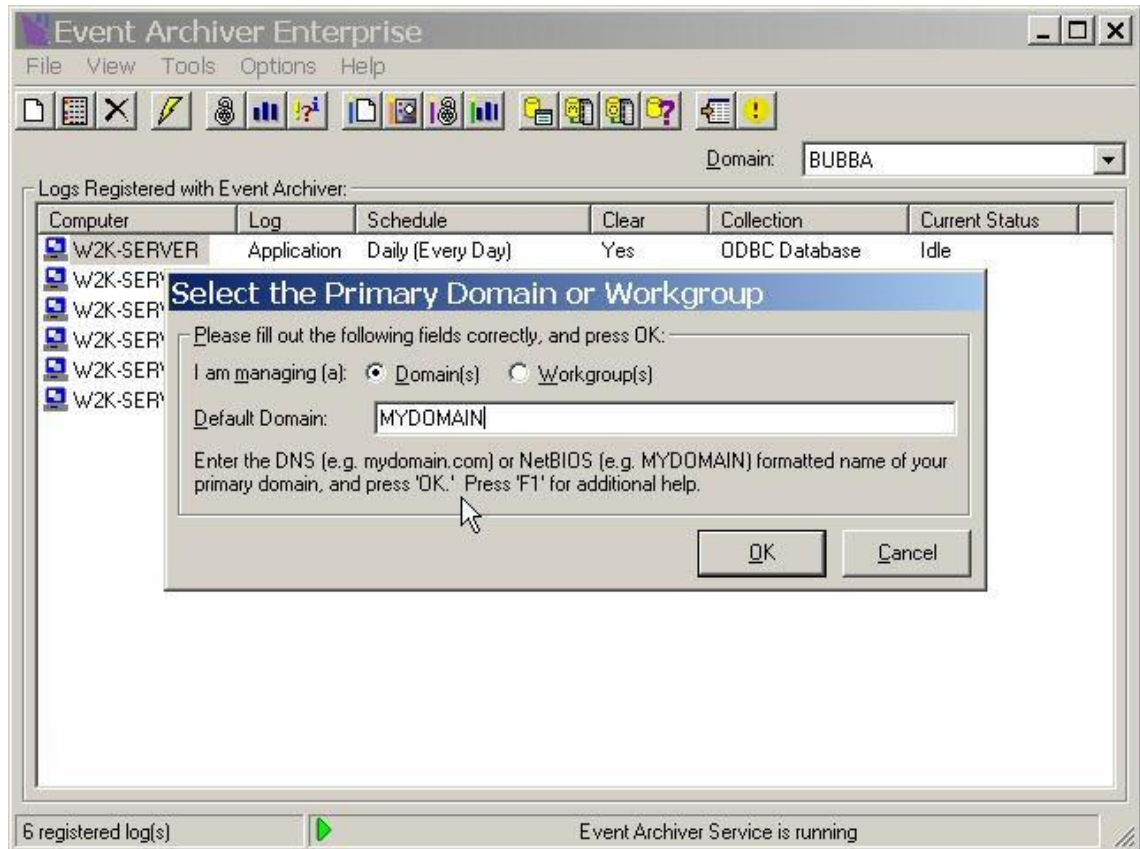
E-mail:

Web page: Other...

Figure 1 OK Cancel Apply



- Determine which domain(s) or workgroup(s) you want WhatsUp Event Alarm to monitor for event logs. If you want to monitor logs from more than one domain, choose a primary domain that is trusted by other domains. WhatsUp Event Alarm refers to this primary domain as the default domain. During the first run of the software, when prompted, enter your chosen default domain.



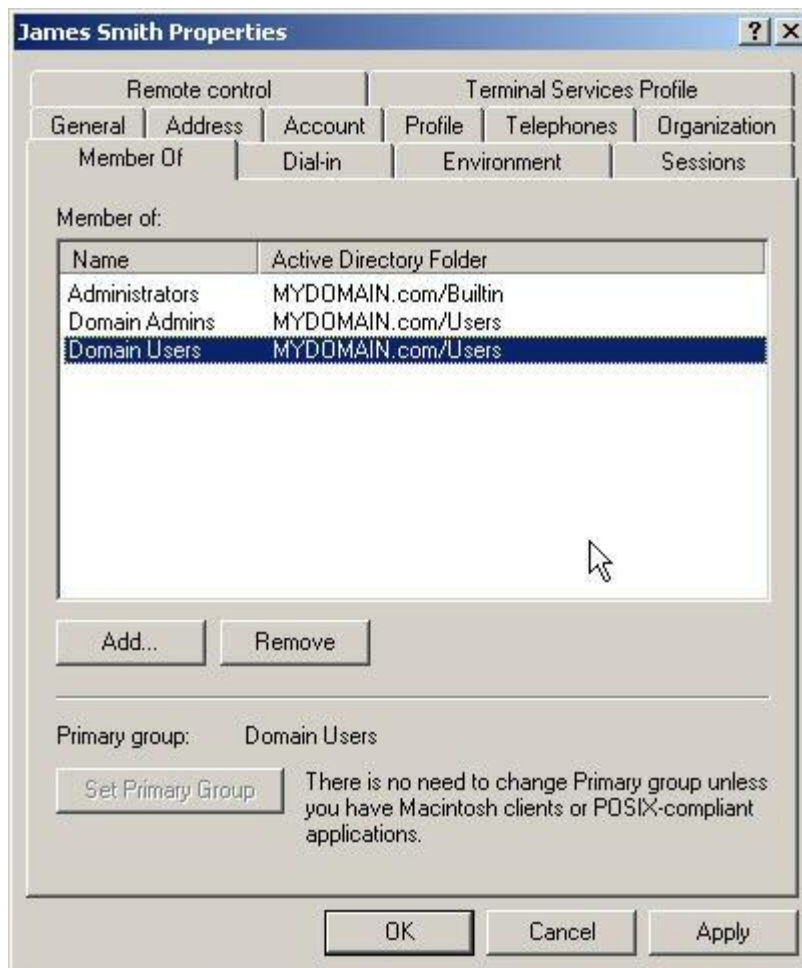
Note: If you are installing WhatsUp Event Alarm to a server or workstation not participating in a domain, please enter its workgroup instead. For complicated networks that include WANs and/or demilitarized zones, please read the Other Recommendations section listed below as well as the Deployment Scenarios section of the WhatsUp Event Alarm User's Guide.

- If you do not already have an established user account with domain admin or organizational unit rights that services can run under in your organization, create one with User Manager or Active Directory for Users and Computers and place it into the Domain Admins group or the OU Admins group of the Organizational Unit you manage. Also, ensure that it has administrator rights (either by itself or via group membership) on the local machine where you installed WhatsUp Event Alarm. Finally, if you are using an OU Admin account, ensure that this account (either by itself or via group membership) is in the local Administrators group of each member server and workstation WhatsUp Event Alarm will monitor.



Note: If you are installing WhatsUp Event Alarm to a server or workstation not participating in a domain, please enter a local user who is an Administrator (e.g. SERVERNAME\Administrator) on the local machine and on any other machines being managed.

- 4 Ensure you (e.g. the interactive user account that runs the WhatsUp Event Alarm Control Panel) have domain admin or OU admin rights in the domains/organizational units you manage with WhatsUp Event Alarm. The WhatsUp Event Alarm Control Panel does some security intensive tasks, such as adjusting audit policies and event log settings, so these elevated rights are required to operate it.



