Kiwi’s Syslog Daemon Documentation

What is Kiwi’s Syslog Daemon?

Syslog Daemon receives standard UDP Syslog messages sent from routers, switches or Unix hosts and displays the details on screen. Optionally you can choose to log some or all of these messages to disk in any number of files.
Syslog Daemon allows you to forward some or all received messages on to other hosts that are also running a Syslog Daemon.

Kiwi’s Syslog Daemon features…

- GUI based (Runs under Win95/Win98/NT4)
- Visual – you can watch the messages on screen as they are received.
- Message forwarding. (All or selected by priority)
- Automatic Log file archiving. (Daily, weekly or monthly)
- Alarm notification (Audible or via SMTP E-Mail)
- Daily mailing of Syslog statistics
- Minimises to the System Tray to avoid task bar clutter.
- Maintains original senders address when forwarding messages
- Cool Statistics display
- Y2K (Year 2000) compliant.

Latest Information

This version of Kiwi’s Syslog Daemon is Ver 5.5.7

To obtain the latest release of Kiwi’s Syslog Daemon please check the web site…
http://members.tripod.com/~Andrew_Ross/software

Or E-Mail me at andrew-ross@usa.net and request to be added to the Syslog Daemon mailing list.

Reporting bugs

Please E-Mail me at andrew-ross@usa.net with the following information

- A description of the problem and what it effects.
- The severity of the problem in your terms. Ie is it just a minor bug or does it stop you using the product until the problem is solved.
- How to reproduce the problem if possible.
- Your return E-Mail address that I can send the corrected version to. (The file is likely to be about 500K)

Upgrading to the registered version

Please E-Mail me at andrew-ross@usa.net stating you would like information on purchasing the full registered version of “Kiwi’s Syslog Daemon” and I will reply with more details and pricing.

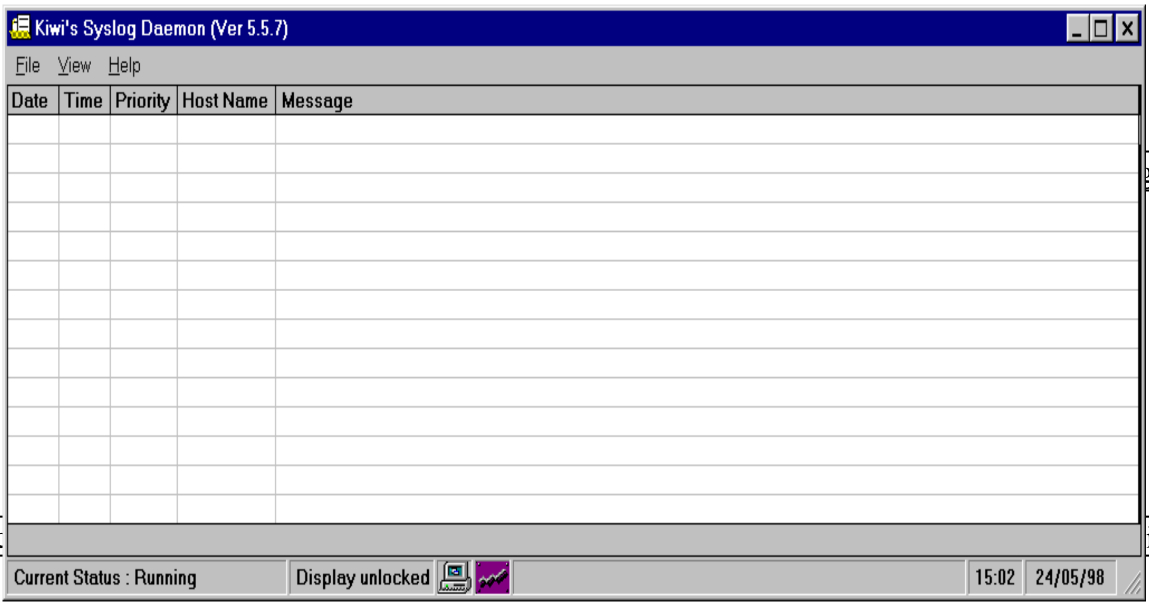
What’s in the registered version?

- Forwarding of all or selected messages via E-Mail depending on priority
- Message filters – choose which messages to log, display or forward depending on content of message, priority or hostname.
- Ability to run external program when alarm threshold exceeded.
- Configurable audible alarms – plays selected WAV file instead of using system beep

Guidelines on Initial setup of Syslog Daemon

When you run Syslog Daemon for the first time you will be asked if you want to initially log all messages to the file “All.Debug.TXT” this is so that you can be sure you aren’t missing any messages from the very start. Therefore it is recommended you choose Yes when prompted.

