WhatsUp Event Alarm v10x Quick Setup Guide

CHAPTER 1 WhatsUp Event Alarm Quick Setup Guide

CHAPTER 2 Manually Creating Firewall Exceptions

CHAPTER 3 Other Recommendations

CHAPTER 1

WhatsUp Event Alarm Quick Setup Guide

In This Chapter

Thank you for choosing to evaluate WhatsUp Event Alarm! Please read the following topics in this help file thoroughly before beginning your installation and configuration.

Click on any of the topics below to review them in depth.

Installation Requirements (on page 18)

Manually Creating Firewall Exceptions (on page 20)

Before You Begin (on page 6)

Vista Requirements and Recommendations (on page 3)

Other Recommendations (on page 21)

Legal Information Including Patent and Trademark Notices

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 NT®, Microsoft Windows 2000®, Microsoft Windows XP®, Microsoft Windows 2003®, Microsoft Windows Vista®, Microsoft Windows Server 2008®, Microsoft Windows 7®, Microsoft Access®, and Microsoft SQL Server® are all registered trademarks of Microsoft Corp. Microsoft Windows NT®, Microsoft Windows 2000®, Microsoft Windows XP®, Microsoft Windows 2003®, Microsoft Windows Vista®, Microsoft Windows Server 2008®, Microsoft Windows 7®, Microsoft Access®, Microsoft Exchange® and Microsoft SQL Server® will hereafter be referred to as NT, 2000, XP, 2003, Vista, 2008, Windows 7, Access, Exchange, and SQL Server respectively. Oracle® is a registered trademark of the Oracle Corporation. All other products or technologies not specifically mentioned here are the registered trademarks of their respective companies, and are used by permission.

Ipswitch Contact Information

Ipswitch, Inc.

Phone: 800-793-4825 / 781-676-5700 Fax: 781-676-5715

WWW: http://www.whatsupgold.com

Microsoft Vista/Server 2008/Windows 7 Requirements/Recommendations

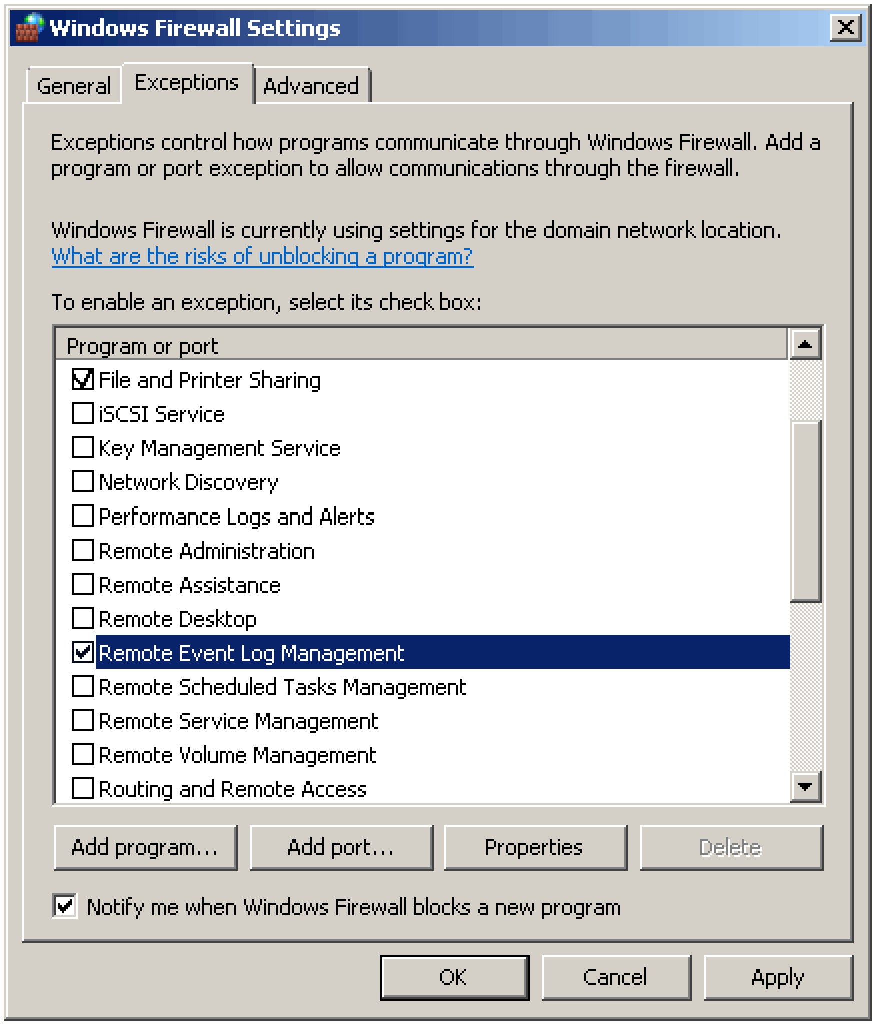
To monitor active Microsoft Vista / Windows Server 2008 / Windows 7 logs in the new EVTX format, WhatsUp Event Alarm must be installed on a Microsoft Vista or later operating system. If you attempt to monitor active Microsoft Vista/2008/7 logs when WhatsUp Event Alarm is installed on an older operating 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 at 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.



Windows Firewall Settings

Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

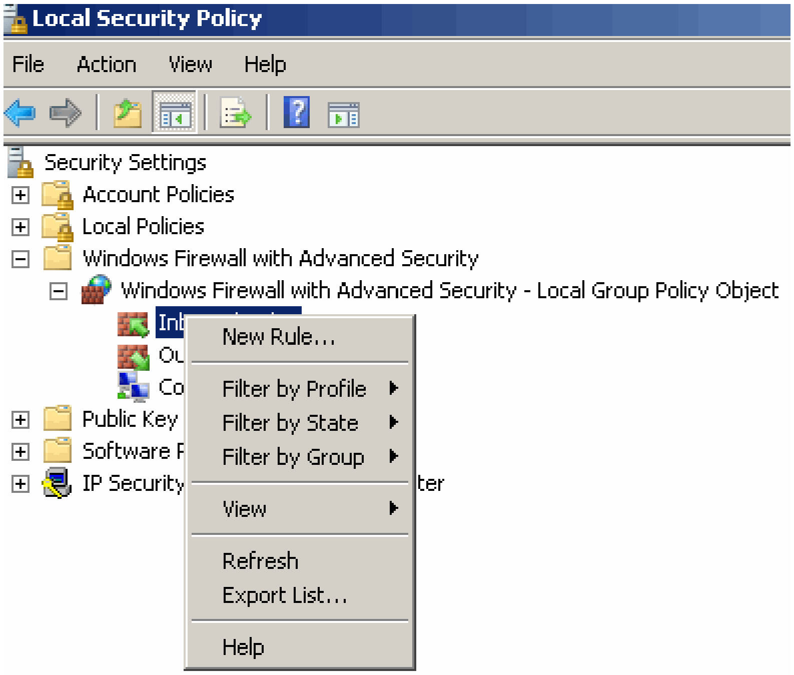
Windows Firewall is currently using settings for the domain network location.
What are the risks of unblocking a program?