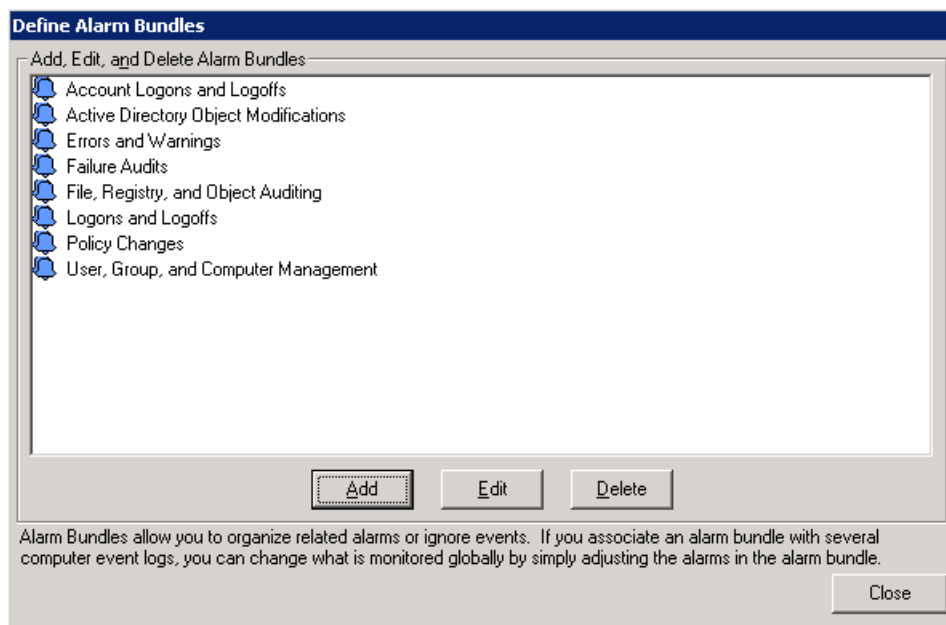
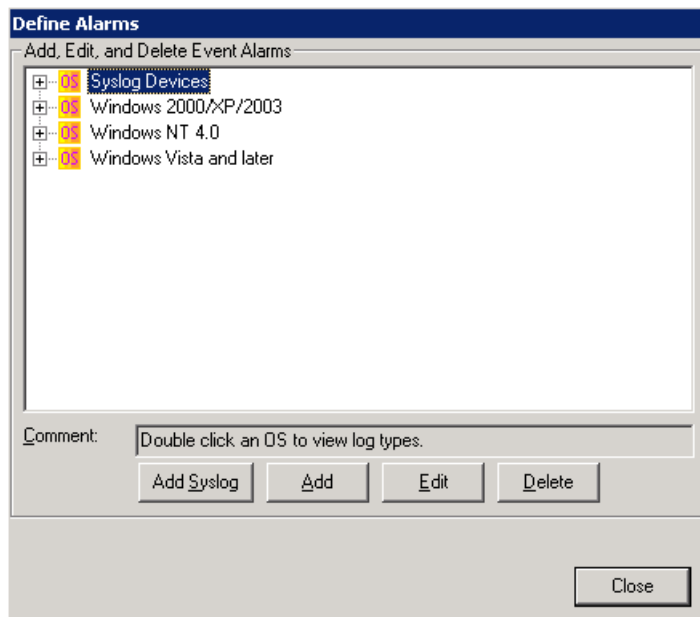
To increase log scanning time, if the majority of the systems being monitored are running Windows 2003, install WhatsUp Event Alarm on a Windows 2003 server. Likewise, a majority of Windows 2008 servers should be watched by WhatsUp Event Alarm running on a Windows 2008 server, etc.

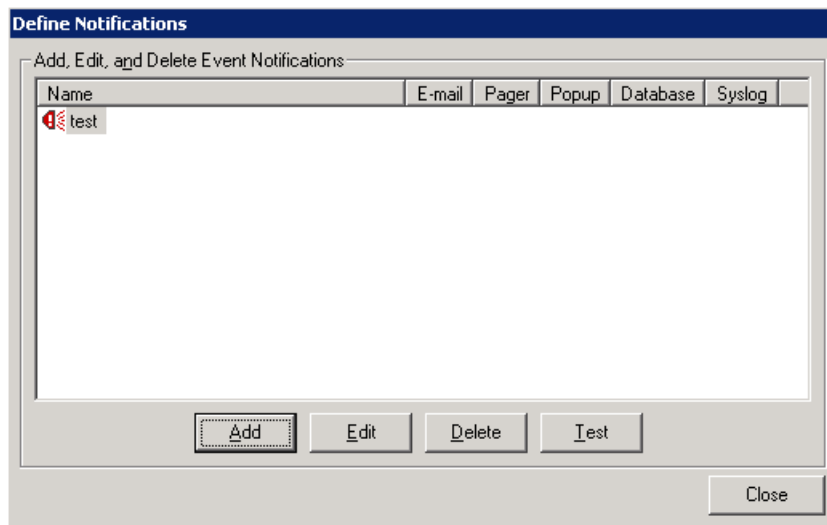
- 5 If you want to be notified about detected events via e-mail, locate an available SMTP server on your network (we recommend the Virtual SMTP Server component that ships free with Microsoft's Internet Information Server), and adjust its security settings so that the WhatsUp Event Alarm server may relay mail through it.
- 6 Determine what events you need to monitor, and who you need to inform if the events are detected. Many common alarms ship with WhatsUp Event Alarm, but you can always

create your own alarm definitions. To manage alarms, click the **Edit** menu, and then select **Define Alarms**. After you have created new or chosen existing alarms, group them logically together into alarm bundles. To manage alarm bundles, click the **Edit** menu, and then select **Define Alarm Bundles**. Finally, create notifications that will inform certain parties when alarms are detected. To manage notifications, click the **Edit** menu, and select **Define Notifications**.



Note: You may be able to perform these actions more easily by using the Rapid Configuration Tool. See below for further details.





- 7 When prompted, enter the default domain or workgroup and service account you have selected. Also, tell WhatsUp Event Alarm from where to list computers (e.g. the browse list, the entire domain, or an OU inside your domain).



Finally, WhatsUp Event Alarm displays the Preferences dialog, where you can optimize WhatsUp Event Alarm's operating parameters for the size of your network, adjust flood control and notification times, and set other communication settings. You must indicate a SMTP server and originating sender email address for email-based notifications. If you do not plan to use email notifications, these can be made-up names, but the fields are required before continuing.

Event Alarm Preferences

Performance Tuning | Flood Control / Notification Times | Communication Info

Processor Uttilization
Lower CPU Utilization More Immediate Notification

☐ Enable Turbo Scanning Mode (no CPU rest cycles are taken during log scans)

Dedicated Event Log Scanning Processes: process(es) (1 to 60)

Old Record Scanning Limit: event log entries (100 - 9999)

Event Log Access Caching
☒ Maintain persistent access to monitored log files

ICMP Echo (Ping) Testing / System Offline Notification
☒ Use ICMP Echo testing when monitoring computer logs Timeout in milliseconds:
☒ Notify me when system(s) go offline/online via

NOTE - Performance adjustments will not take effect until after the Event Alarm Service is stopped and restarted.

Press 'F1' for an explanation of what each configuration item in this dialog controls.