From the **Main Syslog Daemon display**…



Date	Time	Priority	Host Name	Message

Current Status : Running

Display unlocked

15:02 24/05/98

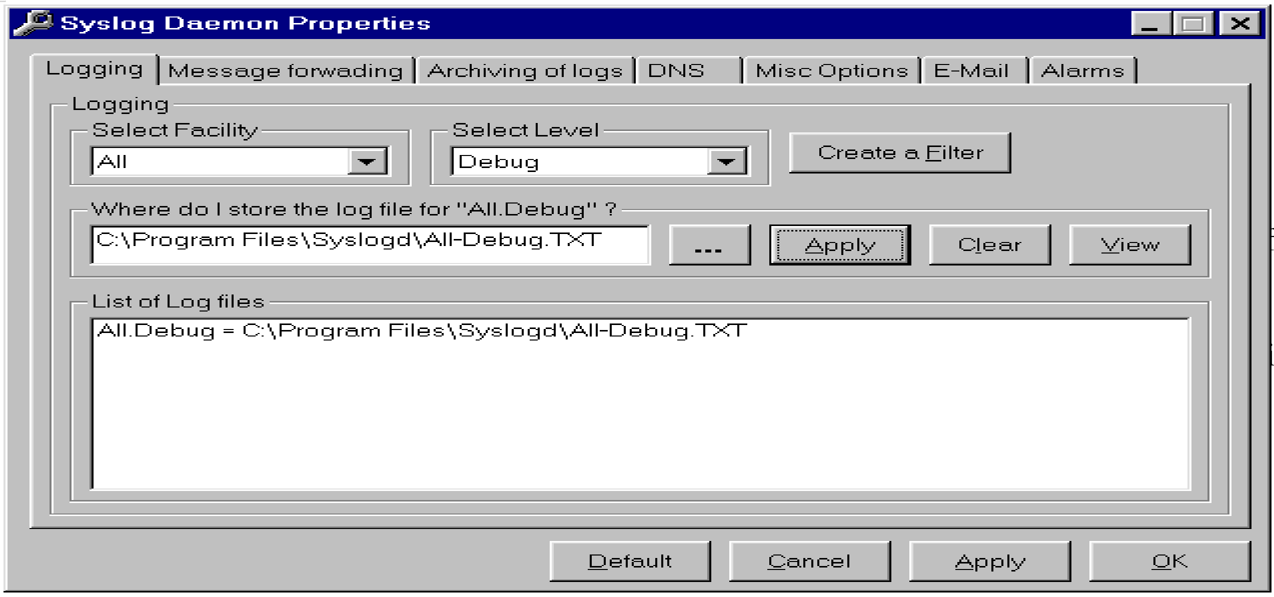
g. (Messages are still lo

Double Clic

istics.

Choose the File menu then Properties or press Ctrl+P.

This will bring up the **Syslog Daemon Properties** window…



Logging

Select Facility: All

Select Level: Debug

Where do I store the log file for "All.Debug" ?: C:\Program Files\Syslogd\All-Debug.TXT

List of Log files

All.Debug = C:\Program Files\Syslogd\All-Debug.TXT

for file button.

ing Apply.

The “Logging” tab is selected by default

If you chose ‘Yes’ when the program first started you will see an entry already added for “All.Debug” in the list.

Rules for logging

'Debug' is the lowest level, if you choose this level then you are logging every level from debug and above all the way up to the level 'Emerg'

If you want to only log the messages with the top five levels for example then choose the 'Warning' level. This means you will only log messages that are equal to or higher than the 'Warning' level. Ie. Warning, Error, Critical, Alert and Emergency.

Unless you have a shortage of disk space or are receiving too many messages it is OK to use the 'Debug' level, this way you wont miss any messages.

Choose the facility that you wish to log. This depends on what facilities you have configured the routers, switches or Unix boxes to send Syslog messages on.

Generally Unix hogs all the facilities except the local0 to local7 so If you are going to be using this Syslog Daemon in a mixed environment then setup your routers and switches to use a local number.
As an example you may set all your switches to 'Local7', your internal routers to log to 'Local6', your terminal servers to 'Local5' and your firewall routers to 'Local4' etc.
This means your Unix proxy server or firewall host can then log to the other facilities.

