



# LogLady v1.8

# 1 Contents

1	Contents.....	2
2	Shareware.....	3
3	Introduction.....	4
3.1	What is LogLady?.....	4
3.2	What is syslog?.....	4
4	Installation.....	5
4.1	Description.....	5
4.2	Install command line options.....	9
5	Overview.....	11
6	User interface.....	12
6.1	Main Window.....	12
6.1.1	Filter Pane.....	12
6.1.2	Message Pane.....	12
6.1.3	Graph Pane.....	13
6.1.4	System Tray Icon.....	13
6.2	Menus.....	13
6.2.1	File Menu.....	13
6.2.2	Edit Menu.....	15
6.2.3	View Menu.....	17
6.2.4	Rules Menu.....	20
6.2.5	Monitors Menu.....	21
6.2.6	Help Menu.....	22
7	Monitors.....	23
8	Rules.....	26
9	Actions.....	28
9.1	Decription.....	28
9.2	Advanced settings.....	29
9.2.1	SNMP Trap.....	29
9.2.2	E-Mail.....	29
9.3	Special string options.....	30
9.3.1	Examples.....	30
9.4	Special Filename Characters.....	30
9.4.1	Examples.....	31
10	Using LogLady, Examples.....	32
10.1	Play a sound when a message of interest arrives.....	32
10.2	Forward All Windows Event Log Messages to a Linux Syslog Server.....	33
10.3	Put some Linux Syslog messages in the Windows Event Log.....	34
10.4	Show me when my firewall traps access a banned website.....	35
10.5	Send me an e-mail when a linux system is rebooted.....	35
10.6	Save a restricted set of messages in their own log file.....	36
10.7	Include the Windows XP SP2 firewall logging in LogLady.....	36
10.8	Discard messages.....	37
10.9	Save all Warning or higher messages to a database.....	38
11	Regular Expressions.....	39
11.1	Description.....	39
11.2	Examples.....	40
12	Syslog Message Fields.....	41
13	Troubleshooting.....	46
13.1	Frequently asked questions.....	46
13.2	LogLady and Windows XP SP2 firewall.....	46
14	Registering and Paying for LogLady.....	49

## 2 Shareware

### Copyright Notice

2004-2015 HC Mingham-Smith Ltd. ("The author")

THE SOFTWARE IS PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EXPRESS, IMPLIED OR OTHERWISE, INCLUDING WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER OR NOT ADVISED OF THE POSSIBILITY OF DAMAGE, AND ON ANY THEORY OF LIABILITY, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

LogLady is Shareware. This is a complete working version. There are no annoying reminder screens about what it costs, and there are no disabled features. If you continue to use it after evaluating it please send the appropriate amount by post to:

HC Mingham-Smith Ltd.  
33 Arthur Rd.  
Wokingham,  
Berkshire RG41 2SS  
England.

A cheque made payable to HC Mingham-Smith Ltd. would be acceptable, or see our website for credit card payments.

**Pricing details are at the back of this manual.**

## 3 Introduction

### 3.1 What is LogLady?

As the number of networked devices increases monitoring them becomes a problem. LogLady is designed to solve the problem of collecting and analysing log messages from many sources.

LogLady provides a way to filter, analyze, and act on log messages. You may want to be e-mailed when a router identifies an issue. Some messages could trigger the execution of a program to deal with the situation. LogLady can do all this and more using *rules* and *actions*. *Rules* allow important messages to be recognised. *Actions* provide a way to react to messages selected by the *rules*.

LogLady is a *syslog* server with extra features to integrate information from non-*syslog* sources.

LogLady provides *monitors* to generate standard *syslog* log messages from system events where none are generated by default or they are generated in an inconvenient form.

In recent versions of Windows there is a 'Windows Event Log' that can be used to collect Windows based messages. LogLady provides a better way to view these messages than the default Event Log Viewer plus it supports logging from other non-windows devices using the *syslog* protocol.

LogLady allows you to collect all the *syslog* traffic on your network in a single place *and* merge them into the Windows Event Log.

### 3.2 What is syslog?

The *Syslog* protocol has been used for many years to transmit logging messages across TCP/IP networks. It was originally part of the University of California Berkeley Software Distribution but now forms part of every distribution of UNIX and Linux. It has proved its worth in operations and management of network based devices.

Typically there is a central *Syslog* server that receives the messages and many client devices that send them. Many network-based devices generate *syslog* output; these include printers, routers, etc.

For more information on *Syslog* refer to RFC 3164 (available on the internet) or the selected extract on page 41.

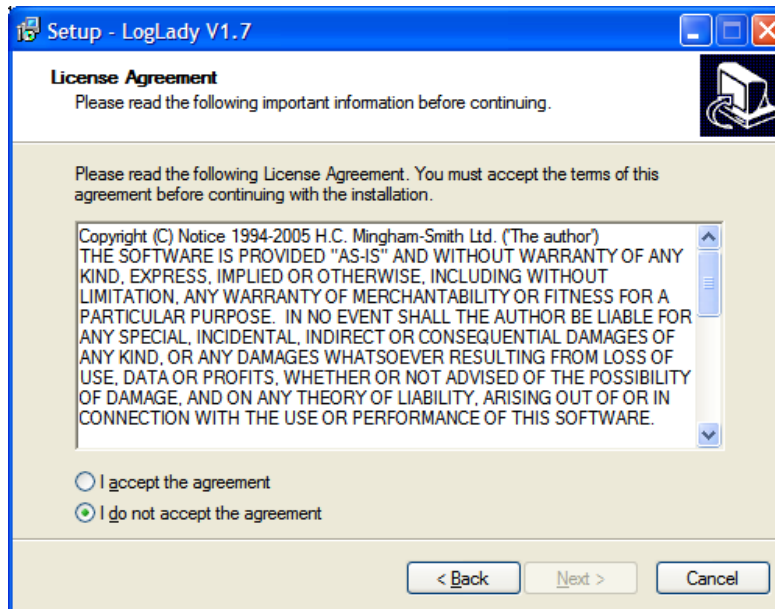
## 4 Installation

### 4.1 Description

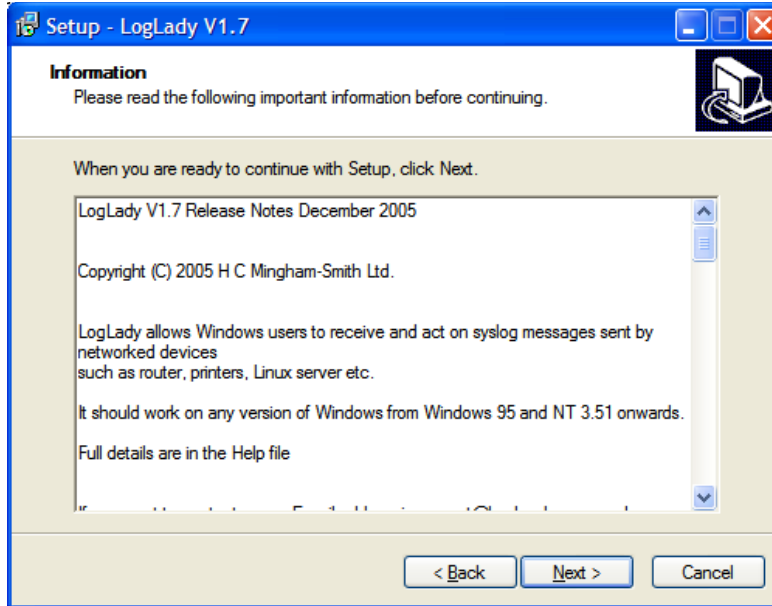
Run the LogLadyVxx.exe setup program.



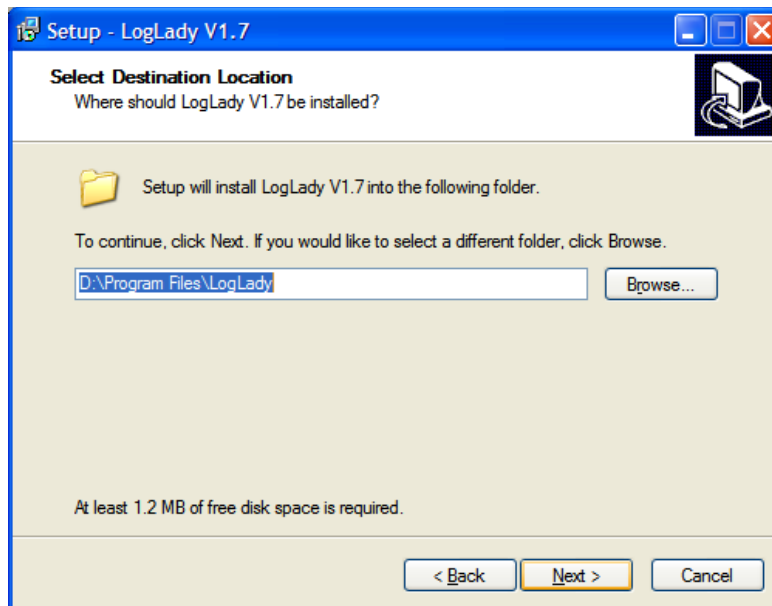
Press Next



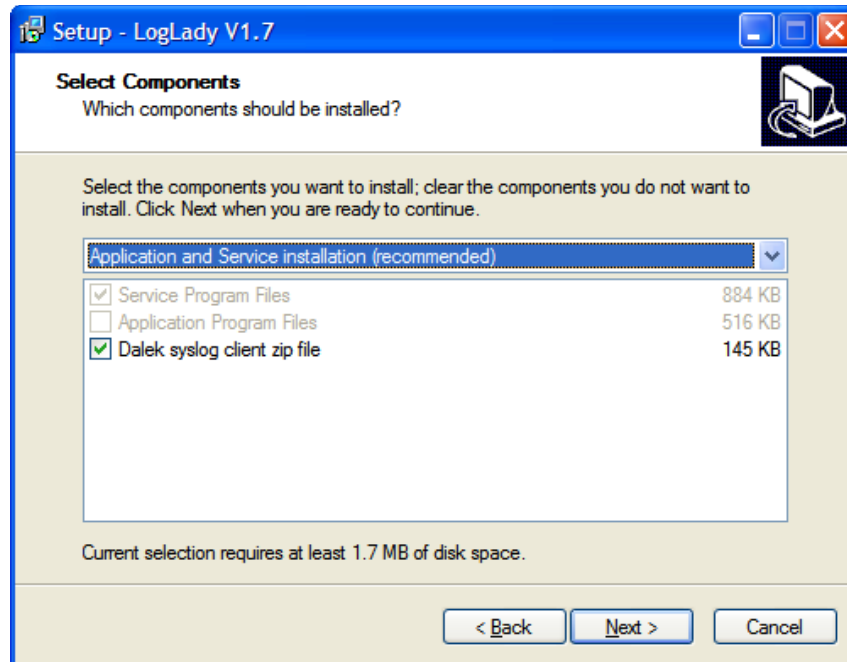
You must accept the agreement and press Next to proceed.



Press Next



Either accept the default folder or choose a new folder, press next.



LogLady is supported on all versions of Windows from Windows 95 onwards. On Windows 95/98/ME LogLady is a standalone application. The application must be running to collect and process messages.

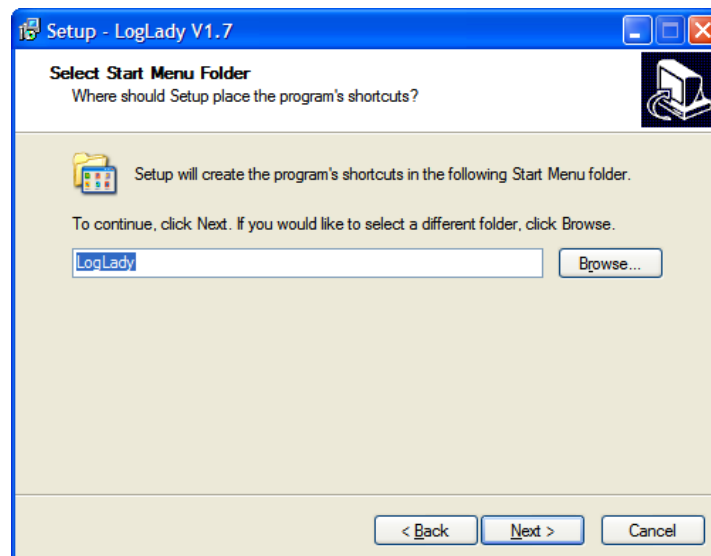
On versions of Windows based on Windows NT technology (NT4, 2000, XP, 2003 etc.) LogLady is split into 2 parts, the application User Interface (UI) and a background Service.