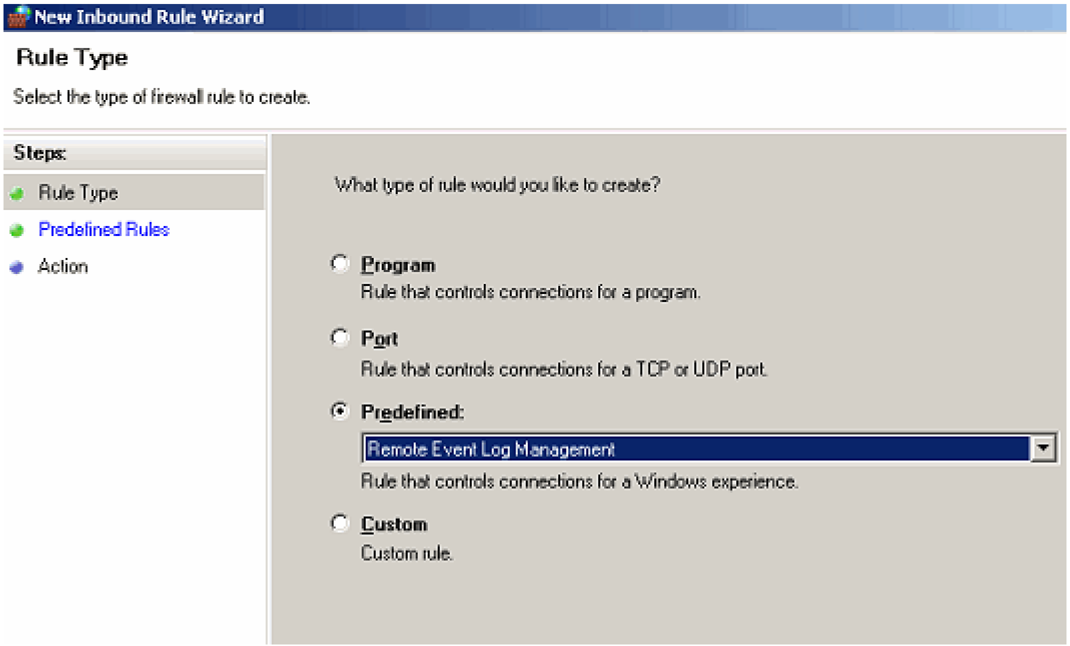
To enable an exception, select its check box:

Program or port
☑ File and Printer Sharing
☐ iSCSI Service
☐ Key Management Service
☐ Network Discovery
☐ Performance Logs and Alerts
☐ Remote Administration
☐ Remote Assistance
☐ Remote Desktop
☑ Remote Event Log Management
☐ Remote Scheduled Tasks Management
☐ Remote Service Management
☐ Remote Volume Management
☐ Routing and Remote Access

☑ Notify me when Windows Firewall blocks a new program

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





Rule Type

Select the type of firewall rule to create.

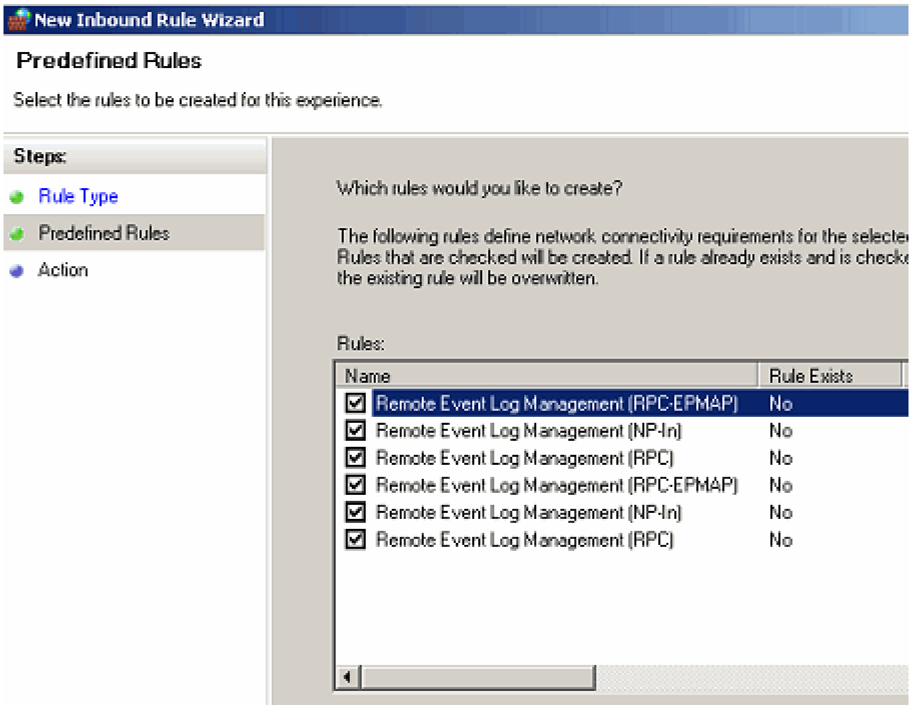
What type of rule would you like to create?

○ Program
Rule that controls connections for a program.

○ Port
Rule that controls connections for a TCP or UDP port.

● Predefined:
Remote Event Log Management
Rule that controls connections for a Windows experience.

○ Custom
Custom rule.



New Inbound Rule Wizard

Predefined Rules

Select the rules to be created for this experience.

Steps:

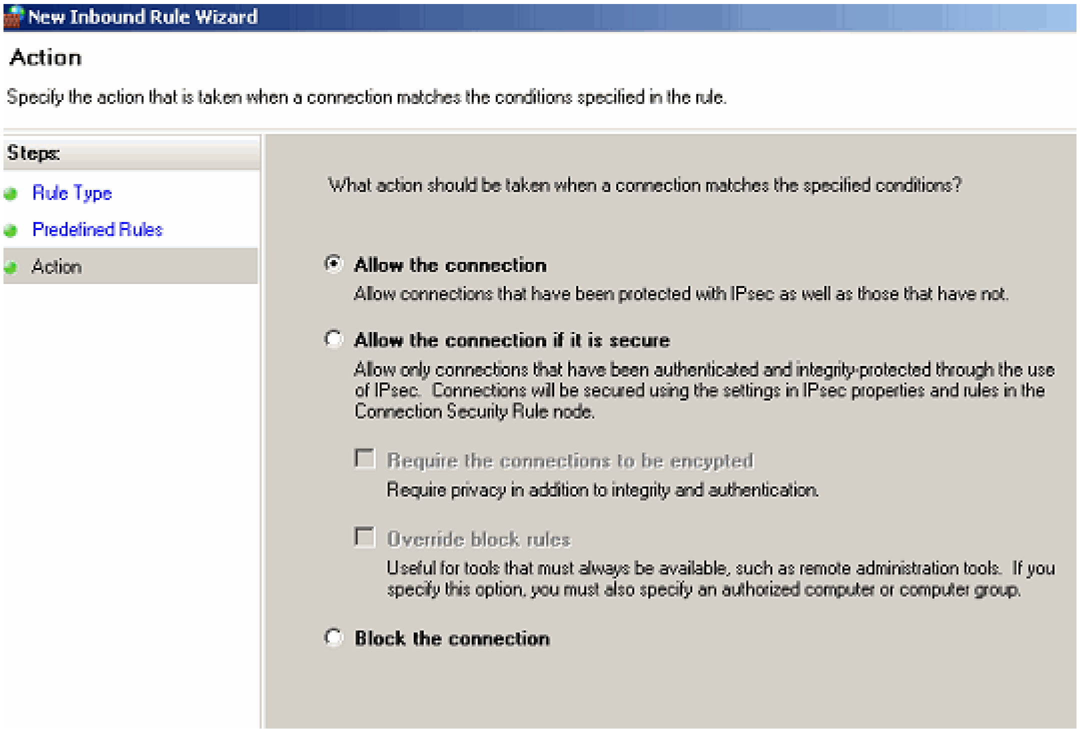
- Rule Type
- Predefined Rules
- Action

Which rules would you like to create?

The following rules define network connectivity requirements for the selecte
Rules that are checked will be created. If a rule already exists and is checke
the existing rule will be overwritten.

Rules:

Name	Rule Exists
☑ Remote Event Log Management (RPC-EPMAP)	No
☑ Remote Event Log Management (NP-In)	No
☑ Remote Event Log Management (RPC)	No
☑ Remote Event Log Management (RPC-EPMAP)	No
☑ Remote Event Log Management (NP-In)	No
☑ Remote Event Log Management (RPC)	No



New Inbound Rule Wizard

Action

Specify the action that is taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Predefined Rules
- Action

What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
Allow connections that have been protected with IPsec as well as those that have not.

○ **Allow the connection if it is secure**
Allow only connections that have been authenticated and integrity-protected through the use of IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

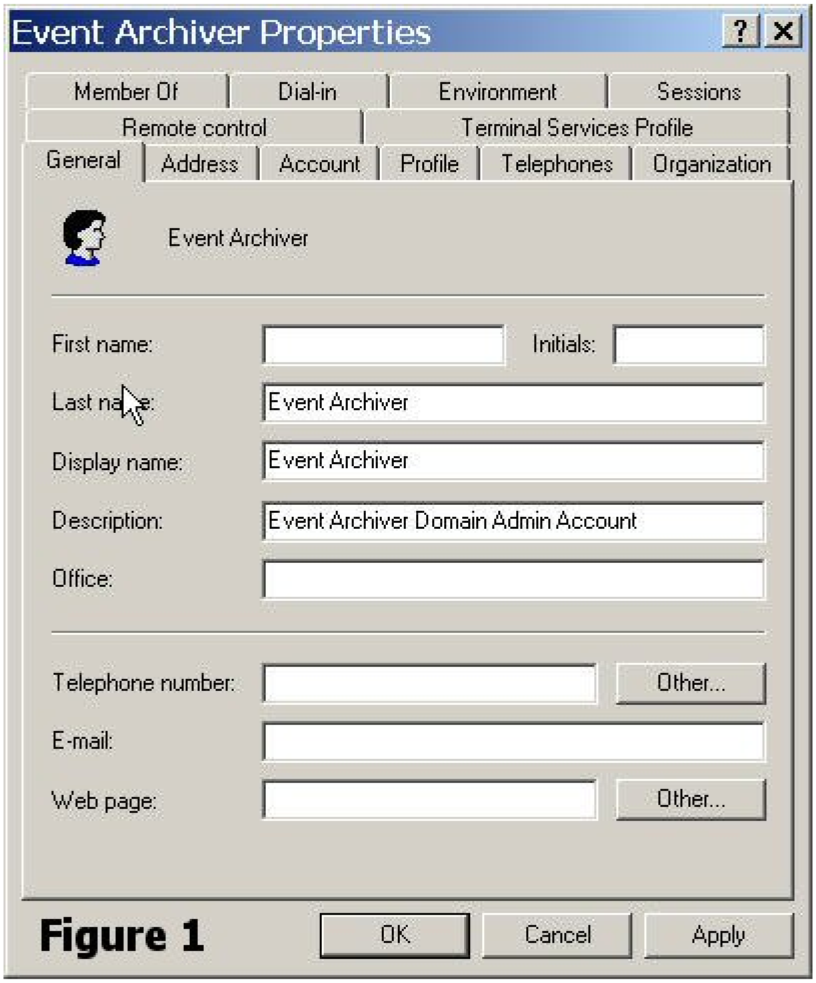
□ Require the connections to be encypted
Require privacy in addition to integrity and authentication.

□ Override block rules
Useful for tools that must always be available, such as remote administration tools. If you specify this option, you must also specify an authorized computer or computer group.

○ **Block the connection**

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.