OK Cancel

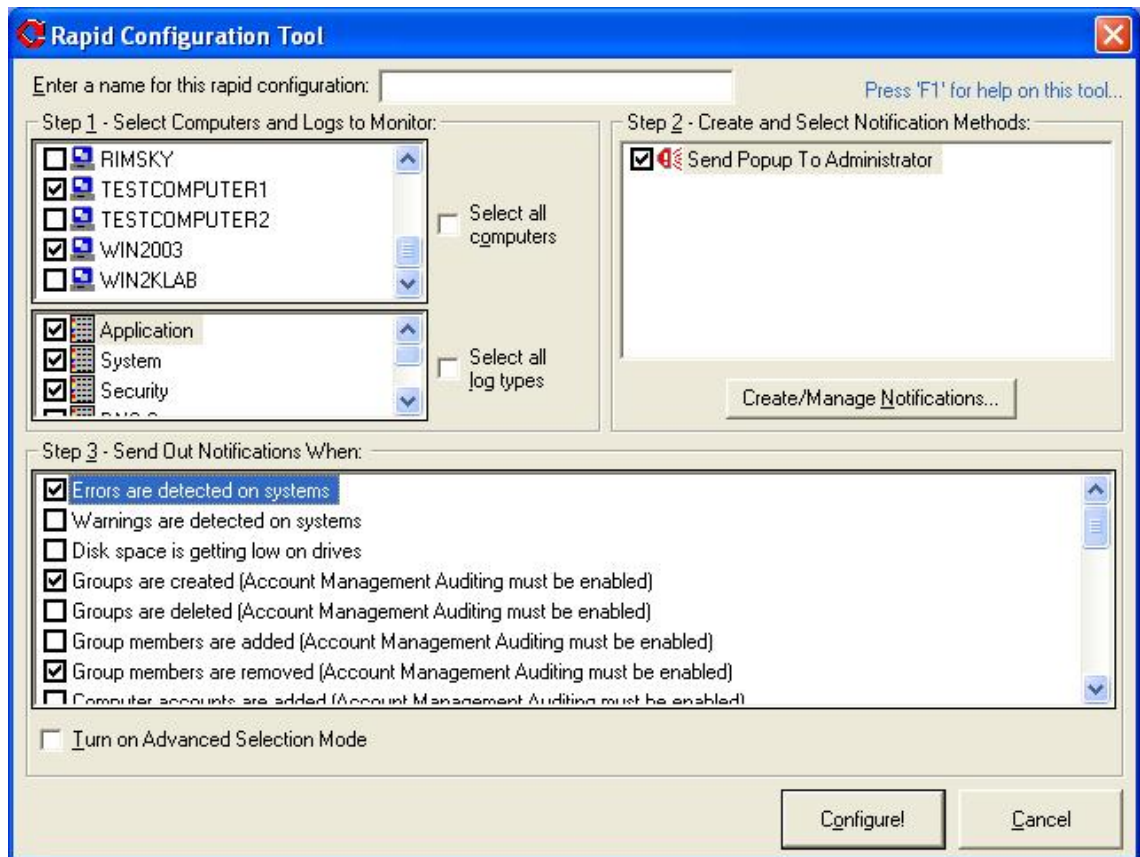


Note: By default, ICMP Echo (Ping) testing is turned on in WhatsUp Event Alarm. This is by design to help the WhatsUp Event Alarm Service only scan event logs on computers that are online. However, if you do not allow ICMP traffic on your network, or block it at a router that WhatsUp Event Alarm must scan logs across, uncheck the **Use ICMP Echo testing** option so your event logs are still scanned as needed.



Note: By default, Turbo Scanning Mode is enabled so that new log entries can be scanned as quickly as possible on computers throughout your network. If the computers you are monitoring do not generate many events, you can disable this setting so that WhatsUp Event Alarm's CPU usage is less.

Once this is accomplished, you can start watching event logs en masse using the WhatsUp Event Alarm Control Panel. When WhatsUp Event Alarm executes for the first time, the Rapid Configuration Tool starts automatically. Use this tool to quickly roll out a monitoring strategy to multiple servers at once.



The Rapid Configuration Tool

The Rapid Configuration Tool in WhatsUp Event Alarm is one of the easiest and simplest ways to establish a log monitoring strategy for multiple computers in your workgroup, domain, or organizational unit. An administrator can choose the computers, logs, notification methods, and events to monitor for in one area. Once a rapid configuration is run, it is saved to disk and can be summoned again in the future to be applied to new systems, or to simply reset everything back to its initial monitoring profile.

Additionally, rapid configurations that are saved after being used to establish a monitoring strategy can be treated as templates in two of WhatsUp Event Alarm's step-by-step wizards: Setup Monitoring for Multiple Computers at Once and Adjust Settings for Currently Monitored Logs.

Step 1 - Select Computers and Logs to Monitor

Type a name for this rapid configuration. The name you supply is the name the rapid configuration is saved as for reuse in the future.

Place a check by all computers you wish to monitor using the same rapid configuration. You can control how WhatsUp Event Alarm retrieves this list of computers by using the Computer Name Retrieval dialog.

Similarly, place a check by all log types on computers that you wish to monitor.

Step 2 - Create and Select Notification Methods

If this is your first time running WhatsUp Event Alarm, create some new notifications that define how WhatsUp Event Alarm will notify you when key events are detected. Clicking the **Create/Manage Notifications** button opens the Define Notifications dialog allowing you to create new ways of being notified. After you have created your notifications, close the Define Notifications dialog and they will then appear in the Rapid Configuration Tool. Place a check by any that you wish to use in the current configuration.

Step 3 - Send Out Notifications When (Basic Selection Mode)

Many common critical actions (e.g. errors/warnings, certain security events) are already predefined in the Rapid Configuration tool. Checking any of these actions makes WhatsUp Event Alarm automatically find the alarms that correspond to these activities in its database and associates them with your computers and logs. If you desire a higher level of granularity when it comes to determining events that must be monitored, check **Turn on Advanced Selection Mode**. This allows you to select individual alarms by hand, as well as allows you to create your own alarms.



Note: The individual alarms associated with one or more activities remain checked once you turn on Advanced Selection Mode. This is for your convenience, as it allows you to define and select custom alarms directly alongside more common log activities.

Step 4 - Select Event Activity to Monitor With Alarms (Advanced Selection Mode)

In advanced selection mode, you can check all of the individual events you want to monitor for on computer logs. clicking the **Create/Manage Alarms** button allows you to define your own custom alarms that correspond to events you want tracked. Alarms categorized under the Security Log are listed on the left-hand listing, and alarms categorized under all other log types appear in the right-hand listing. Place a check by any you wish to include in the rapid configuration.

Configure! Click this button when you are satisfied with the monitoring profile you have created. After your selections are validated, WhatsUp Event Alarm:

- Removes the existing monitoring configuration in WhatsUp Event Alarm for the selected computers and logs

- Groups the security log alarms you selected into an alarm bundle

(e.g. using the format RapidConfigName_SecurityAlarms)

- Groups the other log alarms you selected into an alarm bundle

(e.g. using the format RapidConfigName_OtherAlarms)

- Associates the security log alarm bundle with all of the security logs on the computers you selected for monitoring
- Associates the other logs alarm bundle with all of the other logs on the computers you selected for monitoring
- Associates the notification methods with the monitored servers
- Stops and restarts the WhatsUp Event Alarm Service so your new configuration takes effect immediately to save your rapid configuration to disk for future editing or reuse

If, in the future, you want to adjust what events WhatsUp Event Alarm monitors, you can add or remove alarms from either the Security Alarms alarm bundle or the Other Alarms alarm bundle using the Define Alarm Bundles area under the Edit menu. If you want to set up exclusionary alarms (e.g. ignore events), you may run the Adjust Settings for Currently Monitored Logs wizard, choosing a previous Rapid Configuration as a template and then selecting Ignore Events in Step 3 of the wizard. Likewise, if you want to apply an existing rapid configuration to new servers that appear on your network, you may run the Setup Monitoring for Multiple Computers at Once wizard, and select a previous Rapid Configuration as a template in Step 1.