When the User Interface is not running the background service continues to collect and process messages.

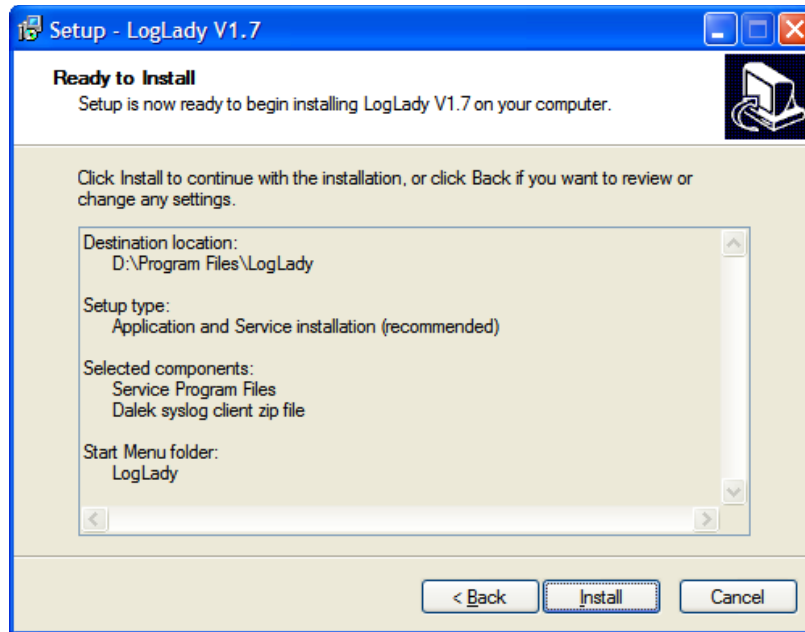
You may still choose the standalone application version if you use a version of Windows based on Windows NT technology. We recommend that you use the service version. Older versions of Windows must use the standalone application.

The dalek syslog client is another of our products that allows *syslog* messages to be sent to LogLady.

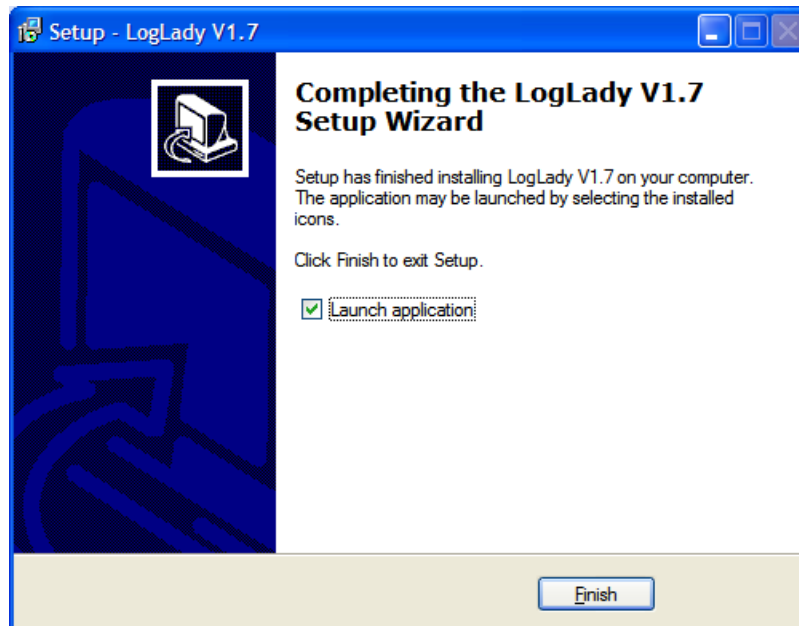
Press Next when you have made your selections. The defaults should match most users' requirements.



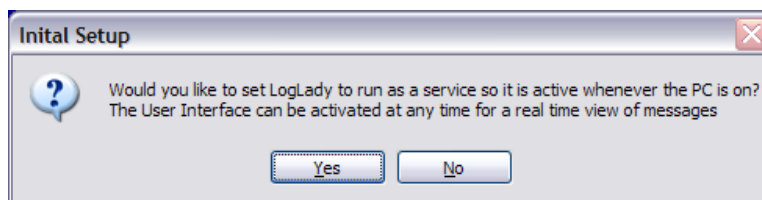
Select the name of the start menu folder, press next.



Press 'Install' to complete the installation



Press 'finish'



This is shown the first time LogLady runs, we recommend that you select 'yes'. LogLady should now start.



## 4.2 Install command line options

LogLady uses the wonderful Inno Setup (<http://www.jrsoftware.org/isinfo.php>). As a result the setup program has the following install options provided by Inno setup.

The Setup program accepts optional command line parameters. These can be useful to system administrators, and to other programs calling the Setup program.

<b>/SP-</b>	Disables the <i>This will install... Do you wish to continue?</i> prompt at the beginning of Setup.
<b>/SILENT, /VERYSILENT</b>	<p>Instructs Setup to be silent or very silent. When Setup is silent the wizard and the background window are not displayed but the installation progress window is. When a setup is very silent this installation progress window is not displayed. Everything else is normal so for example error messages during installation are displayed and the startup prompt is (if you haven't disabled it the '/SP-' command line option explained above)</p> <p>If a restart is necessary and the '/NORESTART' command isn't used (see below) and Setup is silent, it will display a <i>Reboot now?</i> message box. If it's very silent it will reboot without asking.</p>
<b>/LOG</b>	<p>Causes Setup to create a log file in the user's TEMP directory detailing file installation actions taken during the installation process. This can be a helpful debugging aid. For example, if you suspect a file isn't being replaced when you believe it should be (or vice versa), the log file will tell you if the file was really skipped, and why.</p> <p>The log file is created with a unique name based on the current date. (It will not overwrite or append to existing files.) Currently, it is not possible to customize the filename.</p> <p>The information contained in the log file is technical in nature and therefore not intended to be understandable by end users. Nor is it designed to be machine-parseable; the format of the file is subject to change without notice.</p>
<b>/NOCANCEL</b>	Prevents the user from cancelling during the installation process, by disabling the Cancel button and ignoring clicks on the close button. Useful along with '/SILENT' or '/VERYSILENT'.
<b>/NORESTART</b>	Instructs Setup not to reboot even if it's necessary.
<b>/RESTARTEXITCODE=exit code</b>	Specifies the custom exit code that Setup is to return when a restart is needed. Useful along with '/NORESTART'. Also see Setup Exit Codes.
<b>/LOADINF="filename"</b>	<p>Instructs Setup to load the settings from the specified file after having checked the command line. This file can be prepared using the '/SAVEINF=' command as explained below.</p> <p>Don't forget to use quotes if the filename contains spaces.</p>
<b>/SAVEINF="filename"</b>	Instructs Setup to save installation settings to the specified file. Don't forget to use quotes if the filename contains spaces.
<b>/DIR="x:\dirname"</b>	Overrides the default directory name displayed on the Select Destination Location wizard page. A fully qualified pathname must be specified.

<b>/GROUP="folder name"</b>	Overrides the default folder name displayed on the Select Start Menu Folder wizard page.
<b>/NOICONS</b>	Instructs Setup to initially check the Don't create any icons check box on the Select Start Menu Folder wizard page.
<b>/COMPONENTS="comma separated list of component names"</b>	Overrides the default components settings. Using this command line parameter causes Setup to automatically select a custom type.

## 5 Overview

LogLady provides many features to process and analyze log messages.

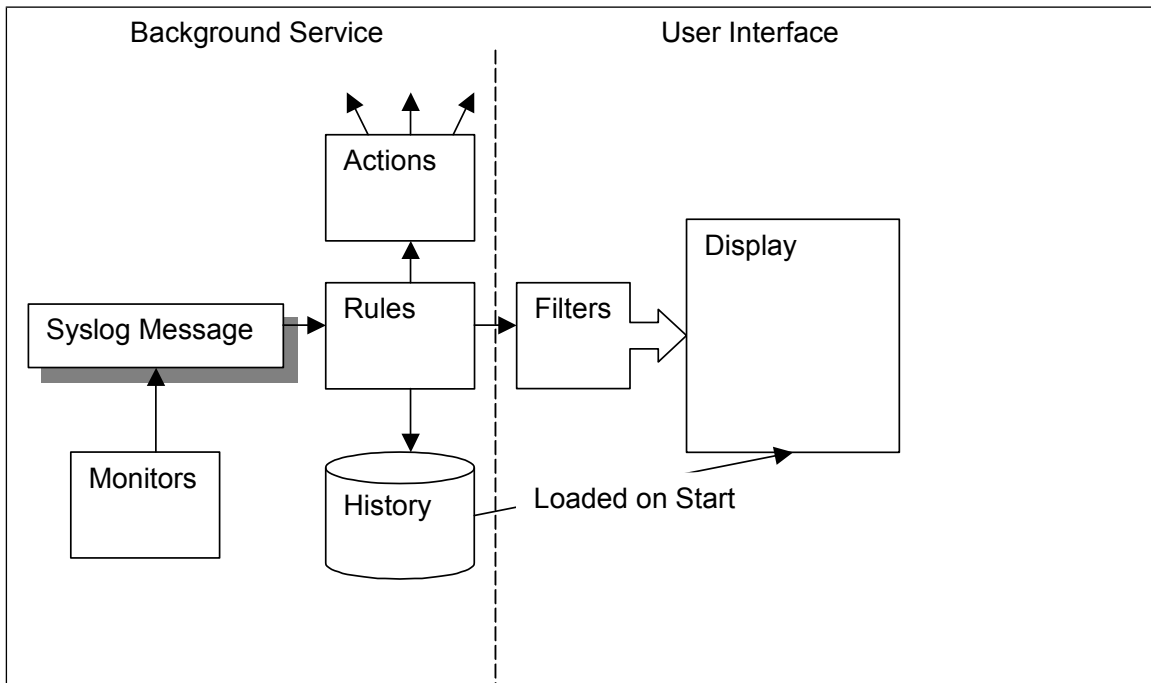
*Monitors* are provided to extract log information from non-*syslog* based sources.

*Rules* can be used to detect messages of interest.

*Actions* allow LogLady to do useful things when interesting messages are detected.

*History* keeps a list of recently received messages.

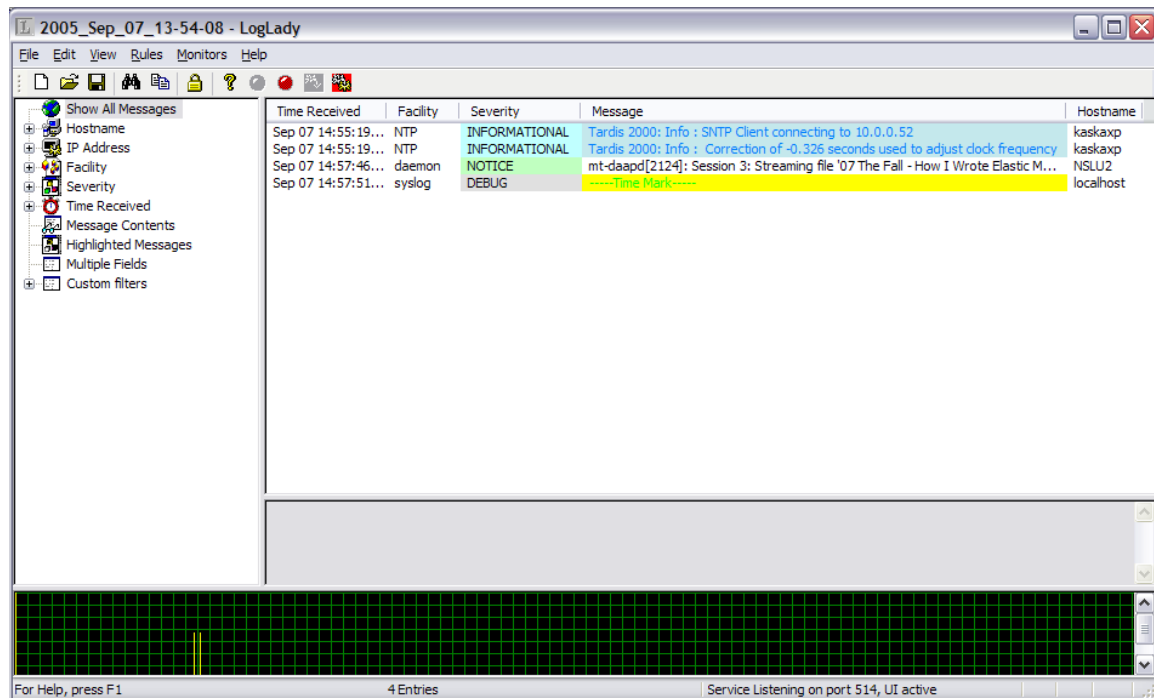
*Filters* provide a way to selectively display only those messages that are of interest.