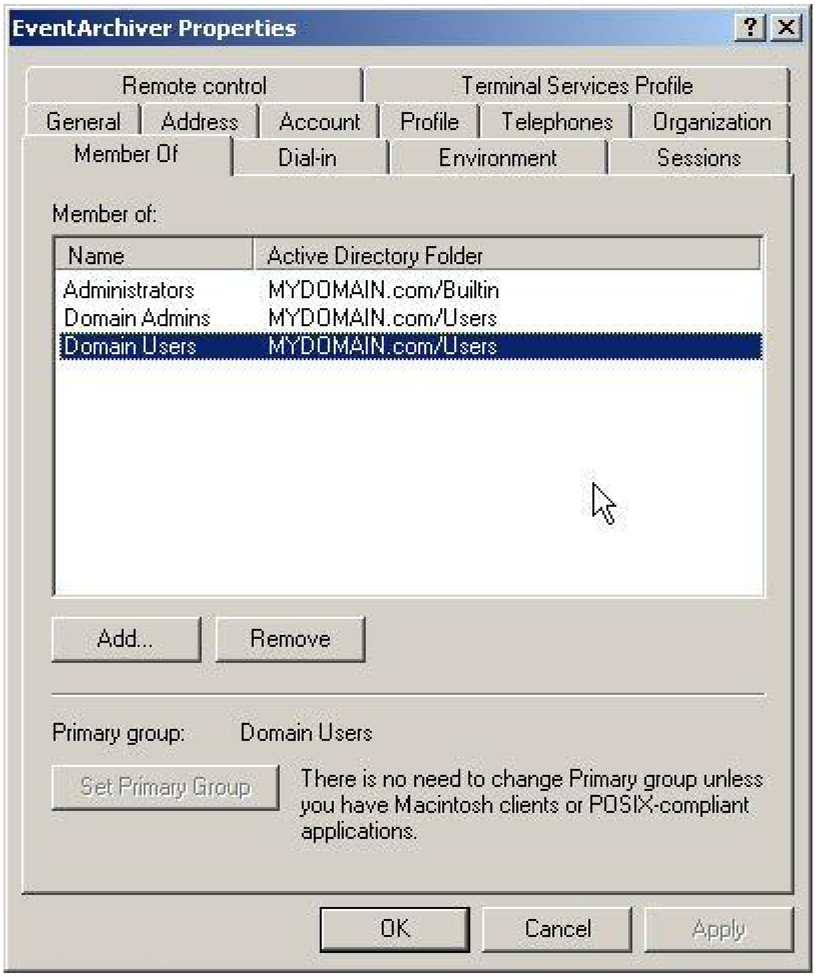


Last name: Event Archiver

Display name: Event Archiver

Description: Event Archiver Domain Admin Account

Figure 1



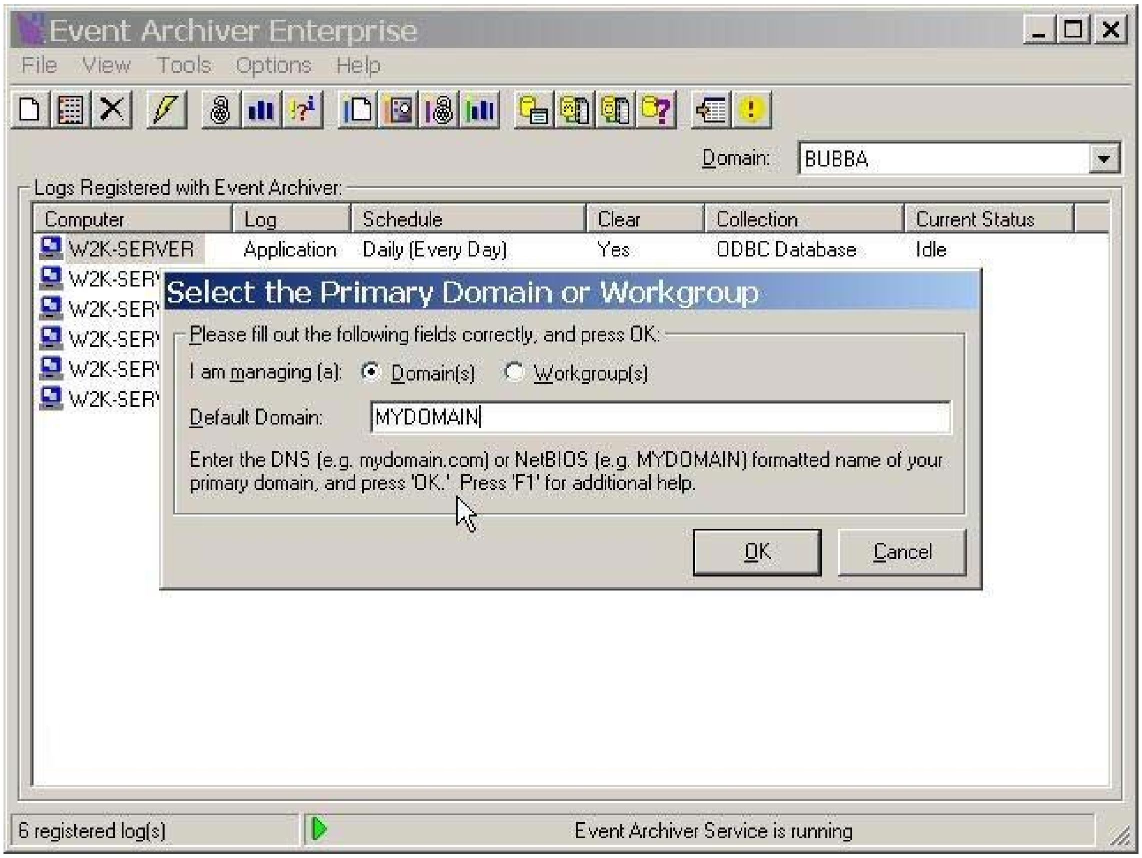
Member of:

Name	Active Directory Folder
Administrators	MYDOMAIN.com/Builtin
Domain Admins	MYDOMAIN.com/Users
Domain Users	MYDOMAIN.com/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

2 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.



Domain: BUBBA

Logs Registered with Event Archiver:

Computer	Log	Schedule	Clear	Collection	Current Status
W2K-SERVER	Application	Daily (Every Day)	Yes	ODBC Database	Idle
W2K-SER'					
W2K-SER'					
W2K-SER'					
W2K-SER'					
W2K-SER'					

Select the Primary Domain or Workgroup

Please fill out the following fields correctly, and press OK:

I am managing (a): ● Domain(s) ○ Workgroup(s)

Default Domain: MYDOMAIN

Enter the DNS (e.g. mydomain.com) or NetBIOS (e.g. MYDOMAIN) formatted name of your primary domain, and press 'OK.' Press 'F1' for additional help.

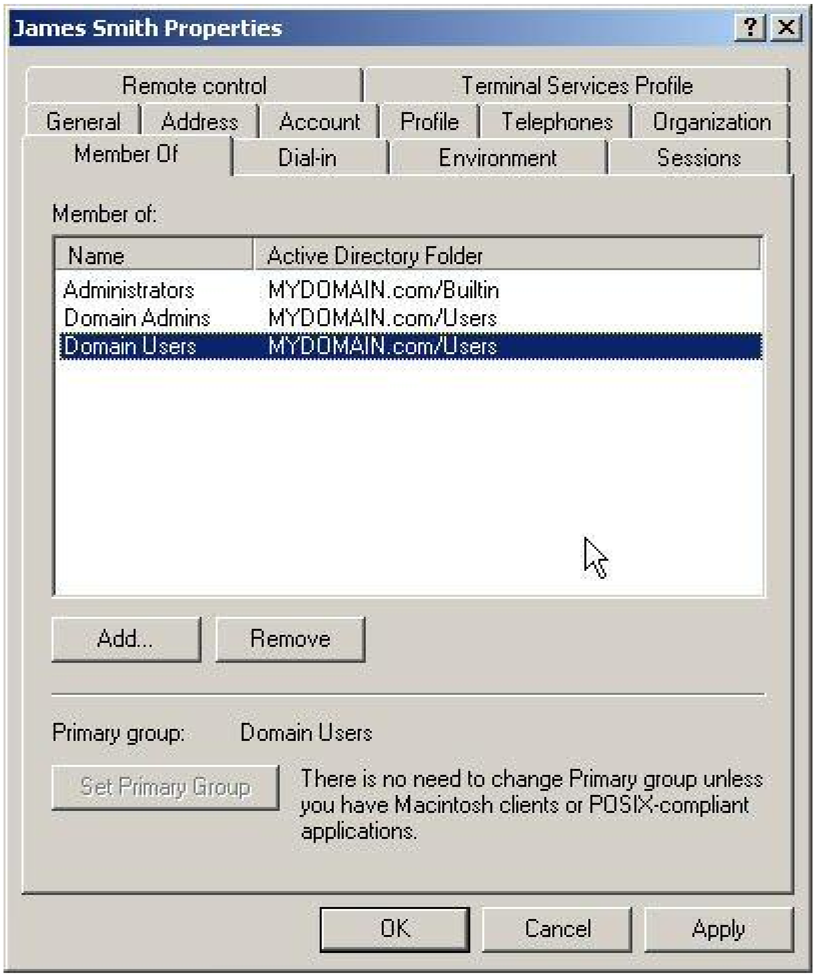
6 registered log(s) Event Archiver Service is running

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.

