IPSWITCH

WhatsUp Event Alarm v10.x Listener Console User Guide

WhatsUp Event Alarm Listener Console Overview

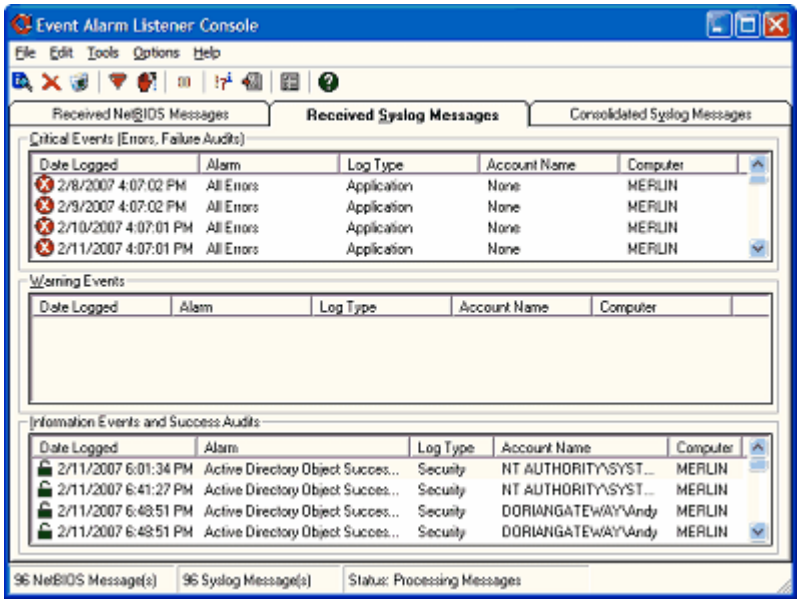
WhatsUp Event Alarm Listener Console Overview

In This Guide

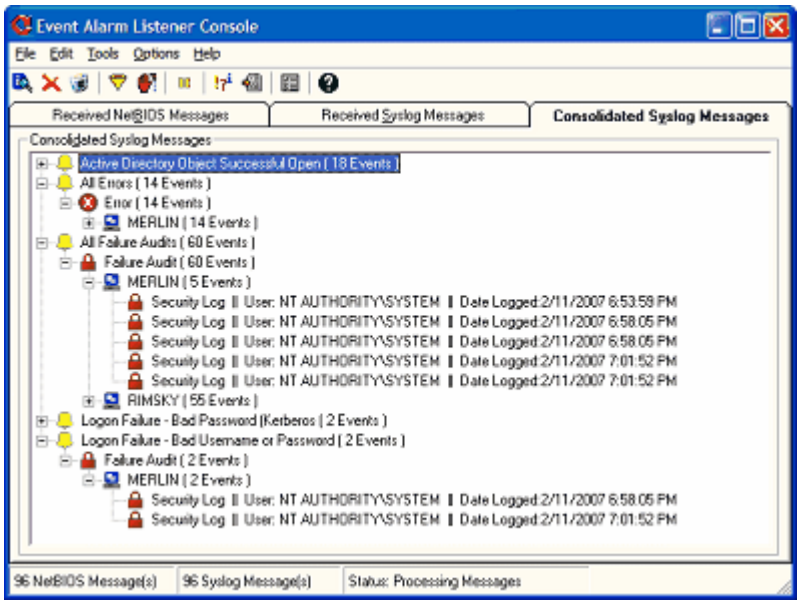
The WhatsUp Event Alarm Listener Console is a small, low-resource program that allows network administrators and other key parties to be notified when the WhatsUp Event Alarm software detects key events on computers throughout their network. When minimized, it sits in the notification area of the taskbar, and flashes and optionally sounds an alert when new notification messages arrive.

Every time the WhatsUp Event Alarm Service detects that a newly generated event log record matches criteria it is looking for, it can send out notification(s) to specific persons via traditional methods such as e-mail messages, pager calls, and network popups. However, if certain events are detected frequently, and generate a large volume of notifications, it may not make sense to use the previously mentioned methods for notification. The WhatsUp Event Alarm Listener Console is ideal for handling larger volumes of events, as it allows you to further filter, consolidated, categorize, and suppress the events that are received.

There are two types of messages the WhatsUp Event Alarm Listener Console can receive from the primary WhatsUp Event Alarm software: targeted UDP datagrams formatted as syslog messages and NetBIOS broadcasts. Both these methods are described in detail below.