Finally, if you want certain events to only generate one particular notification, regardless of the computer being monitored, you can use the Specific Notification feature in the Define Alarms Dialog.

Microsoft Vista / Windows Server 2008 Requirements and Recommendations

To monitor active Microsoft Vista / Windows Server 2008 / Windows 7 logs in the new EVT-X format, WhatsUp Event Alarm must be installed on a Microsoft Vista or later operating system. If you attempt to monitor active Microsoft Vista/2008/7 logs when WhatsUp Event Alarm is installed on an older operating system (e.g. Microsoft Windows XP, Microsoft Windows 2003, etc) the operation will fail.

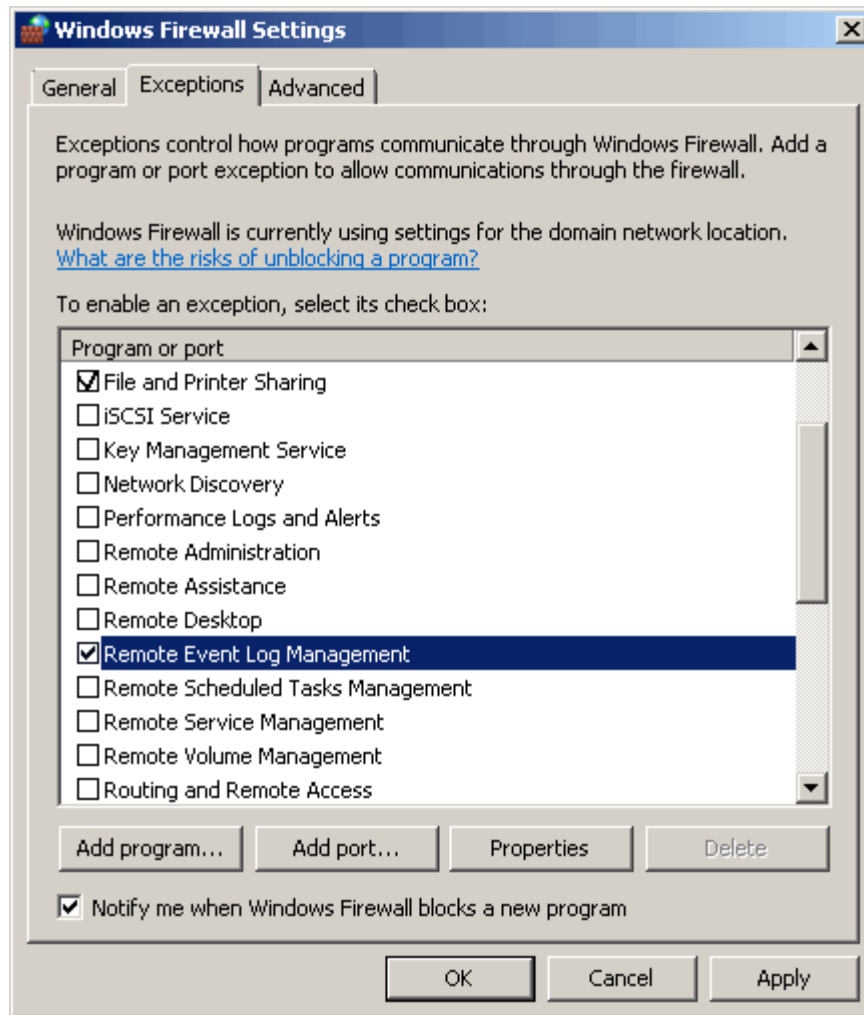
In Microsoft Vista, Windows Server 2008, and Windows 7, the default security settings are much stronger than in previous Microsoft operating systems. This is in keeping with Microsoft's focus on reducing the potential surface area for attacks over the network.

Starting in WhatsUp Event Alarm version 6 and carrying into later versions, the software is redesigned with these considerations in mind, using only the bare minimum of network access techniques to monitor log files from Microsoft Vista/Server 2008/Windows 7 systems. If you can remotely view and manage your event logs with the Microsoft Event Viewer, WhatsUp Event Alarm should have no issues monitoring them.

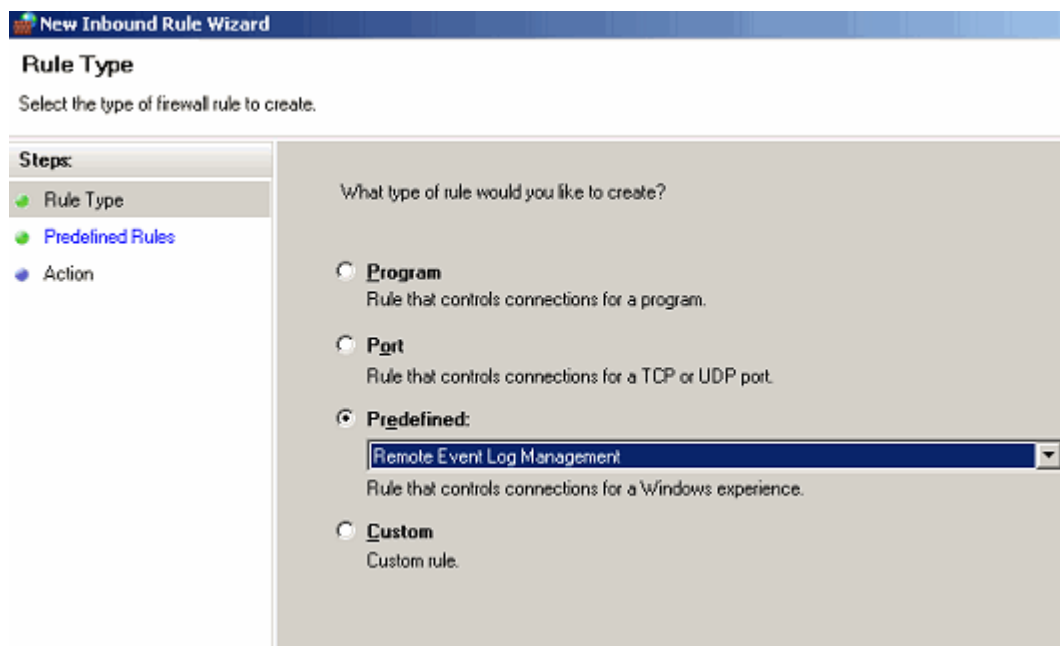
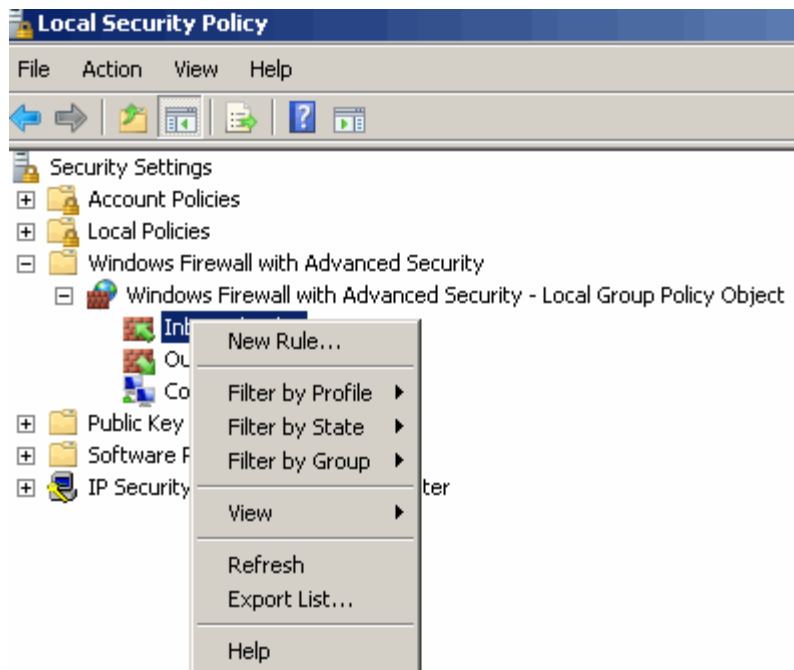
You will need to allow the **Remote Event Log Management** and **File and Print Sharing** exceptions in the Windows Firewall in order for WhatsUp Event Alarm to successfully monitor logs from Microsoft Vista/Server 2008/Windows 7 machines. The easiest way to do this is in a domain is to use a Group Policy Object that governs all Vista workstations and Server 2008 servers. On workgroup or standalone machines, you can either manually set the exception