## 6 User interface

### 6.1 Main Window

The main window is split into 3 panes.



#### 6.1.1 Filter Pane

On the left is the filter pane. This controls which messages are shown. For example, if the severity 'error' is selected, only messages with severity 'error' are shown. This affects current messages and any new messages that arrive.

IP addresses, hostnames, and facilities are added to the tree as they are received.

Double click on the message contents entry to search for matching text.

Double click on the 'multiple fields' entry to search for messages based on several fields at once.

The 'time received' entries are relative to the currently selected message in the message pane. If none is selected, the entries are relative to 'now'.

More complex filters can be created and saved for future use with the Edit Custom Filters dialog.

The status bar at the bottom of the window shows if a filter is active, whether the display is locked, and how many messages are shown.

#### 6.1.2 Message Pane

On the right is the message pane. This shows the messages received by LogLady.

If you right-click on a message you can select whether to start a web browser or telnet session with the client that originated the message. You can also toggle whether a message is highlighted or start the Find dialog. 'Send to Rules' sends the selected messages to the Rules; this can be useful when developing new rules.

Double-clicking on an entry can start a browser, telnet, or the Find dialog. This is configurable in the Preferences dialog.

Messages can be sorted by clicking on the column headers.

The display may be 'locked' using the lock symbol on the Toolbar to prevent new messages being displayed. Messages are still received and stored. They are displayed when the display is unlocked.

The full text of the currently selected message is shown at the bottom of the Message Pane; useful for long messages. IP addresses can be expanded to names in the full text to aid analysis. E.g. 207.46.198.30 would be replaced with [www.microsoft.com](http://www.microsoft.com). This option is off by default but may be switched on in the preferences dialog.

### 6.1.3 Graph Pane

The graph pane shows a map of all the messages currently displayed and their relative time of arrival. A large peak indicates that a lot of messages arrived within a short time. A red line is shown to indicate the message currently selected in the message pane. You can click on the graph to go directly to the messages for a given peak.

### 6.1.4 System Tray Icon

LogLady places an Icon on the system tray that allows the main window to be hidden/shown. Click on it to toggle between hidden/shown.

## 6.2 Menus

### 6.2.1 File Menu

The File menu offers the following commands:

<b>New</b>	Creates a new log
<b>Open</b>	Opens an existing log
<b>Save</b>	Saves an active log using the current file name
<b>Save As</b>	Saves an opened log to a specified file name
<b>Import...</b>	Import records in raw RFC 3164 format
<b>Export...</b>	Export records to raw RFC 3164 format
<b>Load History</b>	Load the saved history
<b>Clear History</b>	Clear the history
<b>Import Settings...</b>	Load rules, filters, and highlighting
<b>Export Settings...</b>	Save rules, filters, and highlighting
<b>Exit</b>	Exits LogLady

#### 6.2.1.1 New command (File menu)

Use this command to create a new log. The active log may be saved if it has been changed.

#### 6.2.1.2 Open command (File menu)

Use this command to open a saved log. The active log may be saved if it has been changed.

### **6.2.1.3 Save command (File menu)**

Use this command to save the active log to its current name and directory. If you want to change the name and directory of an existing document before you save it, choose the Save As command.

### **6.2.1.4 Save As command (File menu)**

Use this command to save and rename the active log. LogLady displays the Save As dialog box so you can name your log.

To save a document with its existing name and directory, use the Save command.

### **6.2.1.5 Import command (File menu)**

Use this command to import one or more logs in RFC3164 format. LogLady displays a dialog box so you can select the files.

### **6.2.1.6 Export command (File menu)**

Use this command to save the active log in RFC 3164 format. LogLady displays a dialog box so you can name your log.

### **6.2.1.7 Load History command (File menu)**

Use this command to load the history enabling LogLady to pick up where it left off. This can be done automatically by setting the 'Load history when program starts' in the Preferences dialog.

### **6.2.1.8 Clear History command (File menu)**

Use this command to clear the history. It has no effect on the messages currently displayed. It clears the saved history that is loaded when the 'Load History' command is used.

### **6.2.1.9 Import Settings... (File menu)**

Use this command to import saved settings, these include the lists of rules, custom filters and highlighting. LogLady displays a dialog box so you can select the files.

### **6.2.1.10 Export Settings... (File menu)**

Use this command to save settings, these include the lists of rules, custom filters and highlighting. LogLady displays a dialog box so you can name your log.

### **6.2.1.11 1, 2, 3, 4 command (File menu)**

Use the numbers and filenames listed at the bottom of the File menu to open the last four logs you closed. Choose the number that corresponds with the log you want to open.

### **6.2.1.12 Exit command (File menu)**

Use this command to end your LogLady session. You can also use the Close command on the application Control menu. LogLady prompts you to save logs with unsaved changes.

## 6.2.2 Edit Menu

The Edit menu offers the following commands:

<b>Copy</b>	Creates a new log.
<b>Select All</b>	Opens an existing log.
<b>Find...</b>	Find log entries
<b>Preferences...</b>	Saves an active log using the current file name.

### 6.2.2.1 Copy command (Edit menu)

Use this command to copy selected data onto the clipboard. Copying data to the clipboard replaces the contents previously stored there.

### 6.2.2.2 Select All command (Edit menu)

Use this command to select all the log entries.

### 6.2.2.3 Find (Edit menu)

Use the find command to find log entries.

The Find dialog box is titled "Find" and contains the following elements:

- Match section:**
  - IP Address: Text input field.
  - Facility: Dropdown menu.
  - Severity: Dropdown menu.
  - Message Contains: Text input field.
  - Match contents using Regexp:
  - Hostname: Text input field.
  - Highlighted:
- Current Message section:**
  - Received: Sep 07 16:20:49 GMT Daylight Time
  - IP Address: 10.0.0.250
  - Hostname: NSLU2
  - Facility: FTP
  - Severity: INFORMATIONAL
- Buttons:** Find Previous, Find Next, Cancel.

The Find dialog allows you to search through the log entries.

The match section of the dialog provides a way of searching the messages. For each field that is specified (as opposed to being left blank) the message must match.

For example if the IP address is specified a message must come from that IP address before it is matched.

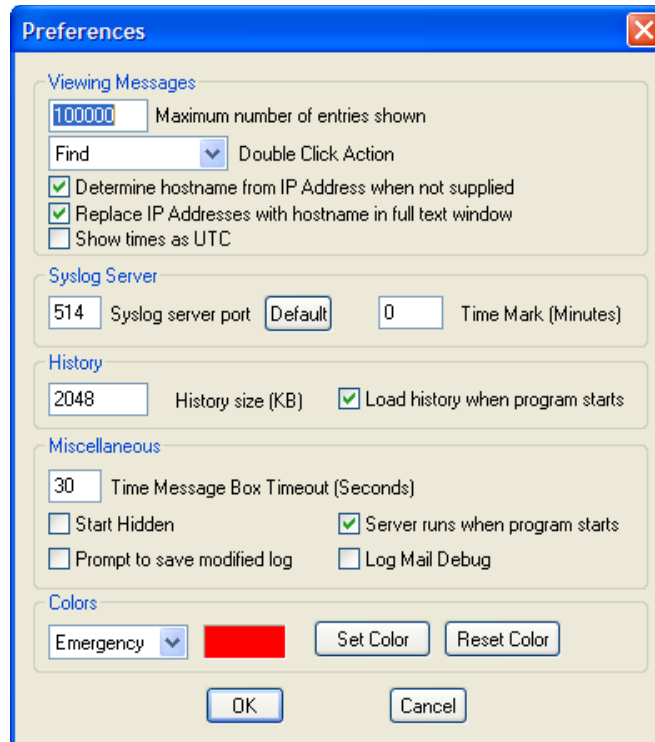
Searching starts from the currently selected message.

If the 'Match contents using Regexp' option is selected the string used to search the message contents is treated as a regular expression.

If this is not set the string is used as a simple case insensitive string that matches if it is contained in the message.

### 6.2.2.4 Preferences... command (Edit menu)

Use this command to edit LogLady's preferences.



The Preferences dialog allows you to change various settings that affect the way LogLady behaves.

<b>Maximum number of entries</b>	This sets the maximum number of messages that LogLady will store before it starts discarding old messages. If you want every message to be saved you can set a Rule to store all messages in a file.
<b>Double click actions</b>	This controls what happens when a message is double-clicked. Either a browser or telnet session is started with the originating device, or the find dialog is shown
<b>Determine hostname from IP Address when not supplied</b>	If a Syslog message doesn't contain the hostname of the sending device, and most don't, LogLady can look it up. This may impact performance a little but LogLady does cache lookups to save time.
<b>Replace IP Addresses with hostname in full text window</b>	IP addresses can be expanded to names in the full text to aid analysis. E.g. 207.46.198.30 would be replaced with <a href="http://www.microsoft.com">www.microsoft.com</a> . This option is off by default. It may cause a delay before the message is displayed as the name is looked up.
<b>Show times as UTC</b>	This controls how times are displayed. The default is to show local



	times. Switch this option on to show as UTC.
<b>Syslog server port</b>	This sets the udp port that LogLady uses to listen for Syslog messages. The default button sets this to the usual value of 514.
<b>Time Mark (Minutes)</b>	Make LogLady insert a Message every x minutes. A value of 0 means no time marks are generated. Inserting time marks are useful in log files to determine that LogLady was active during times when no other messages are received.
<b>History size</b>	Any message that would normally be displayed in LogLady is saved in the history. This sets the maximum size of the history in Kilobytes. If this is set to 0 no history will be saved.
<b>Load History when program starts</b>	Loads messages saved in the LogLady history when the user interface starts.
<b>Message Box Timeout</b>	When a message box is displayed it remains on the screen until the user acknowledges it or the timeout has elapsed.
<b>Start Hidden</b>	LogLady should start on the system tray. Click on the tray icon to see the Main Window.
<b>Server runs when program starts</b>	Sets whether the LogLady user interface (UI) starts listening for messages when it starts. If it is not set LogLady must be told to listen for messages manually by pressing the start button on the Toolbar.
<b>Prompt to save modified log</b>	This controls whether LogLady prompts the user to save a modified log file when it exits.
<b>Log Mail Debug</b>	When a rule is invoked to send an E-Mail message it will log details of the E-Mail session if this option is set. The session is logged to the current log bypassing the Rules.
<b>Set/Reset colors</b>	This allows the colors used to highlight the message severity to be altered.

### 6.2.3 View Menu

The View menu offers the following commands:

<b>Toolbar</b>	Controls whether the Toolbar is shown
<b>Status bar</b>	Controls whether the Status bar is shown
<b>Options...</b>	Set view options
<b>Edit custom filters...</b>	Edit the list of custom filters
<b>Edit Highlighting...</b>	Edit the list of strings that are used to highlight messages

#### 6.2.3.1 Toolbar command (View menu)

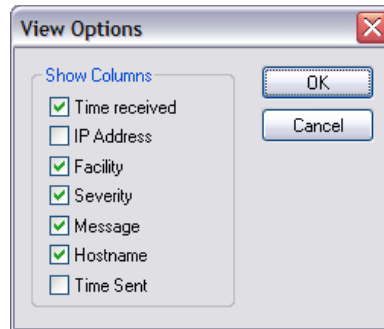
Use this command to display and hide the Toolbar, which includes buttons for some of the most common commands in LogLady, such as New. A check mark appears next to the menu item when the Toolbar is displayed.

### 6.2.3.2 Status Bar command (View menu)

Use this command to display and hide the Status Bar, which describes the action to be executed by the selected menu item or depressed toolbar button, status, and keyboard latch state. A check mark appears next to the menu item when the Status Bar is displayed

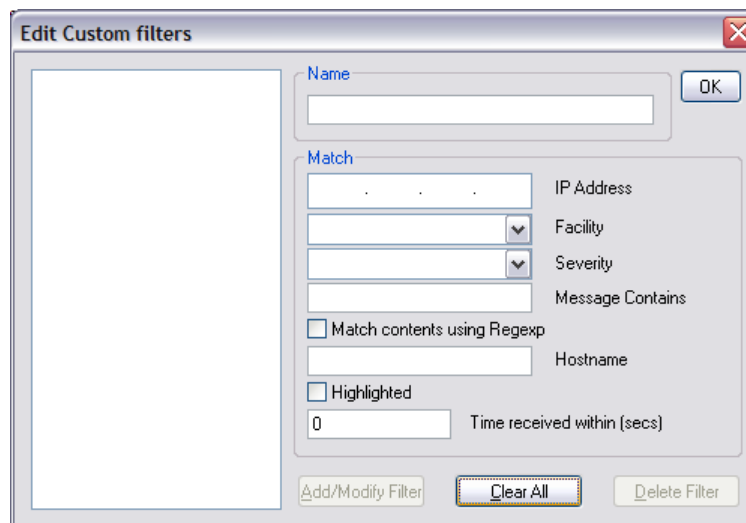
### 6.2.3.3 Options... command (View menu)

Use this to show an option dialog box that controls what information is shown.