WhatsUp Event Alarm Listener Console Displaying Syslog Messages - Non-Consolidated View



WhatsUp Event Alarm Listener Console Displaying Syslog Messages - Consolidated View

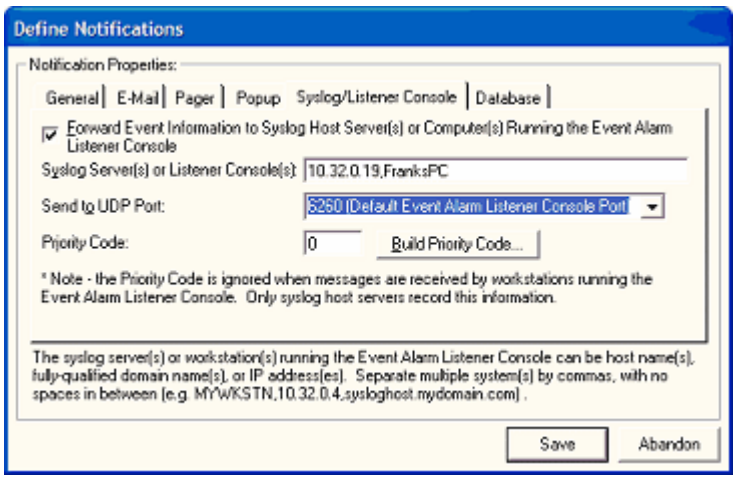
Syslog Messages. The WhatsUp Event Alarm Listener Console can receive UDP datagrams formatted as syslog messages sent from various WhatsUp Event Alarm installations throughout an enterprise network. The main WhatsUp Event Alarm program can be configured to send these messages to specific IP addresses, specific workstation names, or to a limited broadcast IP address.

The advantages of using syslog messages to transmit detected events to the Listener Console are as follows:

1. These messages can cross domain boundaries (whether or not trust relationships are in place)
2. They can be transmitted over any port
3. They can be targeted to individual machines as opposed to being broadcast to all machines
4. They can be saved to disk in between WhatsUp Event Alarm Listener Console sessions. In other words, they are saved to disk when the program is closed, and reloaded from disk when the program is restarted

For the above reasons, syslog messages are the preferred way to transmit detected events from the WhatsUp Event Alarm Service to clients running the WhatsUp Event Alarm Listener Console.

Received syslog messages are displayed in two different tabs in the WhatsUp Event Alarm Listener console, the Received Syslog Messages tab and the Consolidated Syslog Messages tab. The Received Syslog Messages tab groups syslog messages into one of three lists depending on the type of Windows event contained in the message (e.g. Errors/Failure Audits, Warnings, and Information/Success Audits). The Consolidated Syslog Messages tab groups related syslog messages together by the name of the alarm that was triggered, the computer name where the alarm occurred, and the type of Windows event that was detected.



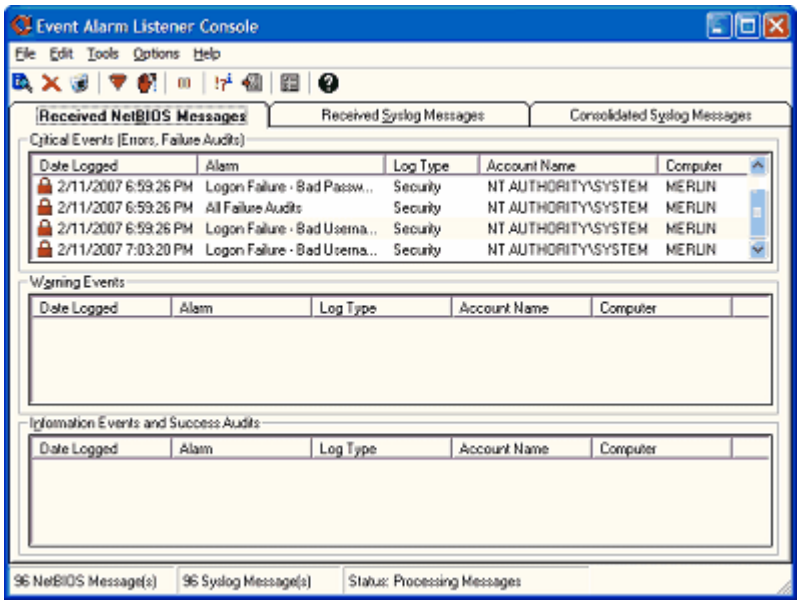
Configuring WhatsUp Event Alarm to send syslog messages to machines running the WhatsUp Event Alarm Listener Console.