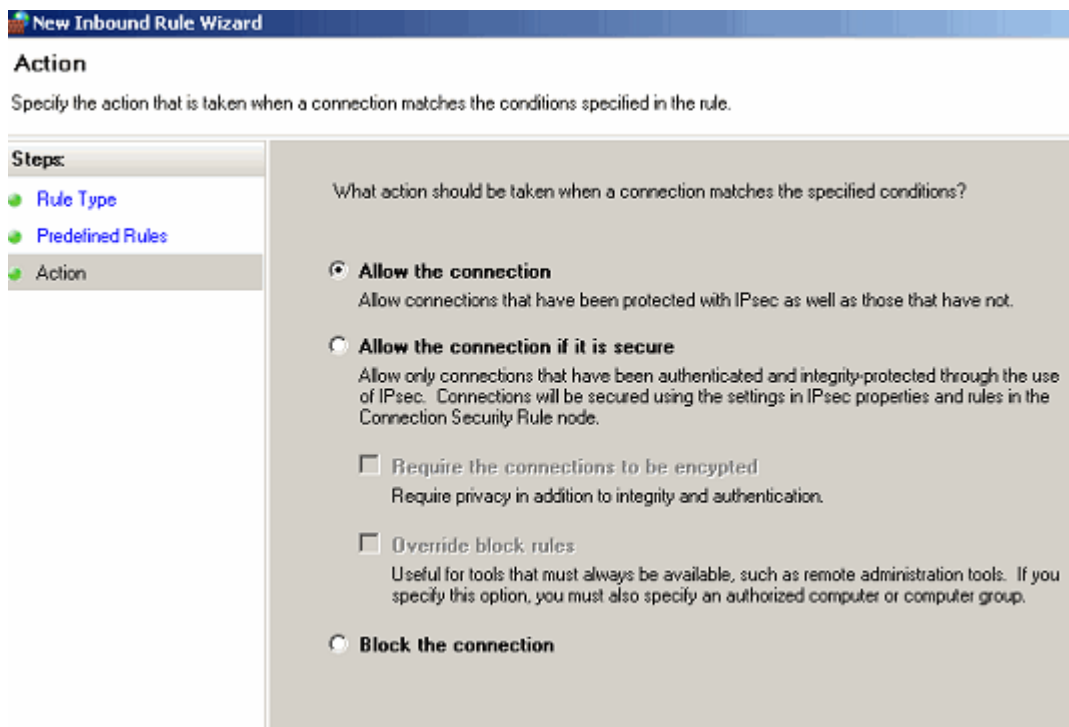
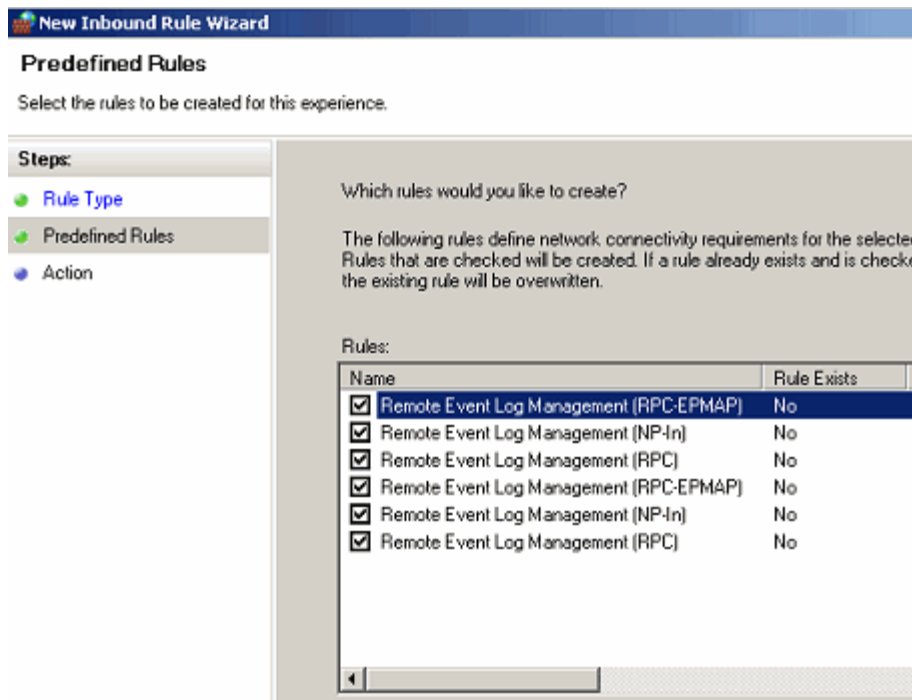
under the Windows Firewall Exceptions tab on each computer, or you can create a Local Security Policy template targeting the Windows Firewall with Advanced Security area and apply it to the Local Security Policy on each machine with the **secedit** command line tool.

In addition to the exceptions above, you may also want to allow ICMP (Ping) traffic between the machine running WhatsUp Event Alarm and your Vista/Windows 7 workstations and 2008 servers. By default, ICMP (Ping) traffic is disabled in Microsoft Windows Vista. However, ICMP Echo (Ping) testing is turned on by default in WhatsUp Event Alarm. This is by design to help the WhatsUp Event Alarm Service only scan event logs on computers that are online. If you do not want to allow ICMP traffic on your network, or block it at a router that WhatsUp Event Alarm must scan logs across, uncheck the Use ICMP Echo testing option in WhatsUp Event Alarm's Preferences dialog so your event logs can still be scanned as needed.



We recommend creating both an inbound and outbound rule allowing Remote Event Log Management and File and Print Sharing.