### 6.2.3.4 Edit custom filters... (View menu)

Use this command to show the Edit Custom Filters dialog.



The Edit Custom Filter dialog allows you to add filters that control what is displayed.

Each custom filter must be given a name.

For each field that is specified (as opposed to being left blank) the message must match before the message is shown.

For example if the IP address is specified a message must come from that IP address if it is to be shown.

If the 'Match contents using Regexp' option is selected the string used to search the message contents is treated as a regular expression. If this is not set the string is used as a simple case insensitive string that matches if it is contained in the message.

If a filter is added that leaves ALL the match fields blank the rule will match ALL incoming messages.

Filters are shown in the order they appear in the list. The order can be changed by clicking on the name and dragging it to the position required.

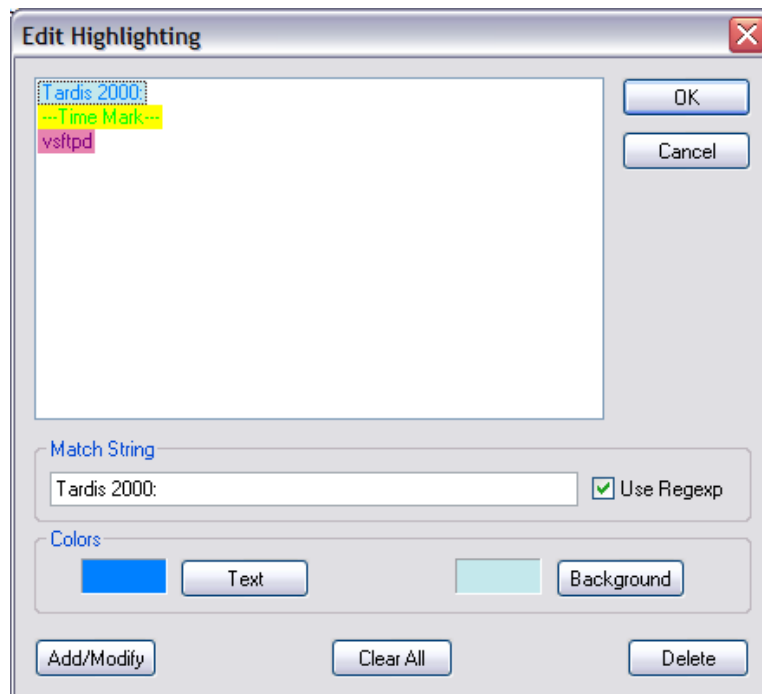
The 'time received within' entry is relative to the currently selected message in the message pane. If none is selected, the entries are relative to 'now'. A value of 0 means don't look at the received time.

To edit a filter double-click on the name in the list. To save the modifications press 'Add/Modify Filter'.

To delete a filter, double-click it then press 'Delete Filter'. Delete all by pressing 'Clear All'.

### 6.2.3.5 Edit Highlighting... (View menu)

Use this command to show the Edit Highlighting dialog.



The Edit Highlighting dialog allows you to control how message text is displayed.

Each message is compared against the match strings. If the message contains a match string the message is shown with the defined text and background colors. Match Strings are compared in the order they appear in the list.

In the case where more than one match string matches, the colors highest in the list are used.

Press the text and background buttons to set the colors.

The order of the match strings may be changed by clicking on the string and dragging it to the position required.

If the 'use Regexp' option is selected the match string used to search the message contents is treated as a regular expression.

If this is not set the match string is used as a simple case insensitive string that matches if it is contained in the message.

To edit an entry double-click on the name in the list. To save the modifications press 'Add/Modify Filter'.

To delete match strings, select them then press 'Delete'. Delete all by pressing 'Clear All'.

For example, if the match string 'router' is specified with red text on a yellow background all messages that contain the text 'router' will be shown with those colors.

**Note:** This type of highlighting is different from the Highlight action. This type of highlighting may be configured differently for each PC using LogLady. A logfile moved from one PC to another would not maintain the same colors. Messages highlighted by the Highlight action do maintain their highlighted state if they are saved to a file and are loaded into another PC running LogLady.

## 6.2.4 Rules Menu

The Rules menu offers the following commands:

<b>Rules Enabled</b>	Enable/Disable Rule processing
<b>Edit rules...</b>	Edit the list of Rules
<b>First rule only</b>	Only act on the first matching Rule
<b>All matching Rules</b>	Act on all matching Rules
<b>E-mail settings...</b>	Configure the E-Mail connection
<b>Database settings...</b>	Set the ODBC DSN to be used for the Write to Database action

### 6.2.4.1 Rules Enabled (Rules menu)

Use this command to enable or disable all rule processing. When rules are enabled this option is checked.

### 6.2.4.2 Edit rules... (Rules menu)

Use this command to show the Edit Rules dialog.

### 6.2.4.3 First Rule only (Rules menu)

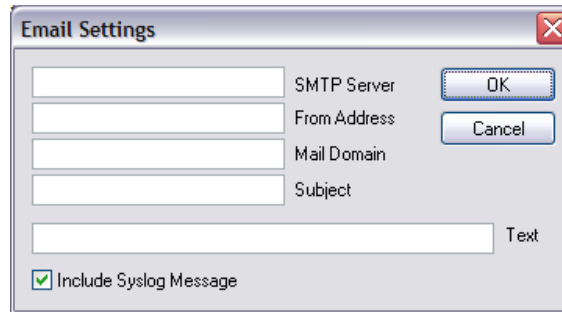
Use this command to tell LogLady that it should use only the first matching rule. This option is checked when it is active.

### 6.2.4.4 All matching rules (Rules menu)

Use this command to tell LogLady that it should use all the matching rules. This option is checked when it is active.

### 6.2.4.5 E-mail settings... (Rules menu)

Use this command to show the E-Mail Settings dialog.



The E-Mail Settings dialog box allows you to set the server that LogLady will use to send E-Mail.

<b>SMTP Server</b>	This is the address of the E-Mail server you want to use.
<b>From Address</b>	This is the E-Mail address that LogLady messages will appear to come from. This should be a valid user as many servers will reject messages that don't have a valid from address.
<b>Mail Domain</b>	This is the part of the E-Mail address after the @ that LogLady messages will appear to come from. This should be a valid address as many servers will reject messages that don't have a valid from address.
<b>Subject</b>	The subject of the E-Mail messages
<b>Text</b>	What the message says
<b>Include Syslog Message</b>	When this is checked the Syslog message that caused the E-Mail to be sent will be included in the E-Mail in human readable form.

### 6.2.4.6 Database settings... (Rules menu)

Use this command to set the ODBC DSN to be used for the 'Write to Database' action.

## 6.2.5 Monitors Menu

The Monitors menu offers the following commands:

<b>Event Log</b>	Enable/Disable Event Log Monitoring
<b>Files/Folders</b>	Enable/Disable File/Folder Monitoring
<b>Edit File/Folder List...</b>	Edit the list of Files/Folders to monitor
<b>Ping Network Devices</b>	Enable/Disable Ping Monitoring
<b>Edit Ping List...</b>	Edit the list of Network Addresses to monitor
<b>Phone Calls</b>	Enable/Disable Phone Call Monitoring
<b>SNMP Traps</b>	Enable/Disable SNMP Trap Monitoring

### 6.2.5.1 Event Log (Monitors menu)

Any messages logged to the local Windows Event Log should be treated as though they were sent as Syslog messages. This allows Windows and Syslog messages to be viewed at the same time and also means that the Windows messages can be filtered, sorted and acted on using Rules. This option is checked when it is active.

### 6.2.5.2 Files/Folders (Monitors menu)

Use this command to tell LogLady that it should watch a list of folders and/or files for modifications. When modifications are made the event is logged as a syslog message. This option is checked when it is active.

### 6.2.5.3 Edit File/Folder List... (Monitors menu)

Use this command to show the Edit List of Files and Folders to Monitor dialog. The dialog controls which files and/or folders are monitored.

### 6.2.5.4 Ping Network Devices (Monitors menu)

Use this command to tell LogLady that it should watch a list of network addresses for changes. When changes are observed the event is logged as a syslog message. This option is checked when it is active.

### 6.2.5.5 Edit Ping List... (Monitors menu)

Use this command to show the Edit Ping List... dialog. The dialog controls which network addresses are monitored.

### 6.2.5.6 Phone Calls (Monitors menu)

Use this command to tell LogLady that it should watch any attached modems for phone calls. If the modem is capable of reporting the phone number being used that is included too. The event is logged as a syslog message. This option is checked when it is active.

### 6.2.5.7 SNMP Traps (Monitors menu)

Use this command to tell LogLady that it should watch for SNMP traps, the event is logged as a syslog message. This option is checked when it is active.

## 6.2.6 Help Menu

The Help menu offers the following commands:

- |                       |                              |
|-----------------------|------------------------------|
| <b>About LogLady</b>  | Show information on LogLady  |
| <b>Help Topics...</b> | Show an index of help topics |

## 7 Monitors

Monitors are used by LogLady to generate syslog messages for events from various sources.

This powerful feature means that many sources of log messages can be merged.

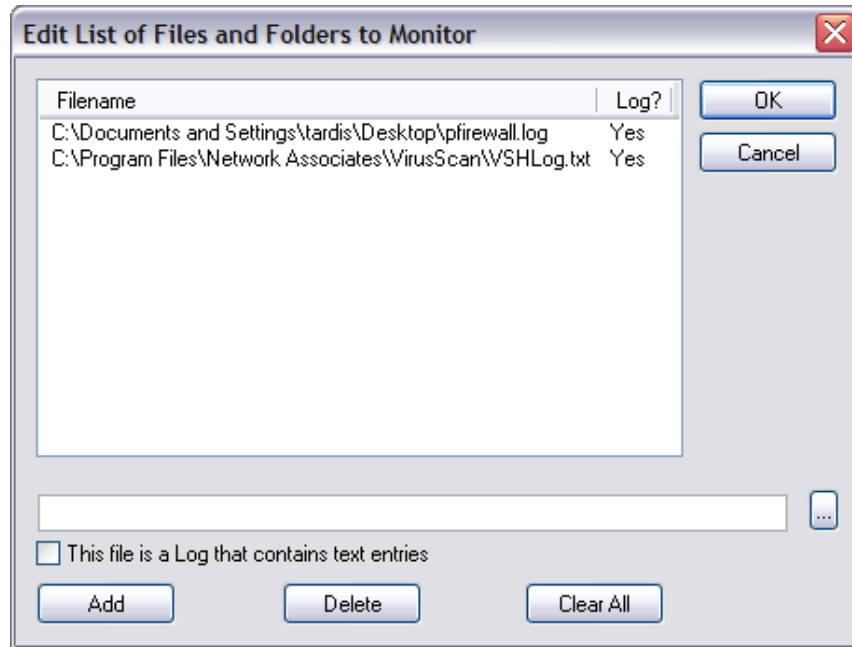
Syslog messages, Windows Event Log messages, and messages from textual log files can all be viewed in sequence using LogLady.

Messages generated by monitors can be filtered, sorted and acted on using Rules.

These are the currently supported types of Monitor.

<b>Eventlog</b>	Any messages logged to the local Windows Event Log should be treated as though they were sent as <i>syslog</i> messages. This allows Windows and <i>syslog</i> messages to be viewed at the same time.
<b>Files/Folders</b>	LogLady can watch a list of files and/or folders for changes. This allows modifications to important files to be audited and actions taken. The list of files can be changed using the Edit Files/Folders List... dialog.  Textual log files generated by other applications can be monitored. New log file entries are merged in with other <i>syslog</i> messages.
<b>Ping Network Device</b>	LogLady can periodically 'ping' a list of network addresses to determine if they respond. This can be used to log devices connecting and disconnecting from the network. The list of addresses to ping can be changed using the Edit Ping List... dialog.
<b>Phone Calls</b>	LogLady can watch any attached modems for phone calls. If the modem is capable of reporting the phone number being used that is included too. The modems must be connected using TAPI.
<b>SNMP Traps</b>	LogLady can watch for SNMP traps generated by other network-based equipment. Any data contained is shown in the log message.