Inside the WhatsUp Event Alarm Control Panel, click the **Edit** menu, and then select **Define Notifications**.

To transmit syslog message notifications to specific client machines running the WhatsUp Event Alarm Listener Console, administrators must:

1. Determine the specific IP addresses or names of computers running the WhatsUp Event Alarm Listener Console, or alternately settle on a local limited broadcast address (e.g. 192.168.1.255) to reach all clients running the Listener Console in a given subnet
2. Create notifications with the WhatsUp Event Alarm Control Panel designed to forward alarms to WhatsUp Event Alarm Listener Consoles on a given port. This is done from the **Edit** menu > **Define Notifications** area in the WhatsUp Event Alarm Control Panel. The default port used by the Listener Console is 6260 as it is not often used by other protocols, but this port number is customizable both within the WhatsUp Event Alarm Control Panel and the WhatsUp Event Alarm Listener Console
3. Associate these notifications with certain specific alarms, or with certain computer event logs, so they will fire when alarms are detected on computers and logs monitored by the WhatsUp Event Alarm Service
4. Open all relevant host-based or network-based firewalls so that UDP traffic over port 6260 (or whatever custom port is used) can flow between the system(s) running WhatsUp Event Alarm and the workstations running the WhatsUp Event Alarm Listener Console

After these steps have been taken, whenever the WhatsUp Event Alarm Service detects that an alarm has been triggered, it will send a syslog message to any workstations specified by the notification defined in WhatsUp Event Alarm. Unlike the NetBIOS broadcast messages described below, WhatsUp Event Alarm will not send out syslog messages every time any alarm is triggered. Instead, it will only send these messages out to select clients (or an IP broadcast address) when events are detected on monitored computers.



WhatsUp Event Alarm Listener Console Displaying NetBIOS messages

NetBIOS Broadcast Messages. If these messages are enabled in the Preferences dialog of the WhatsUp Event Alarm Control Panel, WhatsUp Event Alarm sends out a broadcast message every time any alarm is triggered. These broadcast messages are sent to all Windows NT/2000/XP/2003 clients

1. That are member(s) of the same domain where WhatsUp Event Alarm is installed
2. That are listening for these messages by running the WhatsUp Event Alarm Listener Console program

Workstations not running the WhatsUp Event Alarm Listener Console ignore and discard these messages. The WhatsUp Event Alarm Service does not distinguish between different types of alarms when constructing these types of messages. All detected alarms detected generate a NetBIOS broadcast message.

The limitations of NetBIOS broadcasts are:

1. They are sent to all computers in a domain indiscriminately
2. They cannot cross domain boundaries
3. They require NetBIOS to be enabled over TCP/IP on computers running WhatsUp Event Alarm and the WhatsUp Event Alarm Listener Console
4. The WhatsUp Event Alarm Listener Console does not save NetBIOS messages to disk when it is unloaded, unlike syslog messages

For this reason, they are only recommended for use in small networks with a single domain model.

In order for the WhatsUp Event Alarm Listener Console to receive NetBIOS messages, the following actions must be taken:

1. NetBIOS must be enabled in your domain on top of your default data transmission protocol (e.g. TCP/IP)
2. Broadcast NetBIOS messages must be turned on in the Preferences area of the WhatsUp Event Alarm Control Panel
3. The Received NetBIOS Messages tab must be enabled in the Preferences menu of the WhatsUp Event Alarm Listener Console
4. Workstations running the Listener Console must have NetBIOS over TCP/IP enabled
5. If routers or switches block NetBIOS traffic between the Listener Console and the machine running the WhatsUp Event Alarm Service, messages may not be delivered. NetBIOS traffic must be allowed to pass through all network segments where computers are running the WhatsUp Event Alarm Listener Console

Firewall Considerations

If you are running the WhatsUp Event Alarm Listener Console on an operating system with a built-in host-based firewall (such as Windows XP, Windows Vista, or Windows Server 2008), create an exception to allow UDP syslog packets to pass through the firewall to the WhatsUp Event Alarm Listener Console program. This is also required if you are running a third-party host-based firewall.

The exception should be specified as follows:

Protocol Type. UDP or Both (e.g. TCP and UDP)

Port Number. By default, port 6260, but if you change the default port number in WhatsUp Event Alarm, type the new port number here.

Direction (if applicable). Inbound or both (e.g. inbound/outbound).