3 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.



Member of:

Name	Active Directory Folder
Administrators	MYDOMAIN.com/Builtin
Domain Admins	MYDOMAIN.com/Users
Domain Users	MYDOMAIN.com/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

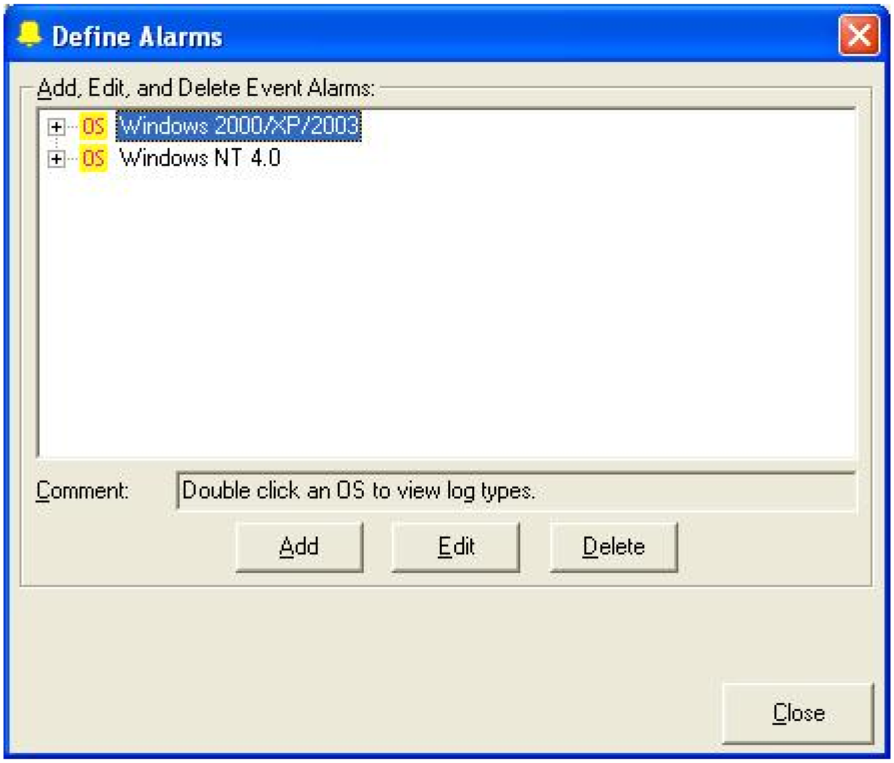
To increase log scanning time, if the majority of the systems being monitored are running Windows 2003, install WhatsUp Event Alarm on a Windows 2003 server. Likewise, a majority of Windows 2008 servers should be watched by WhatsUp Event Alarm running on a Windows 2008 server, etc.

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.

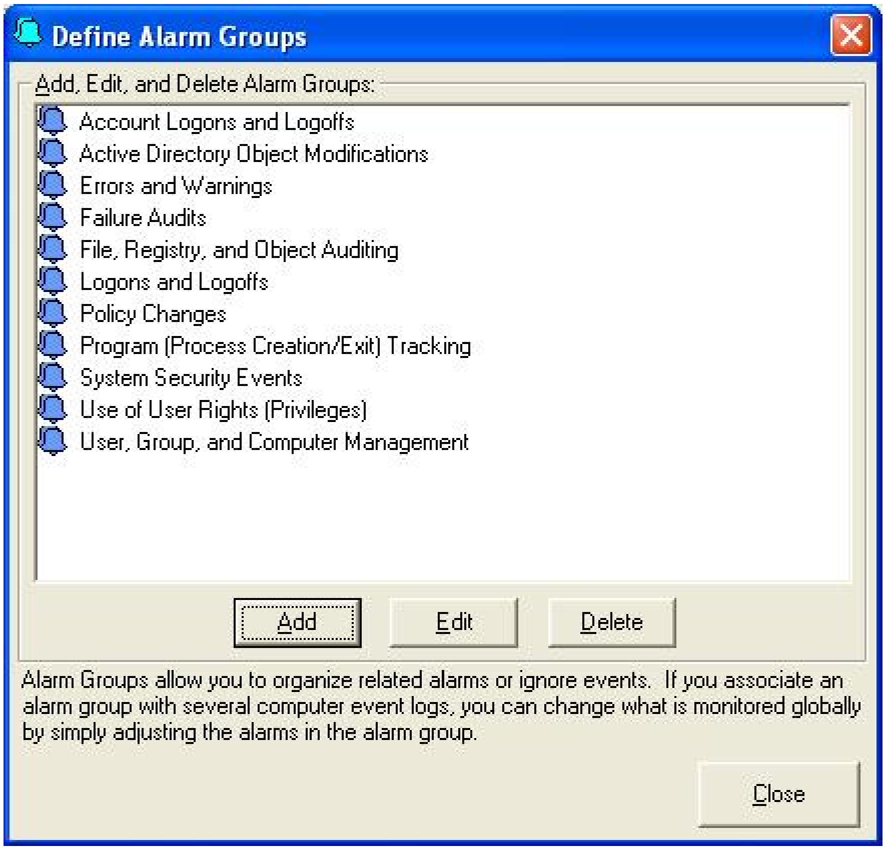


Define Alarms

Add, Edit, and Delete Event Alarms:

- OS Windows 2000/XP/2003
- OS Windows NT 4.0

Comment: Double click an OS to view log types.