The Edit Files/Folders List... dialog allows you to edit the list of files and/or folders to be monitored.



Press the '...' button to select files or just type the name and press 'Add'.

Files can also be added by dragging files to the dialog.

To delete files from the list, select them then press 'Delete'. Delete all by pressing 'Clear All'.

If the '*This file is a Log that contains text entries*' option is set when adding a file the contents of the file are treated as a log file. Log files are often generated by applications to record their ongoing operations. For example the Windows firewall can be set to log messages to a file.

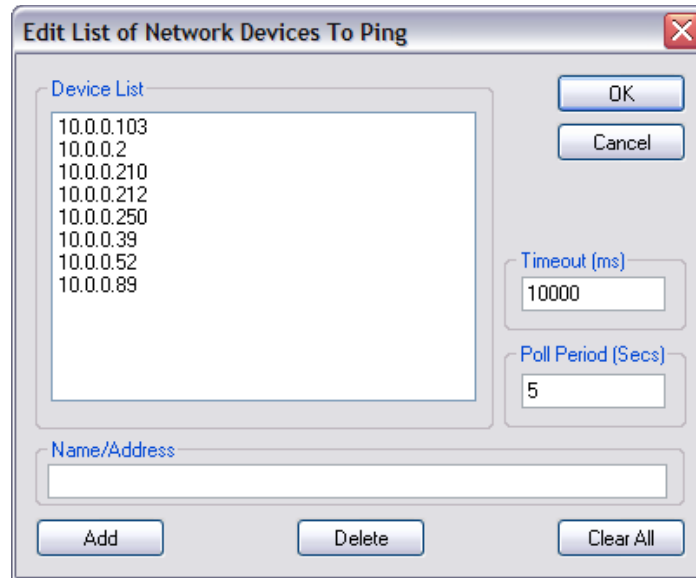
When LogLady knows the file is a log file it will do more than just report that the file has changed. As new messages are added to the log file LogLady will copy them into the list of *syslog* messages.

This powerful feature means that many sources of log messages can be merged into a single list.

*Syslog* messages, Windows Event Log messages and messages from textual log files can all be viewed in sequence using LogLady.

The Edit Ping List... dialog allows you to edit the list of network addresses to be monitored.





Type the name or address and press 'Add'.

To delete from the list, select them then press 'Delete'. Delete all by pressing 'Clear All'.

Poll Period determines how many seconds elapse between attempts to ping the list.

Timeout controls how many milliseconds to wait for a response.

## 8 Rules

Rules enable LogLady to recognize and act on messages of interest.

Each message is compared against each active rule, and, if it matches the fields specified, the relevant action is executed.

For example, if a rule is defined to match messages with severity 'Error' from IP address 10.0.0.20 the action might be to place a dialog box on screen. If the IP address is not specified all messages with severity 'Error' will result in a dialog box. If no severity or any other field is specified ALL messages will result in a dialog box.

If the 'Match contents using Regexp' option is selected the string used to search the message contents is treated as a *regular expression*. If this is not set the string is used as a simple case insensitive string that matches if it is contained in the message.

A single message may result in many actions if many rules match. However, if the first rule only option is set in the Rules Menu only the first matching rule is used.

Rules are searched in the order shown in the list in the Edit Rules dialog.

The Edit Rules dialog allows you to add Rules that control Actions. Actions provide a way to do something about the incoming messages by send E-Mail messages, playing a sound etc.

Each rule must be given a name. The match section of the dialog provides a way of filtering the messages so that only certain messages cause actions. For each field that is specified (as opposed to being left blank) the message must match before the action will happen.

For example if the IP address is specified a message must come from that IP address before the action is triggered.

If the 'Match contents using Regexp' option is selected the string used to search the message contents is treated as a regular expression.

If this is not set the string is used as a simple case insensitive string that matches if it is contained in the message.

If a rule is added that leaves ALL the match fields blank the rule will match ALL incoming messages. This can be used to save all messages to a file.

Rules may have a **threshold** set to prevent a burst of messages that all match the same rule from generating the same action multiple times. This applies to each sending IP address separately. The value is the number of seconds that must elapse since the last matching message before the rule will match again. A value of 0 disables any threshold for the rule.

Rules are searched in the order they appear in the list. The order may be changed by clicking on the name and dragging it to the position required. The order is particularly important when the 'first rule only' option is set in the Rules Menu. Only the highest priority matching rule will be used in this case. Each rule may be disabled individually or all rules may be disabled if the option is set in the Rules Menu.

To start a new rule press 'New Rule'

To edit a rule double-click on the name in the list.

To save the modifications press 'Add/Modify Rule'.

To delete a rule, double-click it then press 'Delete Rule'. Delete all rules by pressing 'Clear All'.

## 9 Actions

### 9.1 Description

When a *rule* matches a message an associated *action* is triggered.

The following Actions are available:

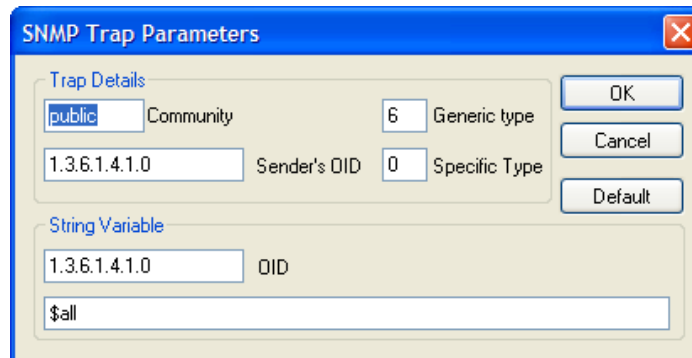
<b>Message Box</b>	Show a message box on the screen. Only one is active at a time. If a new message arrives and a message box is already being displayed it is replaced. The message box is automatically removed after a number of seconds. The length of time it is displayed is configured in the preferences. This action is allowed to use <i>special strings</i> to customise the text of the message box.
<b>Run Program</b>	Run a program. The full path and any parameters may be specified. This action is allowed to use <i>special strings</i> to customise the parameters passed to the program.
<b>Save to file</b>	Save this message to a file. The file can be loaded by LogLady later. The name may contain <i>special filename characters</i> used to influence the name of the file.
<b>Send to another Syslog server</b>	Forward this message to another Syslog server. LogLady can be used to select messages to forward to a main server.
<b>Discard message</b>	Delete this message as if it had never been received. Useful if a device generates a lot of uninteresting messages. If a message is discarded no further rules are processed for it. E.g. a message may match several rules. If a matching rule is higher priority than the discard rule it will be processed. If a rule is lower priority it will not be processed.
<b>Highlight message</b>	Mark this message to be displayed in reversed colors in the main window.
<b>Play sound</b>	Play a .WAV sound.
<b>Send E-Mail</b>	Send an E-Mail message. The details of the E-Mail connection are configured in the E-Mail Settings dialog. The settings may be changed for each rule by pressing the <b>Advanced</b> button.
<b>Copy to Windows Event Log</b>	Syslog messages are copied into the Windows Event Log 'Application' section with the event source 'loglady'
<b>Save to Database</b>	Execute the associated SQL statement. The database used is defined in the Database Settings... option in the Rules menu. This action is allowed to use <i>special strings</i> to customise the SQL statement.
<b>Modify Facility</b>	Change the Facility field of the incoming message. This can be useful when monitoring Windows Event Log messages. For example a Windows message from the security log could be modified to have a 'security' facility. Note: If you use this action it will not be possible to determine the original facility of the message, which might affect the audit trail.
<b>Modify Severity</b>	Change the Severity field of the incoming message. This can be useful if a message very important to you is given a low severity, or if an incoming message is marked as an emergency when it isn't really that bad. Note: If you use this action it will not be possible to determine the original facility of the message, which might affect the audit trail.
<b>Send SNMP Trap</b>	Send an SNMP Trap to an SNMP server. The text of the message is contained in the trap. Traps sent are SNMP V1. Default settings for the trap may be changed for each rule by pressing the <b>Advanced</b> button.

Remember, a message may trigger one or more rules resulting in a number of actions for one message.

## 9.2 *Advanced settings*

### 9.2.1 SNMP Trap

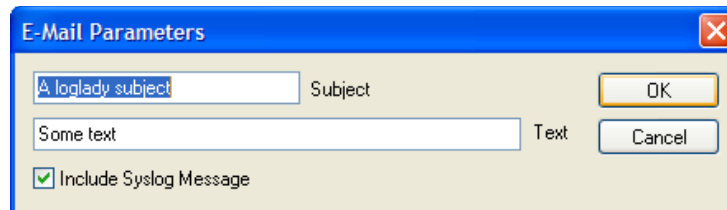
The SNMP trap action has default parameters but you may want to change these on a per rule basis. Pressing the **advanced** button allows the trap's details to be changed.



The image shows a dialog box titled "SNMP Trap Parameters". It has a blue title bar with a close button (X) in the top right corner. The dialog is divided into two sections. The first section, "Trap Details", contains four input fields: "Community" with the value "public", "Generic type" with the value "6", "Sender's OID" with the value "1.3.6.1.4.1.0", and "Specific Type" with the value "0". To the right of these fields are three buttons: "OK", "Cancel", and "Default". The second section, "String Variable", contains two input fields: "OID" with the value "1.3.6.1.4.1.0" and a larger text area containing the value "\$all".

### 9.2.2 E-Mail

The E-mail action has default parameters set in the E-Mail settings dialog box. These may be changed for each rule by pressing the **advanced** button.



The image shows a dialog box titled "E-Mail Parameters". It has a blue title bar with a close button (X) in the top right corner. The dialog contains three input fields: "Subject" with the value "A loglady subject", "Text" with the value "Some text", and a checked checkbox labeled "Include Syslog Message". To the right of these fields are two buttons: "OK" and "Cancel".

### 9.3 Special string options

For some Actions the contents of the Message can be used to make the Action more informative.

The Message Box, Run Program, advanced SNMP Trap string, and Write to Database Actions have associated values that can be modified with the Message contents.

The following values are replaced with information extracted from the message that triggered the Action.

<b>\$facility</b>	Is replaced with the facility E.g. NTP
<b>\$hostname</b>	Is replaced with the hostname
<b>\$ipaddr</b>	Is replaced with the IP Address
<b>\$severity</b>	Is replaced with the severity E.g. Warning
<b>\$recvtime</b>	Is replaced with the time the message was received
<b>\$recvstdtime</b>	Is replaced with the time the message was received, the time is yyyy-mm-dd hh:mm:ss UTC
<b>\$msg</b>	Is replaced with the text of the message
<b>\$all</b>	Is replaced by a combination of all of the above

#### 9.3.1 Examples

If the Action is 'Message Box' the Message can be set to \$msg resulting in the text of the syslog message being placed in the message box.

An Action of 'Write to Database' might have an associated SQL statement like

```
INSERT INTO log VALUES ('$msg')
```

### 9.4 Special Filename Characters

File names may contain 'strftime' escape sequences to allow the logging file to be named appropriately.

This is the full list

<b>%a</b>	Abbreviated weekday name
<b>%A</b>	Full weekday name
<b>%b</b>	Abbreviated month name
<b>%B</b>	Full month name
<b>%c</b>	Date and time representation appropriate for locale
<b>%d</b>	Day of month as decimal number (01 – 31)
<b>%H</b>	Hour in 24-hour format (00 – 23)
<b>%I</b>	Hour in 12-hour format (01 – 12)
<b>%j</b>	Day of year as decimal number (001 – 366)
<b>%m</b>	Month as decimal number (01 – 12)
<b>%M</b>	Minute as decimal number (00 – 59)
<b>%p</b>	Current locale's A.M./P.M. indicator for 12-hour clock
<b>%S</b>	Second as decimal number (00 – 59)
<b>%U</b>	Week of year as decimal number, with Sunday as first day of week (00 – 53)
<b>%w</b>	Weekday as decimal number (0 – 6; Sunday is 0)

<b>%W</b>	Week of year as decimal number, with Monday as first day of week (00 – 53)
<b>%x</b>	Date representation for current locale
<b>%X</b>	Time representation for current locale
<b>%y</b>	Year without century, as decimal number (00 – 99)
<b>%Y</b>	Year with century, as decimal number
<b>%z, %Z</b>	Time-zone name or abbreviation; no characters if time zone is unknown
<b>%%</b>	Percent sign

### 9.4.1 Examples

**%B** will be replaced by the full month name so the log file **%B.txt** will be called **April.txt** in April and **May.txt** in May.

The log file **%d%m.txt** will be called **0101.txt** on 1 jan and **0407.txt** on July 4<sup>th</sup>.