Using the WhatsUp Event Alarm Listener Console

When minimized, the console runs in the notification area located in the lower right corner of the taskbar. You can double-click this icon to maximize the console and view any newly delivered notification messages. Right-clicking the icon displays a context menu capable of showing the console, launching help, or disabling/enabling sound. When minimized in the notification area, the console icon flashes and a sound plays (if desired) when new messages are received.

When maximized, the console displays up to three separate tabs containing received NetBIOS and syslog messages, further separated by type of event. By double-clicking a message, you can view the full details of the event log entry that caused an alarm. Messages can be purged one of several ways: by clicking the delete (X) toolbar button to remove selected messages (File > Delete Messages), by clicking the delete (X) button when viewing message details, by pressing the Del key on the keyboard, or by clicking the trash can button to clear all messages in the console (File Menu > Clear All Messages). The remaining actions that can be performed are listed below.

WhatsUp Event Alarm Listener Console Menu Actions

File Menu Commands

View Message Details. Displays all of the data in the selected message. You can also double-click a selected message in the listing or consolidated view to see details.

Delete Selected Message(s). Deletes all selected message(s) from the console. If the Listener Console is displaying the Consolidated Syslog Messages tab, selecting a higher level tree item and then choosing this menu item deletes all child messages below the selected tree item.

Clear All Messages. Permanently deletes all messages of a particular type (e.g. NetBIOS messages or syslog messages). If the Received NetBIOS Messages tab is selected, all NetBIOS messages are erased. If the Received Syslog Messages or Consolidated Syslog Messages tab is selected, all syslog messages are erased.

Exit. Ends the WhatsUp Event Alarm Listener Console program. Any syslog messages still displayed in the program will be saved to disk and reloaded the next time the WhatsUp Event Alarm Listener Console is started.

Edit Menu Commands

Apply a Filter/Remove Filter. Opens a dialog allowing you to filter for certain types of events among your received messages. After applying a filter, you can remove it by selecting this menu option again. When messages are filtered, only those messages matching the filter are visible. Incoming messages are only displayed if they match the filter, and non-matching messages are displayed after the filter is removed. You can either filter NetBIOS messages or syslog messages at any given time. You cannot filter both kinds of messages at the same time.

Manage Suppression Filters. Opens a dialog allowing you to define one or more suppression filters. Suppression filters prevent incoming messages from being displayed in the WhatsUp Event Alarm Listener Console. It provides the ability to not display events on a customizable, per-user basis. After you have defined one or more suppression filters, the WhatsUp Event Alarm Listener Console compares each received message to all suppression filters, and if the incoming message matches one or more of the filters, it is dropped and never displays in the console.

Pause Message Processing/Resume Message Processing. Periodically, a user may need to prevent incoming messages from being displayed in the console. For example, a user may need to select several different messages from a list and then delete them. If message processing is paused, incoming messages are held in memory, but are not displayed until message processing is resumed. By default, message processing resumes automatically, two minutes after it is paused.

Tools Menu Commands

Event Log Viewer. Launches the Microsoft Event Viewer allowing you to review recent events from a computer's log. If you are running Microsoft Windows XP, the default focus is shifted to the computer featured in the selected message.

Export to Text. Exports all messages displayed in the active tab to a comma-delimited text file of your choosing. You can then import this file into Microsoft Excel or a database for further analysis.

Options Menu Commands

Listener Console Preferences. Opens a dialog allowing you to adjust global properties, such as the types of messages displayed (e.g. NetBIOS messages and syslog messages), the port on which the WhatsUp Event Alarm Listener Console receives incoming syslog messages, and whether audible alerts are heard when notifications arrive.

Help Menu

WhatsUp Event Alarm Listener Console Help File. Displays the help file.

About WhatsUp Event Alarm. Displays the splash screen and version number of the Listener Console.

Event Alarm Listener Console Preferences Dialog

Use the WhatsUp Event Alarm Listener Console Preferences dialog to configure global settings in the program, such as the UDP port the console listens on for incoming syslog messages and the types of messages it displays.

The **Message views** area controls what type of messages (NetBIOS or syslog) display in the console in a separate tab. By default, only Received Syslog Messages and Consolidated Syslog Messages are shown. If you decide to use NetBIOS messages instead, check the Received NetBIOS Messages tab, and uncheck the other tabs.

To set Event Alarm Listener Console Preferences:

1. From the **Options** menu, select **Listener Console Preferences**. The WhatsUp Event Alarm Console Preferences dialog opens.
2. Set preferences using the open dialog.
3. Click **OK** when you are satisfied with your preferences. Your preferences are saved.