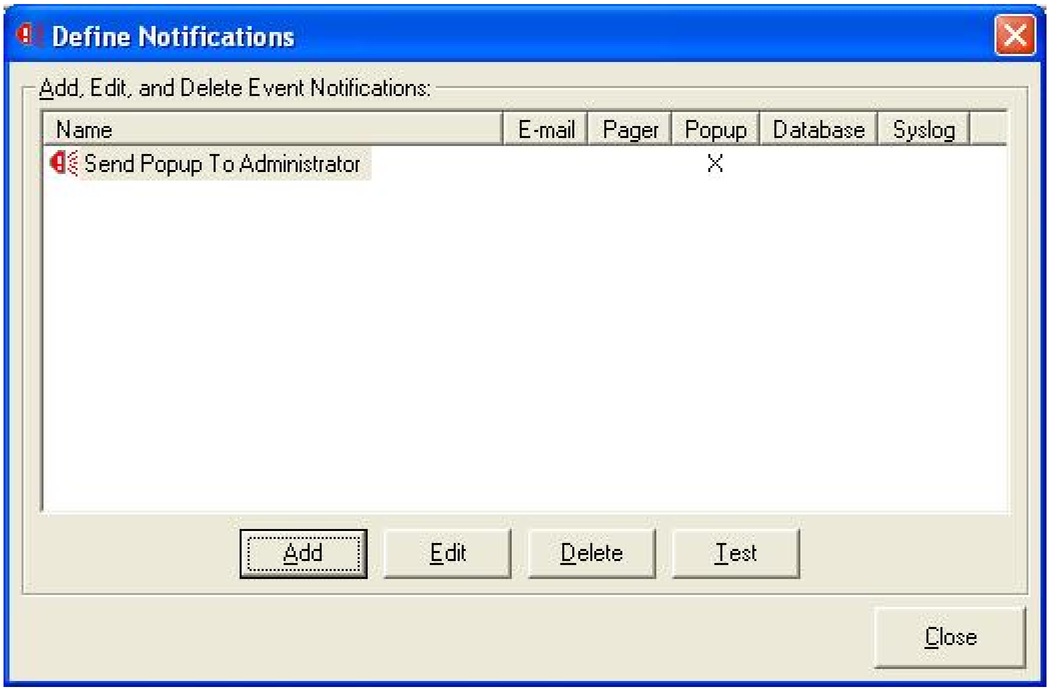


Define Alarm Groups

Add, Edit, and Delete Alarm Groups:

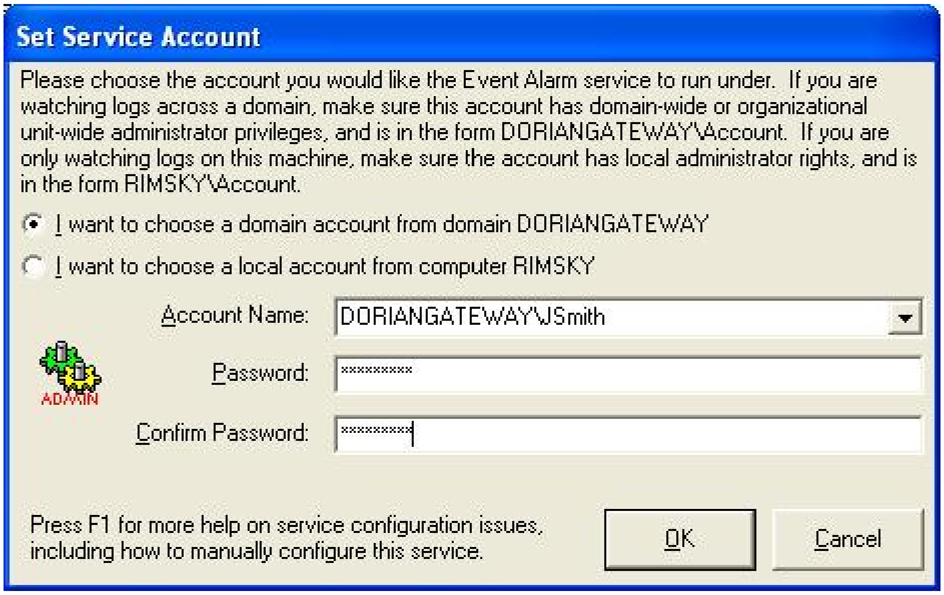
- Account Logons and Logoffs
- Active Directory Object Modifications
- Errors and Warnings
- Failure Audits
- File, Registry, and Object Auditing
- Logons and Logoffs
- Policy Changes
- Program (Process Creation/Exit) Tracking
- System Security Events
- Use of User Rights (Privileges)
- User, Group, and Computer Management

Alarm Groups allow you to organize related alarms or ignore events. If you associate an alarm group with several computer event logs, you can change what is monitored globally by simply adjusting the alarms in the alarm group.



Name	E-mail	Pager	Popup	Database	Syslog
Send Popup To Administrator			X		

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).



Set Service Account

Please choose the account you would like the Event Alarm service to run under. If you are watching logs across a domain, make sure this account has domain-wide or organizational unit-wide administrator privileges, and is in the form DORIANGATEWAY\Account. If you are only watching logs on this machine, make sure the account has local administrator rights, and is in the form RIMSKY\Account.

● I want to choose a domain account from domain DORIANGATEWAY

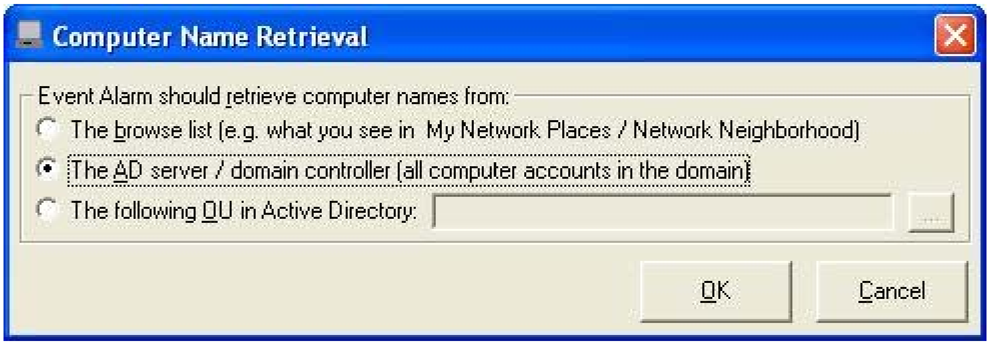
○ I want to choose a local account from computer RIMSKY

Account Name: DORIANGATEWAY\JSmith

Password: **********

Confirm Password: *********

Press F1 for more help on service configuration issues, including how to manually configure this service.