## 10 Using LogLady, Examples

These examples show how LogLady can do useful things when events occur.

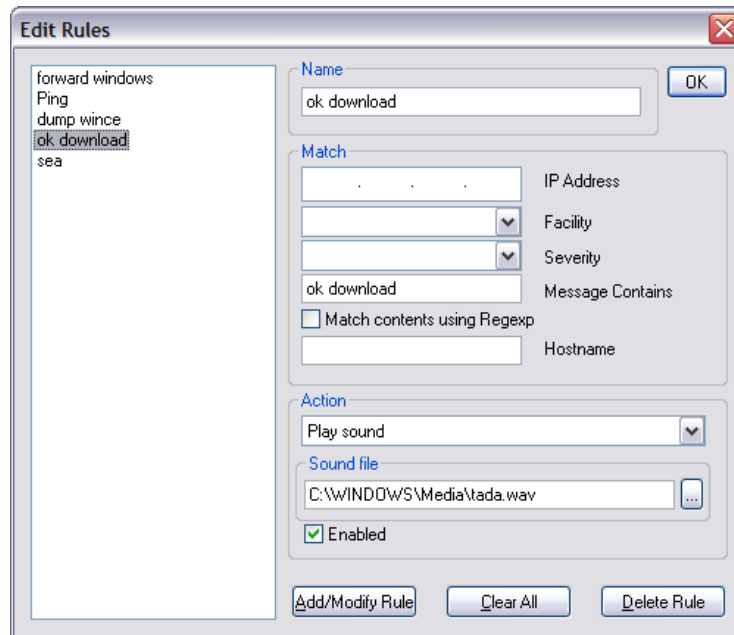
### 10.1 Play a sound when a message of interest arrives

In this example we assume that a Linux server is set up to be an ftp server using vsftpd and that *syslog* messages are forwarded on to a PC running LogLady.

The message received will look something like this

```
vsftpd: Fri Sep 9 15:59:19 2005 [pid 3789] [ftp] OK DOWNLOAD: Client  
"123.123.123.123", "/Tardis2000.pdf", 572883 bytes, 22.30Kbyte/sec
```

Select Rules->Edit Rules, create a rule called 'ok download'.



Enter 'ok download' as the string that the message must contain. Set the action to 'Play Sound' and select a sound file. Press Add/Modify Rule, Press OK to save the change. Now, whenever a message that contains 'ok download' arrives the selected sound is played.



## 10.2 Forward All Windows Event Log Messages to a Linux Syslog Server

In this example we assume that a Linux server is set up to be a syslog server.

Select Rules->Edit Rules, create a rule called 'forward all windows'.

The screenshot shows the 'Edit Rules' dialog box. The 'Name' field is 'forward all windows'. The 'Match' section has 'Facility' set to 'Windows'. The 'Action' is 'Send to another Syslog server' and the 'Server' is '10.0.0.123'. The 'Enabled' checkbox is checked.

Make sure that the Event Log Monitor is enabled, Monitors->Event Log. Windows Event Log messages are copied into LogLady with the special facility 'Windows'.

Select 'Windows' as the required facility that the message must contain. Set the action to 'Send to another Syslog Server' and select the address of the Linux syslog server. Press Add/Modify Rule, Press OK to save the change. Now, whenever a message that had the 'Windows' facility, i.e. comes from the Windows Event Log, arrives the message is forwarded.

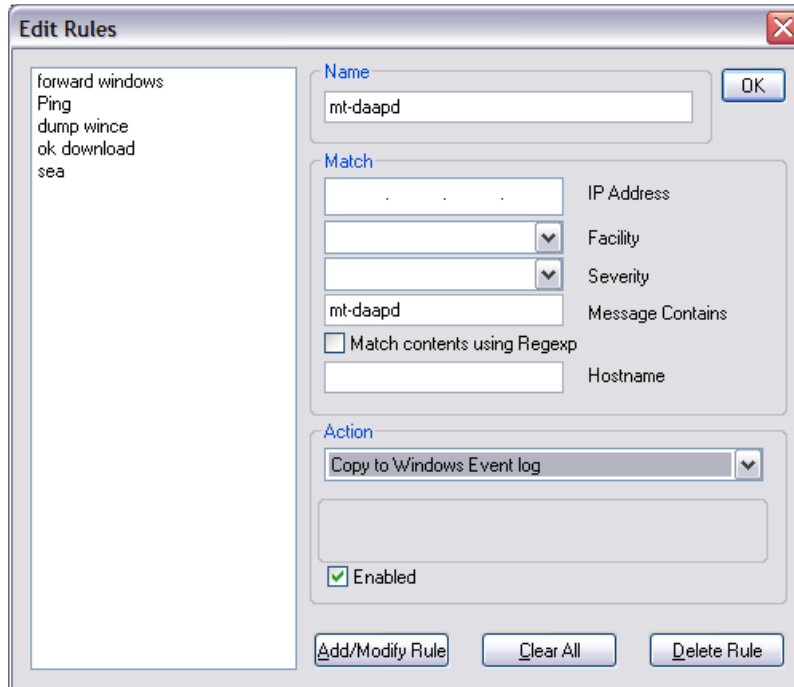
### 10.3 Put some Linux Syslog messages in the Windows Event Log

We assume that a Linux server is set to send *syslog* messages to LogLady. We have decided that we want all messages generated by the *mt-daapd* program running on the Linux system to be copied to the Windows Event Log.

The message received may look something like this

```
mt-daapd[3834]: Session 11: Streaming file '17 The Cure - A Night Like This.mp3' to 123.123.123.123 (offset 0)
```

Select Rules->Edit Rules, create a rule called 'mt-daapd'.



Enter 'mt-daapd' as the string that the message must contain. You may also enter the IP address to the Linux system to further restrict the selection if required. Set the action to 'Copy to Windows Event Log'. Press Add/Modify Rule, Press OK to save the change. Now, whenever a message that contains 'mt-daapd' arrives the message is copied into the Windows Event Log 'Application' section with the event source 'loglady'

### 10.4 Send me an e-mail when a linux system is rebooted

To do this we need to match a message that is sent when the Linux system starts and at no other time.

For example

```
CPU: XScale-IXP425/IXC1100 revision 1
```

This message identifying the CPU is only sent when the system boots. You should look for a similar message that matches your machine. It is highly unlikely that the above message will work for you.

Create a rule containing the IP address of the Linux system and include the full text of the message in the 'message contains'. Set the action to 'Send E-mail' and set the To address to the recipient of the message.

Make sure you have previously set the E-Mail settings in Rules->E-Mail settings...

### 10.5 Show me when my firewall traps access a banned website

In this example we assume that a firewall/router is set to stop access to undesirable websites. The firewall/router is set to send the resulting syslog messages to the PC running LogLady.

The message received may contain a string that LogLady can match e.g. the words 'access denied'

Select Rules->Edit Rules, create a rule called 'banned'.

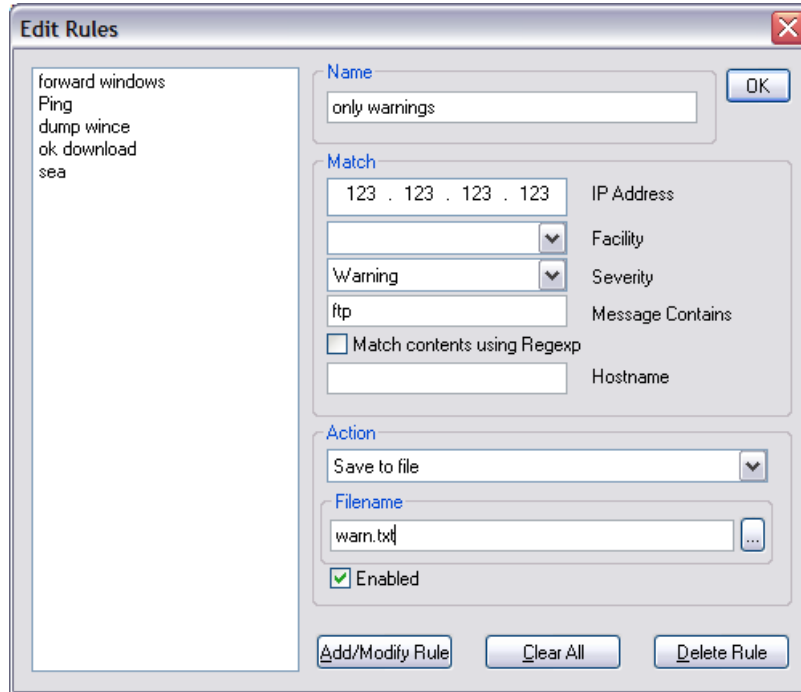
The screenshot shows the 'Edit Rules' dialog box. On the left, a list of rules includes 'forward windows', 'Ping', 'dump wince', 'ok download', and 'sea'. The 'Name' field is 'banned'. The 'Match' section includes fields for 'IP Address', 'Facility', 'Severity', and 'Message Contains' (set to 'access denied'). There is an unchecked checkbox for 'Match contents using Regexp' and an empty 'Hostname' field. The 'Action' dropdown is 'Message Box'. The 'Message' field contains '\$msg'. The 'Enabled' checkbox is checked. At the bottom are buttons for 'Add/Modify Rule', 'Clear All', and 'Delete Rule'.

Enter 'access denied' as the string that the message must contain. Set the action to 'message box' and enter \$msg as the message. Press Add/Modify Rule, Press OK to save the change. Now, whenever a message that contains 'access denied' arrives the contents of the message is shown on in a message box.

## 10.6 Save a restricted set of messages in their own log file

Create a rule called 'only warning'; enter the restrictions on the messages we want to save to their own file.

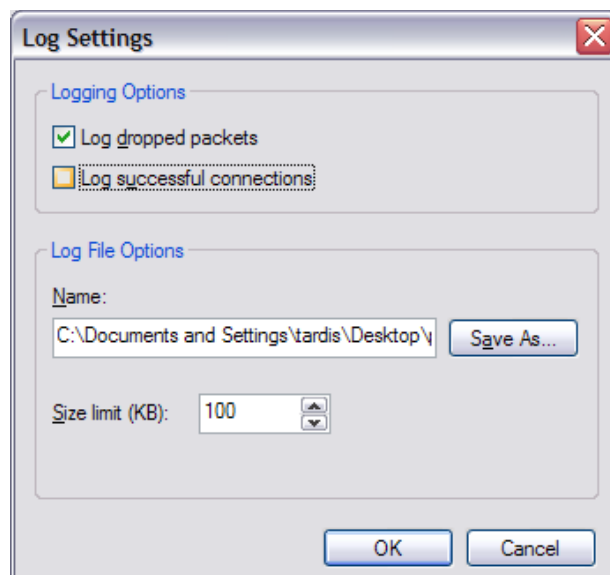
E.g they must come from 123.123.123.123 AND be a warning AND contain the word ftp. Select the action 'write to file' and enter the name 'warn.txt'. All messages that match will be written to the file in addition to the default log. The new file warn.txt can be loaded into LogLady at any time for analysis.



## 10.7 Include the Windows firewall logging in LogLady

This demonstrates how to monitor a file for changes and incorporate the lines added into the logging.

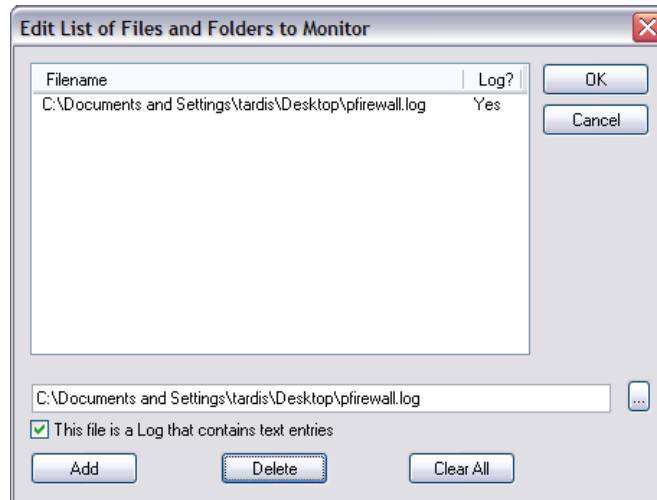
First switch on the firewall advanced logging. In the firewall control panel select the 'advanced' tab and press the 'security logging' button.



Switch on one or both Logging options and select a location and size for the logfile. Remember the location.

In LogLady Select Monitors->Edit File/Folder List...