Other Recommendations

Network Performance / Usage

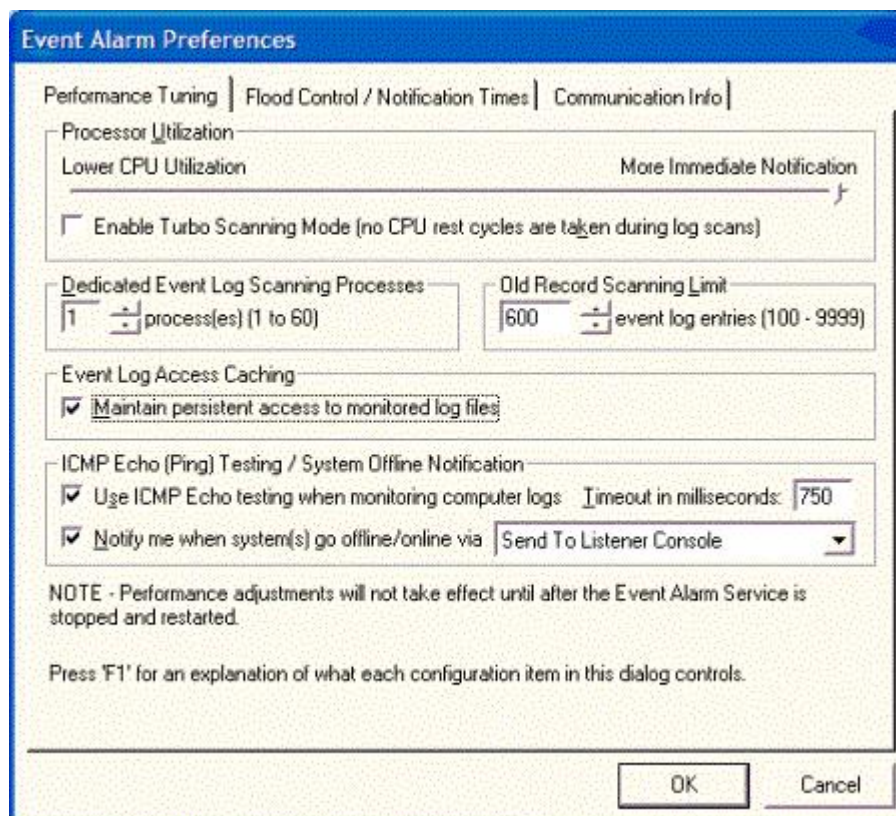
WhatsUp Event Alarm Help and Users Guide

WhatsUp Event Alarm works best in a well-connected LAN environment (e.g. 100 Mbit Ethernet or greater). As a general rule, it is best to locate your WhatsUp Event Alarm server near a Primary Domain Controller / Active Directory Server for the purpose of account lookups. If you plan to use WhatsUp Event Alarm in a WAN environment, it is beneficial to install a WhatsUp Event Alarm Server at each remote site to ensure new entries are scanned and processed in a timely manner.



Note: Scanning event log files over WAN links will most likely prove slow and unreliable, and is not recommended.

When deploying WhatsUp Event Alarm, you can install it on multiple servers (e.g. distributing the total monitoring load, where each WhatsUp Event Alarm station monitors a different subset of server/workstation logs on your LAN). By doing this, you can also take advantage of your network topology to minimize network traffic caused by the WhatsUp Event Alarm Service. On a LAN where the average server event log is not generating more than 25 entries per minute, network usage has been calculated to be approximately 6% of a 10Mbit connection, and less than 1 percent of a 100Mbit connection given WhatsUp Event Alarm's default settings. You can adjust how often WhatsUp Event Alarm scans your event logs (and consequently increase/reduce bandwidth use) via **Options > WhatsUp Event Alarm Preferences**. Settings of interest include the Processor Utilization slider, Turbo Scanning Mode and the Dedicated Event Log Scanning Processes number. See below for more information.



In addition, you may have very high activity servers on your network, such as email servers or domain controllers (Active Directory servers) logging hundreds of events per minute. In these

situations, it may be best to dedicate a WhatsUp Event Alarm installation to monitor those critical servers and use another WhatsUp Event Alarm installation to monitor the rest of logs on a network segment.

Memory and CPU Usage

You can control the resource burden placed on your WhatsUp Event Alarm server by configuring preferences via **Options > WhatsUp Event Alarm Preferences**. In general, if you want more immediate notification capabilities (e.g. receiving notification within seconds of a new event log entry being recorded), you must increase the resource burden (CPU, memory, and network traffic) on the WhatsUp Event Alarm Server. Conversely, if notifications need not be immediate, you can reduce the resource burden on the server and make it scan log entries more infrequently. The following three sections of the Preferences dialog should be configured based on your network's log activity volume:

Processor Utilization. This slider establishes a baseline number of milliseconds for how long the WhatsUp Event Alarm Service rests between each new scan of event logs stored in its log monitoring database. The default setting is 2000ms, or 2 seconds per run through all of the server logs being monitored. In addition, the service rests for 1/4 this value in between log entries (e.g. .5 seconds in this case). In this example, if you are monitoring 20 event logs, WhatsUp Event Alarm visits each log in a round robin fashion to scan for new entries. $20 \times .5 \text{ seconds} = 10 \text{ seconds}$ plus 2 seconds at the end of the run, representing a minimum interval of 12 seconds before a log is revisited again for a scan of new event log entries. On a larger network generating many event log entries, it may be necessary to reduce this interval and increase the number of scanning processes. Conversely, on a smaller network, you may be able to increase the interval and only use a single scanning process, if new events are logged infrequently on your servers.

Enable Turbo Scanning Mode. If you turn this option on, the WhatsUp Event Alarm Service will not yield any processor time during the intervals when it is actively scanning new events that have occurred on computer logs. Typically, this results in CPU utilization of 3 to 15% of total processor time per log scanning process used. Therefore, the more dedicated event log scanning processes you instruct WhatsUp Event Alarm to use (see below), the more total CPU time will be consumed. Enabling Turbo Scanning Mode is often useful if you are trying to scan many computers' event logs from one WhatsUp Event Alarm installation, especially if several of the servers audit many events per minute (e.g. Domain Controllers).

Dedicated Event Log Scanning Processes. This setting controls how many event logs can be scanned at the same time with the WhatsUp Event Alarm Service. Typically, the busier the network, the more event log scanning processes you want to use to keep up with the volume. E.g. if a few servers are generating hundreds of events per minute, you want to use multiple processes so that scanning the new entries in the busier servers will not unnecessarily delay the other logs needing to be scanned on the network. A good rule of thumb is to add an additional scanning process for every 1000 log entries / minute produced by your network. If the servers you were monitoring were producing a total of 4000 log entries / minute, you would want to use between 4 and 6 scanning processes.



Note: Each additional scanning process you create uses an additional 5 to 10 MB of system memory, on top of the 15MB working minimum for the WhatsUp Event Alarm Service and notification engine. Make sure you have enough RAM available on your monitoring server to support the additional processes.

Notification Options (and their respective strengths and weaknesses)

One of the first tasks you should undertake after installing WhatsUp Event Alarm is to define your notification methods (**Edit > Define Notifications**). Here are some recommendations on how to most effectively design them given your network's structure.

The most robust notification method is email. WhatsUp Event Alarm has been specially designed to be capable of generating hundreds of email messages per second using a multithreaded architecture. Email can be queued by SMTP servers pending delivery, and it is sent over a connection-oriented protocol (TCP/IP). Network popups are simple and convenient, but if too many are generated and sent to the same recipient, an NT/2000/XP/2003 desktop can only display a certain number (between 6-12) at a time before some messages are dropped. Network popups are also not necessarily connection-oriented, and therefore, delivery is not guaranteed. Syslog messages are also sent with a multithreaded architecture like email messages, but are not connection-oriented because they travel over the network as UDP packets. Lastly, pager notifications should be reserved for the most critical events on the most critical logs. This is because a modem cannot communicate with multiple pagers at once, and at best, can only send out two to three notifications per minute. Because most pagers/cell phones now support text messaging with email addresses, email can often be used to deliver messages to wireless devices, and is preferred over traditional numeric pager messages.