To change the **UDP port** number that the WhatsUp Event Alarm Listener Console receives syslog messages on, you can do so here. If you change the port number in the Listener Console, you must update your Listener Console notification port number in the main WhatsUp Event Alarm Control Panel. This is done from the **Edit** menu > **Define Notifications** menu option.

If **Audible alerts** are on, the WhatsUp Event Alarm Listener Console plays a sound every time a new message is received. This feature is disabled by default. If you want to change the sound the Listener Console plays, you can do so by taking your own WAV file and placing it in the WhatsUp Event Alarm Listener Console installation directory with a filename of sound.wav.

Display Dates allow you to customize how dates are displayed and formatted when they arrive in the Listener Console.

Message Details Dialog

View message details using the Message Details dialog. To open the Message Details dialog, double-click a received message in the WhatsUp Event Alarm Listener Console, or when you highlight a message, and click the **View Message Details** option from the **File** menu.

You can perform several actions when viewing a message.

 **View Previous Message**. When you press this button, the Message Details dialog skips one message back in the currently selected list of messages, or in the current tree branch of messages you are viewing. This can be useful to quickly scan backwards while reviewing received messages. Ctrl+Up Arrow is the keyboard shortcut for this action.

 **View Next Message**. When you press this button, the Message Details dialog skips one message forward in the currently selected list of messages, or in the current tree branch of

messages you are viewing. Pressing this button repeatedly lets you scan forward when reviewing messages. Ctrl+Down Arrow is the keyboard shortcut for this action.

 **Copy To Clipboard**. Pressing this button copies all of the message details displayed in the dialog to the clipboard, so you can paste them into another application like an email client. Ctrl+C is the keyboard shortcut for this action.

 **Suppress Event**. Clicking this button opens the Manage Suppression Filters Dialog, and automatically transfers the Source, Event ID, and Type of Event featured in the current message to that dialog. This allows you to quickly create a Suppression Filter so that this type of message will not be displayed in the future in the WhatsUp Event Alarm Listener Console. Ctrl+S is the keyboard shortcut for this action.

 **Delete Message**. Press this button to delete the message you are viewing. If possible, focus is shifted to the next message in the list after the current message is deleted. Ctrl+Del is the keyboard shortcut for this action.

Apply Filter Dialog

Occasionally, you may find it necessary to focus on a subset of received messages that share a common set of properties.

The Apply Filter dialog allows you to select one or more criteria to filter on, and once applied, only messages matching that filter are shown in the WhatsUp Event Alarm Listener Console.

 **Note**: You can only filter messages of a specific type at any given time. For example, you can filter your NetBIOS messages, or your syslog messages, but not both at the same time.

To apply a filter to received messages:

1. From the WhatsUp Event Alarm Listener Console, click the **Edit** menu, and then select **Apply a Filter to Received Messages**. The Apply Filter dialog opens.
2. Place a check by one or more properties to filter.
3. Select specific values in the list to filter. The list is automatically generated from all values found for that property among all received messages.
4. Click the **Apply** button. After a filter is applied, only messages matching your filter display in the tabs corresponding to the message types being filtered (e.g. NetBIOS or syslog).

To remove a filter, click the **Edit** menu, and then select **Remove Filter**.

Manage Suppression Filters Dialog

Because the WhatsUp Event Alarm Listener Console can run on multiple user workstations, some users may receive alarms that they deem unimportant. An easy, per-user way to suppress certain alarms is through the creation of suppression filters.

To create, edit, or remove suppression filters, click the **Edit** menu, and then select **Manage Suppression Filters** To create a new suppression filter, click the **Add** button. To edit an existing suppression filter, click the **Edit** button. To delete an existing suppression filter, click the **Delete** button.

To create or edit a suppression filter, type in a name for the filter, and then enter in values for the fields you want the WhatsUp Event Alarm Listener Console to examine when new events arrive. Only type values in fields that you wish to filter by; leave all other fields blank**.** A general rule of thumb is to type the source of the event, followed by the EventID number, and then the Types of events applicable.

After defining a suppression filter, click **OK** to create it or update it in the WhatsUp Event Alarm Listener Console. Click **Cancel** to abandon the creation of a new suppression filter, or to abandon the changing of an existing filter.

When suppression filters are defined, the WhatsUp Event Alarm Listener Console compares every incoming event to see if the fields in the event match all the targeted fields in one or more suppression filters. If so, the WhatsUp Event Alarm Listener Console discards the event rather than displaying it in the appropriate tab.