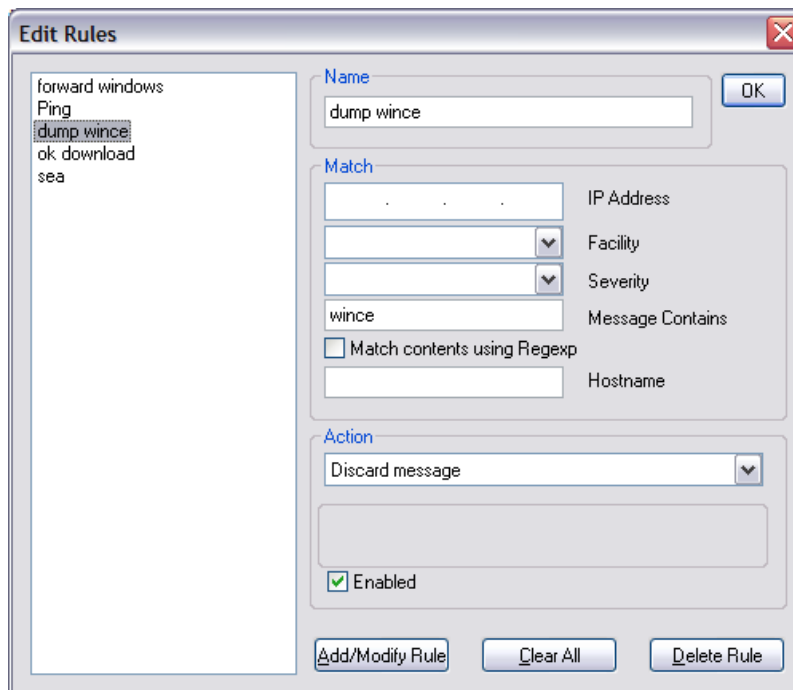
Add the full name of the firewall logfile that you remembered and select the 'This file is a Log that contains text entries' option. Press 'Add' then OK.



Make sure that Monitors->Files/Folders is selected to make LogLady watch the firewall log for changes. When changes occur LogLady will determine which lines have been added and will include them as if it had been sent them using the *syslog* protocol.

## 10.8 Discard messages

Create a rule to discard messages that we aren't interested in. Enter the string to match e.g. 'wince' select the action 'discard message'.



Every message that arrives containing 'wince' will be removed. It will not appear in the log.

### 10.9 Save all Warning or higher messages to a database

Create a rule with an appropriate name e.g. 'write to db'.

Set the severity to 'Warning or greater'. Set the action to 'Write to database'. Enter an appropriate SQL statement to write the entry.

The screenshot shows the 'Edit Rules' dialog box. On the left is a list of rules: 'forward windows', 'Ping', 'dump wince', 'ok download', and 'sea'. The 'write to db' rule is selected. The 'Name' field contains 'write to db'. The 'Match' section has 'Warning or Higher' selected for Severity. The 'Action' is 'Save to Database' and the 'SQL Statement' is 'INSERT INTO log VALUES('\$msg')'. The 'Enabled' checkbox is checked. Buttons for 'Add/Modify Rule', 'Clear All', and 'Delete Rule' are at the bottom.

You must have previously set up the database connection in Rules->Database settings AND created the database table (named 'log' in this example). You will need some database knowledge to do this.

## 11 Regular Expressions

### 11.1 Description

A *regular expression* is a formula for matching strings that follow some pattern. Regular expressions are made up of normal characters and metacharacters. Normal characters include upper and lower case letters and digits. The metacharacters have special meanings and are described in detail below.

Metacharacter	Meaning
<code>^</code>	Match the beginning of line
<code>\$</code>	Match the end of line
<code>.</code>	Match any character
<code>[]</code>	Match characters in set
<code>[^ ]</code>	Match characters not in set
<code>?</code>	Match previous pattern 0 or 1 times (greedy)
<code> </code>	Match previous or next pattern
<code>@</code>	Match previous pattern 0 or more times (non-greedy)
<code>#</code>	Match previous pattern 1 or more times (non-greedy)
<code>*</code>	Match previous pattern 0 or more times (greedy)
<code>+</code>	Match previous pattern 1 or more times (greedy)
<code>{ }</code>	Group characters to form one pattern
<code>( )</code>	Group and remember
<code>\</code>	Quote next character (only of not a-z)
<code>&lt;</code>	Match beginning of a word
<code>&gt;</code>	Match end of a word
<code>\x##</code>	Match character with ASCII code ## (hex)
<code>\N###</code>	Match ASCII code ### (dec)
<code>\o###</code>	Match ASCII code
<code>\a</code>	Match \a
<code>\r</code>	Match 0x13 (cr)
<code>\b</code>	Match \b
<code>\t</code>	Match 0x09 (tab)
<code>\f</code>	Match \f
<code>\v</code>	Match \v
<code>\n</code>	Match 0x10 (lf)
<code>\e</code>	Match escape (^E)
<code>\s</code>	Match whitespace (cr/lf/tab/space)
<code>\S</code>	Match nonwhitespace (!\S)
<code>\w</code>	Match word character
<code>\W</code>	Match non-word character
<code>\d</code>	Match digit character
<code>\D</code>	Match non-digit character
<code>\U</code>	Match uppercase
<code>\L</code>	Match lowercase
<code>\C</code>	Match case sensitively from here on
<code>\c</code>	Match case ignore from here on

## 11.2 Examples

### Regular expression

### Matches

"a"	"a"
"aaaa"	"aaaa"
"."	"a"
"a.."	"axx"
"a?b"	"ab"
"a?b"	"xb"
"{aa}?b"	"aab"
"{aa}?b"	"xab"
"^aa"	"aa"
"^aa\$"	"aa"
"a*b"	"aaab"
"{aa}*b"	"aaab"
"b+"	"bb"
"b+"	"b"
"^b+\$"	"b"
"a b"	" a "
"a b"	" b "
"a b c d e"	" a "
"a b c d e"	" c "
"a b c d e"	" e "
"{a} {b} {c} {d} {e}"	" a "
"{a} {b} {c} {d} {e}"	" c "
"{a} {b} {c} {d} {e}"	" e "
"^xx{alpha} {beta}xx\$"	"xxalphaxx"
"^xx{alpha} {beta}xx\$"	"xxbetaxx"
"[a-z]"	"aaa"
"^{Error} {Warning}"	"Warning search.cpp 35: Conversion may lose significant digits in function AskReplace()"
"^{Error} {Warning} (.+)"	"Warning search.cpp 35: Conversion may lose significant digits in function AskReplace()"
"^{Error} {Warning} ([a-z.]#) ([0-9]#)"	"Warning search.cpp 35: Conversion may lose significant digits in function AskReplace()"
"^{Error} {Warning} (.+) ([0-9]+): (.*)\$"	"Warning search.cpp 35: Conversion may lose significant digits in function AskReplace()"
"^{Error} {Warning} (.+) ([0-9]+): (.*)\$"	"Error search.cpp 35: Conversion may lose significant digits in function AskReplace()"
"^([a-z]+ +)*\\("	"blabla bla bla bla ("
"^([a-z]+\\s+)+\\("	"blabla bla bla bla ("
"^([a-z]+\\s*)+\\("	"blabla bla bla bla ("
"^([a-z]+\\s+)+\\("	"blabla bla bla bla ("
"^([a-z]+\\s*)+\\("	"blabla bla bla bla ("
"^([a-z]# #)*\\("	"blabla bla bla bla ("
"^([a-z]+ @)@\\("	"blabla bla bla bla ("
"^[\x20-\xFF]+\$"	"blabla"
"{a}{a}{a a} {a a}a}a a}"	"aaaaaaaaaaaaaaaaa"

Regexp code by Marko Macek



## 12 Syslog Message Fields

The important parts of a Syslog message are:

- The address of the device that sent it.
- The facility that originated the message, i.e. the subsystem on the device.
- The severity of the message. How important the message is.
- When it was sent.
- The text of the message itself.

LogLady can filter and sort messages based on the contents of these fields.

There follows a more technical description of the format of a Syslog message. It is an extract from the full text found in RFC 3164.

### 4.1 syslog Message Parts

The full format of a syslog message seen on the wire has three discernable parts. The first part is called the PRI, the second part is the HEADER, and the third part is the MSG. The total length of the packet MUST be 1024 bytes or less. There is no minimum length of the syslog message although sending a syslog packet with no contents is worthless and SHOULD NOT be transmitted.

#### 4.1.1 PRI Part

The PRI part MUST have three, four, or five characters and will be bound with angle brackets as the first and last characters. The PRI part starts with a leading "<" ('less-than' character), followed by a number, which is followed by a ">" ('greater-than' character). The code set used in this part MUST be seven-bit ASCII in an eight-bit field as described in RFC 2234 [2]. These are the ASCII codes as defined in "USA Standard Code for Information Interchange" [3]. In this, the "<" character is defined as the Augmented Backus-Naur Form (ABNF) %d60, and the ">" character has ABNF value %d62. The number contained within these angle brackets is known as the Priority value and represents both the Facility and Severity as described below. The Priority value consists of one, two, or three decimal integers (ABNF DIGITS) using values of %d48 (for "0") through %d57 (for "9").

The Facilities and Severities of the messages are numerically coded with decimal values. Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following table along with their numerical code values.

Numerical Facility

Value	Meaning
0	kernel messages
1	user-level messages
2	mail system
3	system daemons

4	security/authorization messages (note 1)
5	messages generated internally by syslogd
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon (note 2)
10	security/authorization messages (note 1)
11	FTP daemon
12	NTP subsystem
13	log audit (note 1)
14	log alert (note 1)
15	clock daemon (note 2)
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

Table 1. syslog Message Facilities

Note 1 - Various operating systems have been found to utilize Facilities 4, 10, 13 and 14 for security/authorization, audit, and alert messages which seem to be similar.

Note 2 - Various operating systems have been found to utilize both Facilities 9 and 15 for clock (cron/at) messages.

Each message Priority also has a decimal Severity level indicator. These are described in the following table along with their numerical values.

#### Numerical Severity

Value	Meaning
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

Table 2. syslog Message Severities

The Priority value is calculated by first multiplying the Facility number by 8 and then adding the numerical value of the Severity. For example, a kernel message (Facility=0) with a Severity of Emergency

(Severity=0) would have a Priority value of 0. Also, a "local use 4" message (Facility=20) with a Severity of Notice (Severity=5) would have a Priority value of 165. In the PRI part of a syslog message, these values would be placed between the angle brackets as <0> and <165> respectively. The only time a value of "0" will follow the "<" is for the Priority value of "0". Otherwise, leading "0"s MUST NOT be used.

#### 4.1.2 HEADER Part of a syslog Packet

The HEADER part contains a timestamp and an indication of the hostname or IP address of the device. The HEADER part of the syslog packet MUST contain visible (printing) characters. The code set used MUST also be seven-bit ASCII in an eight-bit field like that used in the PRI part. In this code set, the only allowable characters are the ABNF VCHAR values (%d33-126) and spaces (SP value %d32).

The HEADER contains two fields called the TIMESTAMP and the HOSTNAME. The TIMESTAMP will immediately follow the trailing ">" from the PRI part and single space characters MUST follow each of the TIMESTAMP and HOSTNAME fields. HOSTNAME will contain the hostname, as it knows itself. If it does not have a hostname, then it will contain its own IP address. If a device has multiple IP addresses, it has usually been seen to use the IP address from which the message is transmitted. An alternative to this behavior has also been seen. In that case, a device may be configured to send all messages using a single source IP address regardless of the interface from which the message is sent. This will provide a single consistent HOSTNAME for all messages sent from a device.

The TIMESTAMP field is the local time and is in the format of "Mmm dd hh:mm:ss" (without the quote marks) where:

Mmm is the English language abbreviation for the month of the year with the first character in uppercase and the other two characters in lowercase. The following are the only acceptable values:

Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec

dd is the day of the month. If the day of the month is less than 10, then it MUST be represented as a space and then the number. For example, the 7th day of August would be represented as "Aug 7", with two spaces between the "g" and the "7".

hh:mm:ss is the local time. The hour (hh) is represented in a 24-hour format. Valid entries are between 00 and 23, inclusive. The minute (mm) and second (ss) entries are between 00 and 59 inclusive.

A single space character MUST follow the TIMESTAMP field.

The HOSTNAME field will contain only the hostname, the IPv4 address, or the IPv6 address of the originator of the message. The preferred value is the hostname. If the hostname is used, the HOSTNAME field MUST contain the hostname of the device as specified in STD 13 [4]. It should be noted that this MUST NOT contain any embedded spaces. The Domain Name MUST NOT be included in the HOSTNAME field. If the IPv4 address is used, it MUST be shown as the dotted decimal notation as used in STD 13 [5]. If an IPv6 address is used, any valid representation used in RFC 2373 [6] MAY be used. A single space character MUST also follow the HOSTNAME field.