Also, every time specific notifications are sent out (e.g. email, network popup, syslog, or pager), the WhatsUp Event Alarm Service can be instructed to broadcast the same notification to all WhatsUp Event Alarm Listener Console clients listening in its primary domain. Multiple administrators can install and run the WhatsUp Event Alarm Listener Console application, and each one will be informed via the broadcast message when an alarm is triggered.

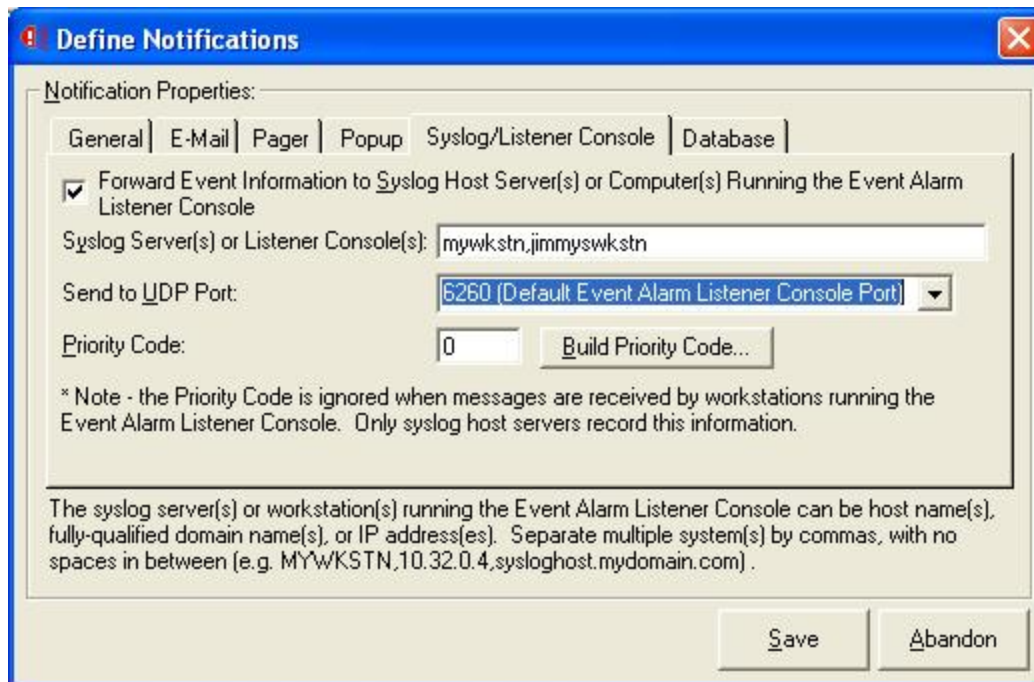


Note: You control whether this feature is enabled or disabled in the WhatsUp Event Alarm Preferences (**Options > WhatsUp Event Alarm Preferences**).

If you do not need to be informed immediately about a certain type of event happening on your network, but would like to review the data that was detected on a regular basis, you can define a notification that places event log data into an Access or ODBC database. Then, you can retrieve that data via queries you define, or you can use Ipswitch's specialized analysis tool, WhatsUp Event Analyst.



Note: You can combine notification types into a single defined notification in WhatsUp Event Alarm. For instance, you may want detected events sent to the WhatsUp Event Alarm Listener Console running on your desktop, but also placed into a SQL database. Check and configure both of these types when defining a single notification.



Setting Alarms

WhatsUp Event Alarm ships with many predefined alarms for the Microsoft Windows NT/2000/XP/2003/Vista/2008 operating systems. You can add your own to WhatsUp Event Alarm's database by clicking the **Edit** menu, and then select **Define Alarms**.

As a general rule, be conservative when setting alarms. It is best only to select alarms that reflect critical situations on particular computers (e.g. a bad login, low disk space, fault-tolerant disk error, etc). The more alarms you attach to a log, the longer it takes WhatsUp Event Alarm to scan through new entries that occur on that event log. In general, if you need a large range of possible events, set fewer but broader alarms. For instance, instead of creating 10 alarms each scanning for a particular EventID, create an alarm that is associated with a certain type of event (e.g. error) and source (e.g. Microsoft Exchange Server) - or a category and type of event (e.g. Account Management - Success Audits).

Rapid Configuration Chooser Dialog

Before performing a rapid configuration, you must first indicate whether you want to create a new one, or edit an existing one that was run and saved previously.

I am creating a new rapid configuration for the following domain/workgroup

Choose this option to select the domain or workgroup containing the computers you wish to configure, and then create a new rapid configuration.

I am editing an existing rapid configuration

Select this option to choose from one or more existing rapid configurations in order to edit their settings and reapply them to certain computers.

Show this dialog at startup. If checked, this dialog displays when the WhatsUp Event Alarm Control Panel loads, allowing you to create or edit a rapid configuration.

OK. Closes the dialog and allows you start preparing a rapid configuration with the Rapid Configuration tool.

Cancel. Closes the dialog without taking any further action.

Rapid Configuration Chooser Dialog

Before performing a rapid configuration, you must first indicate whether you want to create a new one, or edit an existing one that was run and saved previously.

I am creating a new rapid configuration for the following domain/workgroup

Choose this option to select the domain or workgroup containing the computers you wish to configure, and then create a new rapid configuration.

I am editing an existing rapid configuration

Select this option to choose from one or more existing rapid configurations in order to edit their settings and reapply them to certain computers.

Show this dialog at startup. If checked, this dialog displays when the WhatsUp Event Alarm Control Panel loads, allowing you to create or edit a rapid configuration.

OK. Closes the dialog and allows you start preparing a rapid configuration with the Rapid Configuration tool.

Cancel. Closes the dialog without taking any further action.

Service Account Dialog

Use the Service Account dialog to configure the WhatsUp Event Alarm Service to run under a specific user account. If WhatsUp Event Alarm is installed on a computer participating in a domain, this account must have domain administrative rights, or at minimum, a domain user account with local administrative rights on all member servers and workstations being monitored (e.g. an OU admin account), since it is responsible for reading event logs on domain computers over the network. If you are running WhatsUp Event Alarm on a computer not participating in a domain, or you 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.



Note: This dialog does not set the service account for the Syslog Bridge service. The WhatsUp Event Alarm Syslog Bridge service should always run under the default LocalSystem account.

Setting Up the WhatsUp Event Alarm Service with the Service Account dialog field descriptions

- § **I want to choose a domain account from a domain.** Attempts to populate the Account Name listing with all user accounts present in the primary domain where you are running WhatsUp Event Alarm.
- § **I want to choose a local account from this computer.** Attempts to populate the Account Name listing with all of the user accounts present on the computer where WhatsUp Event Alarm is installed.
- § **Account Name.** Choose the name of the user account you want the WhatsUp Event Alarm service to run under. If WhatsUp Event Alarm cannot automatically populate this list with account names, you can type in an account name yourself. Ensure 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, type in IPSWITCH\EAService.



Make sure this user account is in the local administrators group on each member server/workstation in the domain, if monitoring 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 monitor logs from the local computer, or are planning to monitor logs from other workgroup machines that have a common administrator account, make the service account a local administrator. The WhatsUp Event Alarm service will not run properly under a LocalSystem context.

You must select an account that is not subject to routine password expiration. If the WhatsUp Event Alarm Service account password expires, the service stops working and logs are no longer monitored.