Computer Name Retrieval

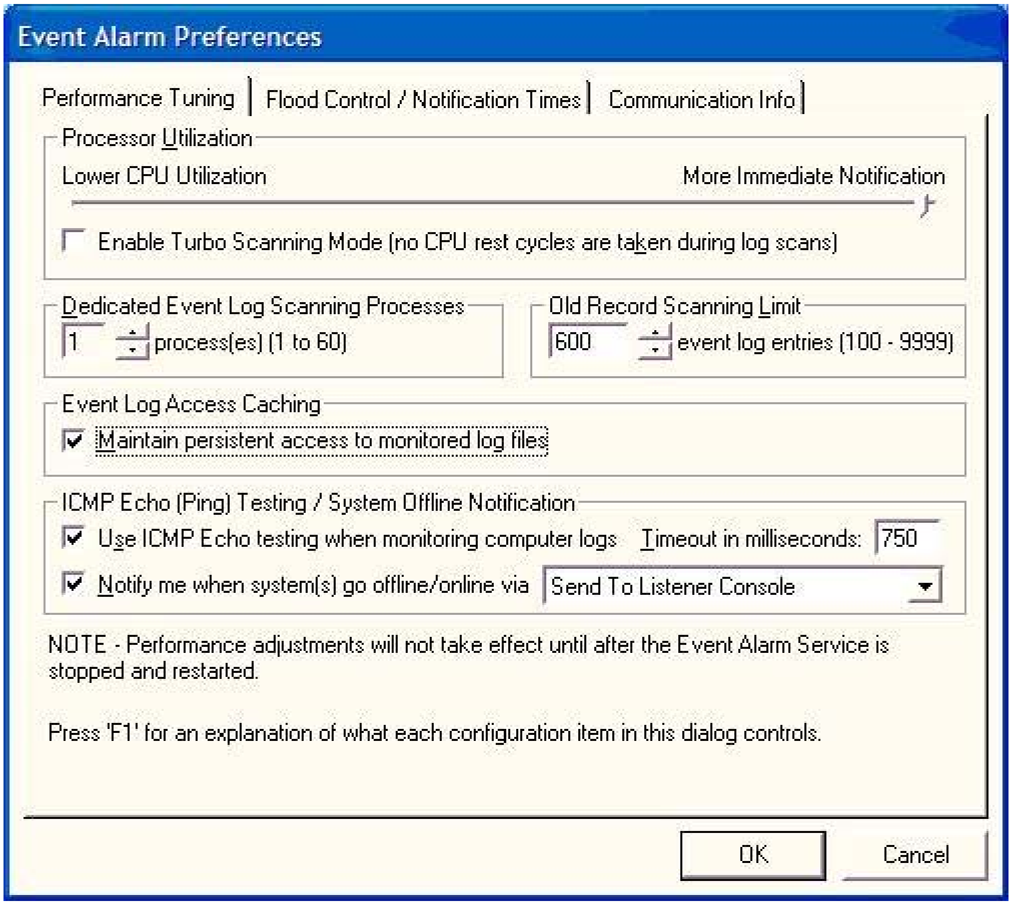
Event Alarm should retrieve computer names from:

○ The browse list (e.g. what you see in My Network Places / Network Neighborhood)

● The AD server / domain controller (all computer accounts in the domain)

○ The following OU in Active Directory:

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 Utilization

Lower CPU Utilization — More Immediate Notification

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

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

Old Record Scanning Limit: 600 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: 750

☑ Notify me when system(s) go offline/online via: Send To Listener Console

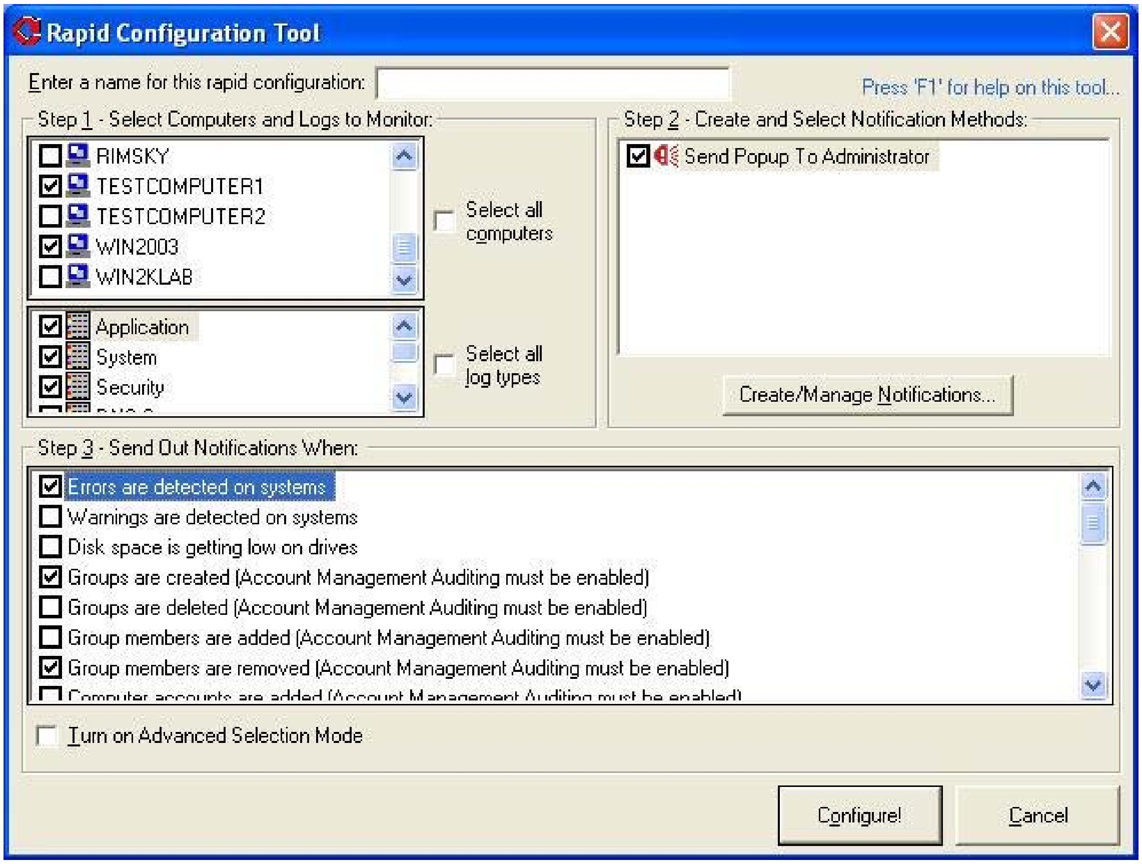
NOTE - Performance adjustments will not take effect until after the Event Alarm Service is stopped and restarted.

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

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 at 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.



Rapid Configuration Tool

Enter a name for this rapid configuration:

Press 'F1' for help on this tool...

Step 1 - Select Computers and Logs to Monitor:

- □ RIMSKY
- ☑ TESTCOMPUTER1
- □ TESTCOMPUTER2
- ☑ WIN2003
- □ WIN2KLAB

□ Select all computers

- ☑ Application
- ☑ System
- ☑ Security

□ Select all log types

Step 2 - Create and Select Notification Methods:

- ☑ Send Popup To Administrator

Step 3 - Send Out Notifications When:

- ☑ Errors are detected on systems
- □ Warnings are detected on systems
- □ Disk space is getting low on drives
- ☑ Groups are created (Account Management Auditing must be enabled)
- □ Groups are deleted (Account Management Auditing must be enabled)
- □ Group members are added (Account Management Auditing must be enabled)
- ☑ Group members are removed (Account Management Auditing must be enabled)
- □ Computer accounts are added (Account Management Auditing must be enabled)

□ Turn on Advanced Selection Mode

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.

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.

CHAPTER 2

Manually Creating Firewall Exceptions

In This Chapter

Manually Creating Firewall Exceptions

During the installation process, WhatsUp Event Archiver creates firewall exceptions for all critical ports. However, if the Windows firewall is turned off at the time of installation, WhatsUp Event Archiver does not create a firewall exception for the Windows firewall. If you decide to turn on the Windows firewall after you install WhatsUp Event Archiver, you must manually create a Windows firewall exception for WhatsUp Event Archiver to work properly.