#### 4.1.3 MSG Part of a syslog Packet

The MSG part will fill the remainder of the syslog packet. This will usually contain some additional information of the process that

generated the message, and then the text of the message. There is no ending delimiter to this part. The MSG part of the syslog packet MUST contain visible (printing) characters. The code set traditionally and most often used has also been seven-bit ASCII in an eight-bit field like that used in the PRI and HEADER parts. In this code set, the only allowable characters are the ABNF VCHAR values (%d33-126) and spaces (SP value %d32). However, no indication of the code set used within the MSG is required, nor is it expected. Other code sets MAY be used as long as the characters used in the MSG are exclusively visible characters and spaces similar to those described above. The selection of a code set used in the MSG part SHOULD be made with thoughts of the intended receiver. A message containing characters in a code set that cannot be viewed or understood by a recipient will yield no information of value to an operator or administrator looking at it.

The MSG part has two fields known as the TAG field and the CONTENT field. The value in the TAG field will be the name of the program or process that generated the message. The CONTENT contains the details of the message. This has traditionally been a freeform message that gives some detailed information of the event. The TAG is a string of ABNF alphanumeric characters that MUST NOT exceed 32 characters. Any non-alphanumeric character will terminate the TAG field and will be assumed to be the starting character of the CONTENT field. Most commonly, the first character of the CONTENT field that signifies the conclusion of the TAG field has been seen to be the left square bracket character ("["), a colon character (":"), or a space character. This is explained in more detail in Section 5.3.

#### **4.2 Original syslog Packets Generated by a Device**

There are no set requirements on the contents of the syslog packet as it is originally sent from a device. It should be reiterated here that the payload of any IP packet destined to UDP port 514 MUST be considered to be a valid syslog message. It is, however, RECOMMENDED that the syslog packet have all of the parts described in Section 4.1 - PRI, HEADER and MSG - as this enhances readability by the recipient and eliminates the need for a relay to modify the message.

For implementers that do choose to construct syslog messages with the RECOMMENDED format, the following guidance is offered.

If the originally formed message has a TIMESTAMP in the HEADER part, then it SHOULD be the local time of the device within its timezone.

If the originally formed message has a HOSTNAME field, then it will contain the hostname as it knows itself. If it does not have a hostname, then it will contain its own IP address.

If the originally formed message has a TAG value, then that will be the name of the program or process that generated the message.

Author's Address

Chris Lonvick

Cisco Systems

12515 Research Blvd. Austin, TX, USA

Phone: +1.512.378.1182 EMail: clonvick@cisco.com

Full Copyright Statement Copyright (C)

The Internet Society (2001). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement Funding for the RFC Editor function is currently provided by the Internet Society.

## 13 Troubleshooting

### 13.1 Frequently asked questions

- Q** Why is it called LogLady?
- A** LogLady is named after a character in the Twin Peaks TV series. The name has 'log' in it so it seemed to make sense at the time
- Q** The UNIX/Linux syslogd isn't receiving the messages LogLady sends.
- A** The syslogd must be started with the `-r` option to allow messages that originate from machines to be logged. By default this is usually not set. Another possibility is that the Windows PC has a firewall configured that is blocking the messages
- Q** When might LogLady be useful?
- A** Any time a PC or network device does something interesting that you might want to record and/or react to.

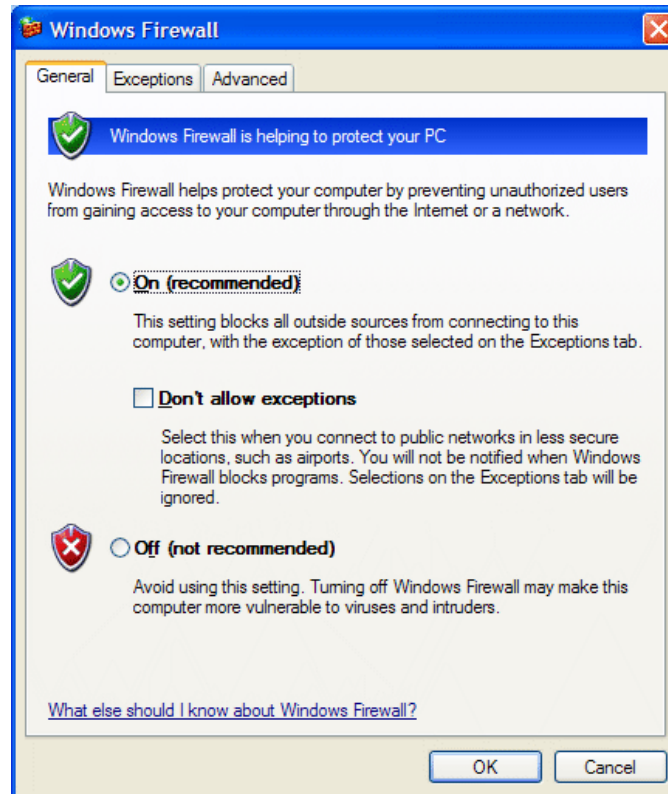
### 13.2 LogLady and Windows firewall

Windows contains a new firewall feature that may interfere with the normal operation of LogLady.

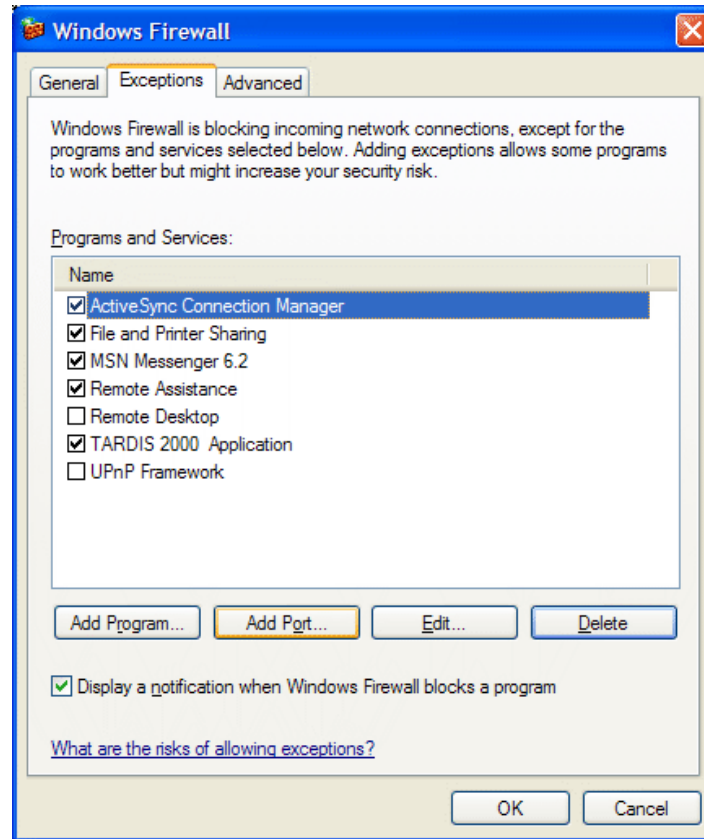
When LogLady runs you may get a message requesting whether LogLady should be Blocked or UnBlocked. You should select 'unblock'. You may also choose to manually configure the firewall.

This describes how to configure the firewall to allow unsolicited syslog messages through to LogLady.

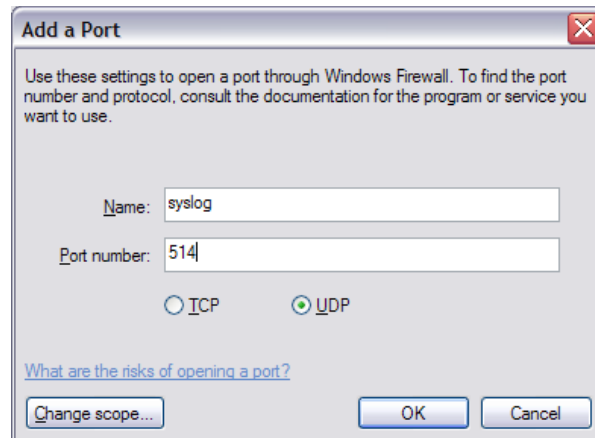
Open the firewall control panel. Make sure the settings are set like this



On the Exception tab click on 'Add Port'



Then add a setting to allow *syslog*.



Press OK and everything should work like it did before SP2 improved things.

Other firewalls may have similar issues. Follow your firewall's recommended process to allow UDP port 514 to be used by LogLady.

If you are using SNMP traps follow the same procedure with the name 'SNMP Traps' and udp port number 162.



## 14 Registering and Paying for LogLady

The following pages details the volume-based charges for LogLady and incorporates a registration form.

There are three ways to pay for registration:

**1) By cheque** payable to HC Mingham-Smith Ltd. Please post to the following address:

HC Mingham-Smith Ltd.  
33 Arthur Rd.  
Wokingham,  
Berkshire RG41 2SS  
England.

### 2) By Bank Transfer

If you would prefer to pay by this method, please contact us on the following e-mail address to request bank account details.

E-mail address: [support@mingham-smith.com](mailto:support@mingham-smith.com)

### 3) By Credit Card

We have arrangements with mycommerce.com who provide on-line credit card registration for LogLady.

To register online click on the link [Buy LogLady](#)

### Invoices

If your company requires an invoice before sending payment, please e-mail us at [support@mingham-smith.com](mailto:support@mingham-smith.com) or post your purchase order to the above address.

**Charges** for registering your use of LogLady are based on the number of computers on which it is installed and are detailed on the registration forms which customers are requested to complete. Prices are quoted in US dollars, Euros and £ Sterling. Customers outside the US or European Union are requested to convert the US dollar prices to the equivalent amount in their local currency.

Please note that **receipts** are normally sent via e-mail. If you require a receipt to be sent by post or a license to be issued, please request this when registering.

### 4) Our Company Details

HC Mingham-Smith Limited Registered in England No: 3676999.

Registered Office: TSB House, 39A Peach Street, Wokingham, Berks RG40 1XJ

VAT Registration Number: 642 4733 43

### LogLady Registration Form

**(For customers outside the European Union)**

UK VAT (Value Added Tax) does not apply to customers outside the European Union. The following prices are given in US\$. Non-US customers are invited to convert the following prices to their local currency.

**Quantity**

Please indicate the number of computers on which LogLady is installed and calculate the correct price

Computer(s) at \$75 each =

\_\_\_\_\_

**Corporate License**

Any number of copies for your whole company/organisation \$4000

Please provide the following information when registering:

Full Name/Name of company:

Your Address:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

E-Mail Address:

Windows Version:

LogLady version

Where did you hear about  
LogLady?

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Please send e-mail regarding LogLady to [support@mingham-smith.com](mailto:support@mingham-smith.com)

Visit the LogLady Home Page <http://www.mingham-smith.com>

**LogLady Registration Form****(For customers in the European Union, but not in the UK)**

Customers in the European Union who use the software for business purposes are responsible for paying VAT at the appropriate rate in their home country. Customers registering their own personal use should pay VAT at the UK rate of 20% to HC Mingham-Smith Limited. The following prices are in Euros and are exclusive of VAT. Prices may be converted to the customer's "home" currency if preferred.

**Quantity**

Please indicate the number of computers on which LogLady is installed and calculate the correct price

\_\_\_\_\_ Computer(s) at 75 € plus VAT each = \_\_\_\_\_

**Corporate License**

Any number of copies for your whole company/organisation 4000 € plus VAT

Please provide the following information when registering:

Full Name/Name of company:

Your Address:

E-Mail Address:

Windows Version:

LogLady version

Where did you hear about  
LogLady?

Please send e-mail regarding LogLady to [support@mingham-smith.com](mailto:support@mingham-smith.com)

Visit the LogLady Home Page <http://www.mingham-smith.com>

**LogLady Registration Form****(For UK customers)**

UK VAT (Value Added Tax) at 20% applies to sales to UK customers. The following prices are exclusive of VAT please add 20% to the final total.

**Quantity**

Please indicate the number of computers on which LogLady is installed and calculate the correct price

Computer(s) at £45 plus VAT each =

\_\_\_\_\_

**Corporate License**

Any number of copies for your whole company/organisation £2400 plus VAT

Please provide the following information when registering:

Full Name/Name of company:

Your Address:

E-Mail Address:

Windows Version:

LogLady version

Where did you hear about  
LogLady?

Please send e-mail regarding LogLady to [support@mingham-smith.com](mailto:support@mingham-smith.com)

Visit the LogLady Home Page <http://www.mingham-smith.com>