- § **Password.** Type the password of the account you listed in the Account Name field.
- § **Confirm Password.** Retype the password for verification.
- § **OK.** WhatsUp Event Alarm reconfigures the WhatsUp Event Alarm Service to run under the account you specified. In addition, it attempts to add the **Log on as a service** and **Act as part of the operating system** user rights to the account to ensure proper operation. If for any reason it cannot add these user rights (e.g. your currently logged-on account is not an admin), it displays a warning message with instructions on how to add these rights manually.
- § **Cancel.** Aborts the account reconfiguration and leaves the current WhatsUp Event Alarm Service account unchanged.

Setting Up the WhatsUp Event Alarm Service Account Manually

If for any reason you cannot set the WhatsUp Event Alarm Service account from within the Service Account dialog, you can perform this process manually by visiting the **Control Panel > Administrative Tools > Services** and using the Services MMC Snapin.

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

- § The service account is a local administrator (e.g. in the local Administrators group) on every member server and workstation you plan to monitor. 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 monitor domain controllers, only Domain Admins can perform this action.
- § 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
- § The service account's password will not expire due to account policies in your domain.

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

Build Priority Dialog

Use the Build Priority dialog to create a priority number that is appended to syslog messages sent by WhatsUp Event Alarm. A syslog priority number is a combination of a facility value (where the facility typically indicates the subsystem or process generating the message) and a level value (indicating the severity of the message). The priority value is calculated as follows:

$(\text{Facility Value} \times 8) + \text{Level Value}$

The facilities and levels included in this dialog are taken from RFC 3164; the BSD Syslog Protocol. If you have a different facility and level structure on your syslog host server, calculate the priority value manually and type the number directly in the Notifications dialog.

Select Facility. Choose the subsystem or process you want to associate with the syslog message.

Select Level. Choose the severity level of the syslog message.

OK. Calculates the priority value from the facility and level, and returns this number to the Notifications dialog.

Cancel. Closes the dialog without returning a priority value.

Facilities Supported by WhatsUp Event Alarm (and their number)

Kernel 0

User 1

Mail 2

Daemon 3

Auth 4

Syslog 5

LPR 6

News 7

UUCP 8

Cron 9

Security 10

FTP 11

NTP 12

LogAudit 13

LogAlert 14

Clock 15

Local0 16

Local1 17

Local2 18

Local3 19

Local4 20

Local5 21

Local6 22

Local7 23

Levels Supported by WhatsUp Event Alarm (and their number)

Emergency 0

Alert 1

Critical 2

Error 3

Warning 4

Notice 5

Information 6

Debug 7

WhatsUp Event Alarm Log Entries Viewer Dialog

If 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 warnings 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. When launched, the WhatsUp Event Alarm Log Entries Viewer dialog loads all of the WhatsUp Event Alarm Service events from the Windows event log. You can filter out certain types of activity by unchecking 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 Alarm 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 Software Support, click **Export to HTML**.



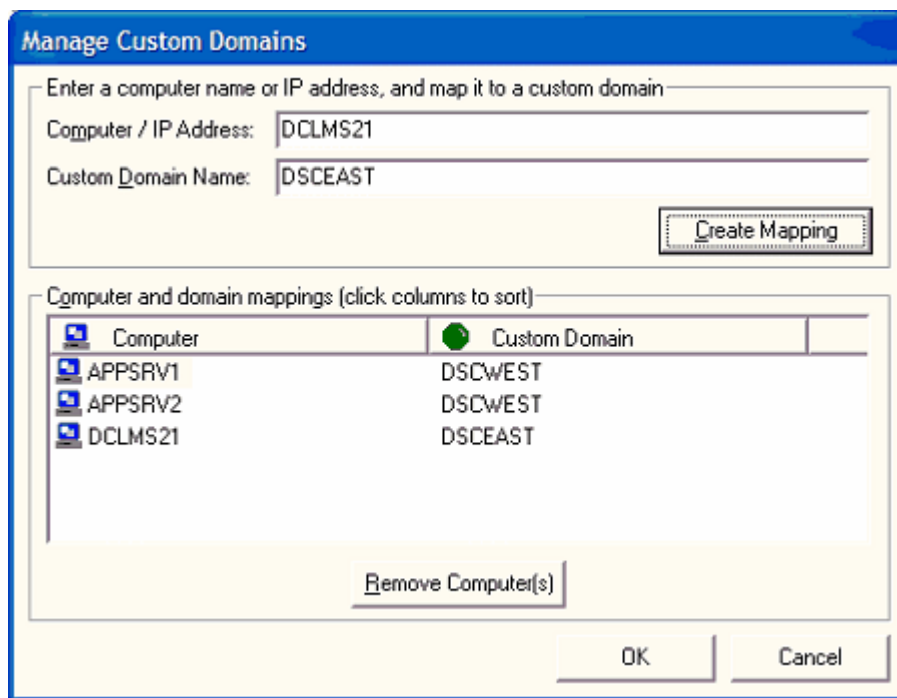
Note: Only WhatsUp Event Alarm Service events currently present in the active Application Event Log are displayed. Older events may already be archived into saved EVT files, and if so, you must load those older files in the Microsoft Event Viewer to view their contents.

Custom Domain Manager Dialog

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

For example, delegation of administration may require you to monitor specific servers in three different organizational units of a larger domain. Or, you may have to monitor logs from servers and workstations that reside in different workgroups. Using WhatsUp Event Alarm,

you can map these individual computer names to a custom domain. Then, you can easily reference that custom domain to adjust log-monitoring settings on all of these computers at once using built-in WhatsUp Event Alarm wizards or Rapid Configuration tool.



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 are created as above, WhatsUp Event Alarm displays two additional domains in its domain list in the upper right corner of the WhatsUp Event Alarm Control Panel, specifically CUSTOM: MYDOMAIN1 and CUSTOM: MYDOMAIN2. When you change focus to one of the custom domains, WhatsUp Event Alarm shows all computer logs monitored in that custom domain. Furthermore, when you add a computer log for individual monitoring, or when you complete a wizard to setup monitoring on many computers' logs at the same time, WhatsUp Event Alarm displays all computer names associated with the currently selected custom domain.



Note: To monitor all types of logs successfully from computers, the WhatsUp Event Alarm Service must run under a.) an account whose user name and password is common to all machines in the custom domain whose logs are being monitored, and b.) an account 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 selected computers from the list above, disassociating them from the custom domain.

OK. Saves computer to custom domain mappings.

Cancel. Cancels the operation without saving the changes.

Computer Name Retrieval Dialog

When setting up computer logs for monitoring (either individually or via a wizard or Rapid Configuration), WhatsUp Event Alarm presents you with a list of computers to choose from. You can control how WhatsUp Event Alarm prepares this list of computers in certain dialogs by setting the appropriate option in the Computer Name Retrieval Dialog as well as the *Custom Domain Manager* (on page 97) dialog.

Computer Name Retrieval Options

The Browse List. Choose this option if you are using WhatsUp Event Alarm to monitor logs in a workgroup, not a domain. WhatsUp Event Alarm 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 Alarm to monitor logs from a domain or multiple domains. When selected, WhatsUp Event Alarm enumerates all computer accounts directly from the domain controller / Active Directory server. This can take a while on very large domains.

The Following OU in Active Directory. If you are only monitoring logs on servers in a particular organizational unit in your Active Directory, select this option. Once selected, use the browse (...) button to select the organizational unit from which you want to retrieve computer accounts.

Creating Custom Computer Lists with the Manage Custom Domains Dialog

You can also create specialized lists of computers and group them into related custom domains. For more information, refer to the *Custom Domain Manager* (on page 97) dialog help topic.