Note: The steps below may vary slightly based on your operating system

To manually create a Windows firewall exception

1 From the Windows Start menu, click **Control Panel**, then select **System and Security**.

Note: Depending on your operating system, your selection may vary. For example, from the Control Panel, you may see an option for Windows Firewall, in which case you would select Windows Firewall.

2 Click **Windows Firewall**, then select **Allow programs to communicate through Windows Firewall**.

3 Click the **Allow Another Program** button.

4 Browse to **Program Files(X86) > Common Files > Ipswitch > Syslog Listener**.

5 Select the **Service Host** check box, then click **Add**.

6 Check the **Domain** check box associated with Service Host.

CHAPTER 3

Other Recommendations

In This Chapter

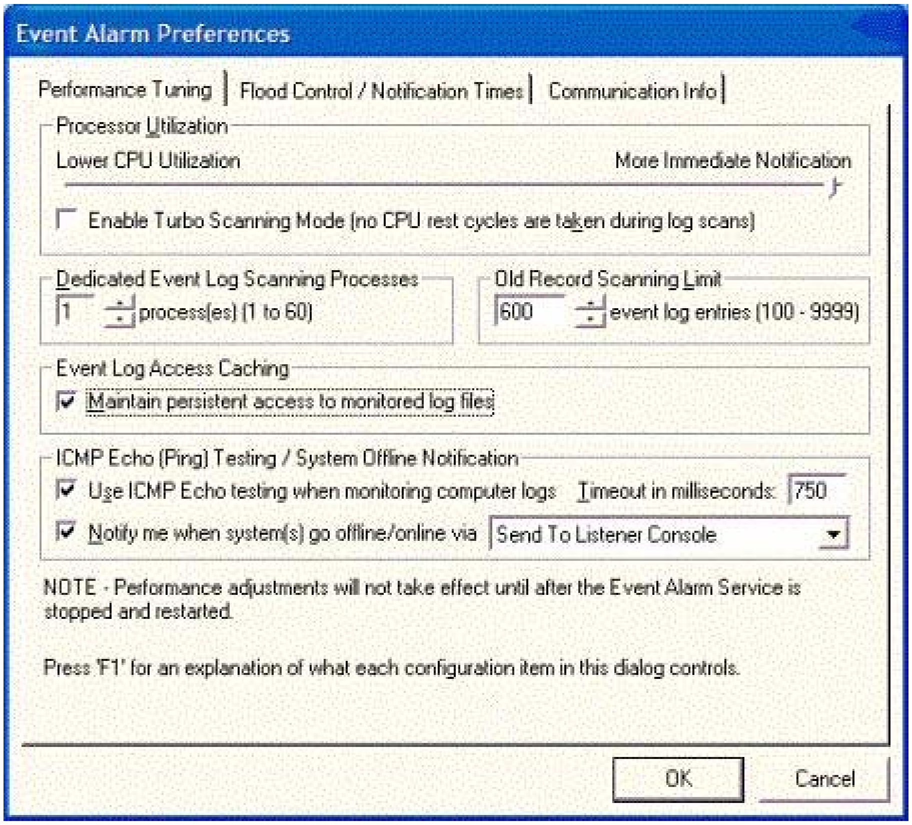
Other Recommendations

Network Performance / Usage

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.



Event Alarm Preferences

Processor Utilization

Lower CPU Utilization — More Immediate Notification

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

Dedicated Event Log Scanning Processes

1 process(es) (1 to 60)

Old Record Scanning Limit

600 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: 750

☑ Notify me when system(s) go offline/online via Send To Listener Console

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.

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 x .5 seconds = 10 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.

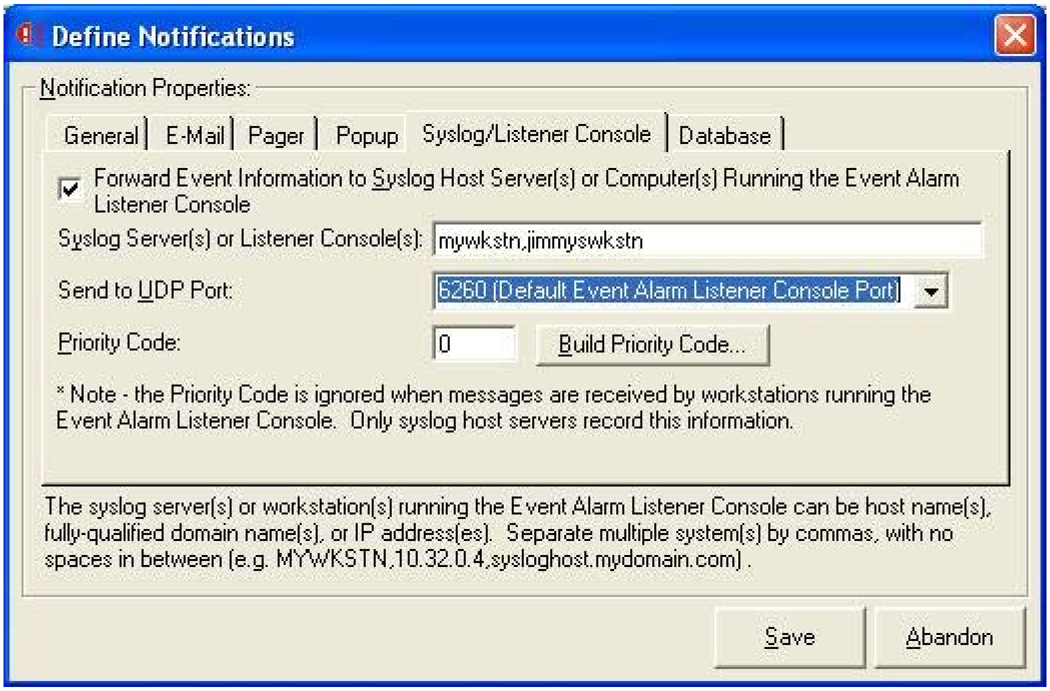
The most robust notification method is email. WhatsUp Event Alarm has been specially designed to be capable of generating hundreds of email messages per second using a multithreaded architecture. Email can be queued by SMTP servers pending delivery, and it is sent over a connection-oriented protocol (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.



☑ Forward Event Information to Syslog Host Server(s) or Computer(s) Running the Event Alarm Listener Console

Syslog Server(s) or Listener Console(s): mywkstn,jimmyswkstn

Send to UDP Port: 6260 (Default Event Alarm Listener Console Port)

Priority Code: 0

* Note - the Priority Code is ignored when messages are received by workstations running the Event Alarm Listener Console. Only syslog host servers record this information.

The syslog server(s) or workstation(s) running the Event Alarm Listener Console can be host name(s), fully-qualified domain name(s), or IP address(es). Separate multiple system(s) by commas, with no spaces in between (e.g. MYWKSTN,10.32.0.4,sysloghost.mydomain.com) .

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).