See also – Setting up Routers, Switches and Unix to send Syslog messages.

To setup logging for a facility and level…

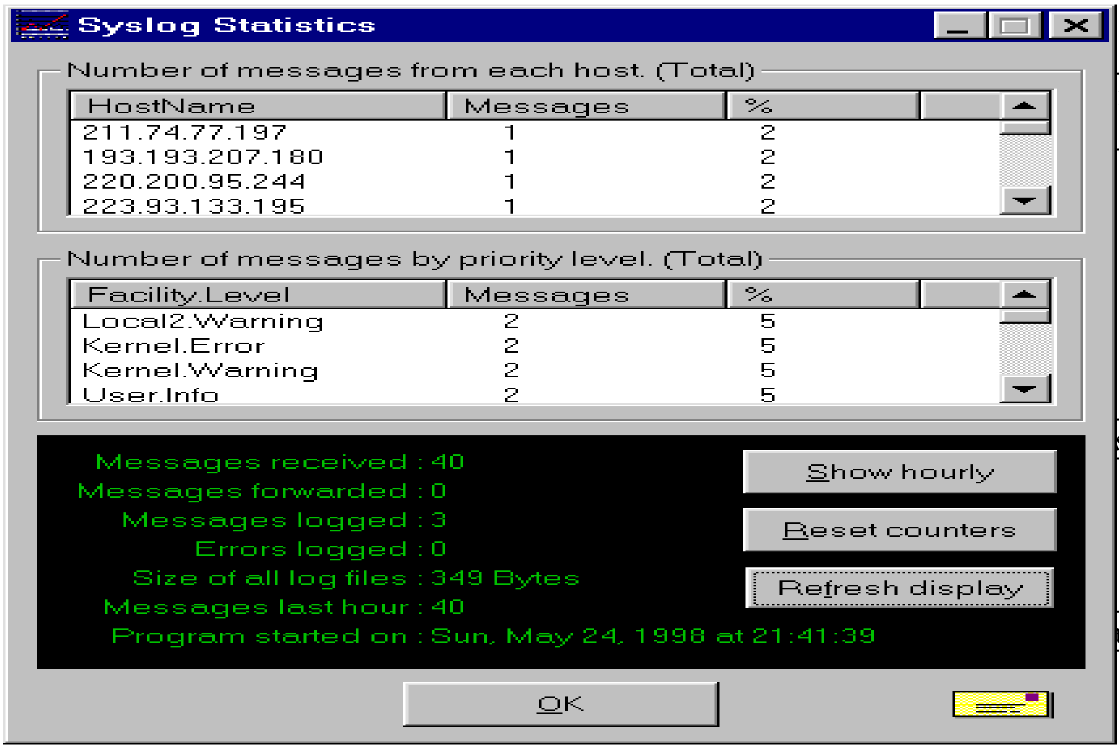
1. Select the Facility from the dropdown list.
2. Select the Level from the dropdown list.
3. Type in a path and file name for the log file or choose the "**…**" button to browse for a file.
4. Apply this path and file name by pressing the "Apply button" (next to the "**…**" button)
5. Check the new entry appears in the "list of log files" list.
6. Repeat from step 1 until you have set a log file for all the facilities you expect to receive messages on.

For most of the other Syslog property settings the defaults should be OK. However if you have a DNS you may want to enable DNS resolution as it is turned off by default.
To enable DNS options choose the 'DNS' tab and check the box marked 'Show Hostname instead of IP address (Resolve to Hostname)'

For details on setting each of the other property tabs check the details further on in the document.

Syslog statistics

From the Syslog Daemon main display, choose the View menu, then Statistics or press Ctrl-S
This will bring up the **Syslog Statistics** window…



Syslog Statistics

Number of messages from each host. (Total)

HostName	Messages	%
211.74.77.197	1	2
193.193.207.180	1	2
220.200.95.244	1	2
223.93.133.195	1	2

Number of messages by priority level. (Total)

Facility.Level	Messages	%
Local2.Warning	2	5
Kernel.Error	2	5
Kernel.Warning	2	5
User.Info	2	5

```
   Messages received : 40
  Messages forwarded : 0
     Messages logged : 3
       Errors logged : 0
Size of all log files : 349 Bytes
   Messages last hour : 40
  Program started on : Sun, May 24, 1998 at 21:41:39
```

reverse the sort order.

s.

ily statistics E-Mail list.

Exporting and importing settings to INI file

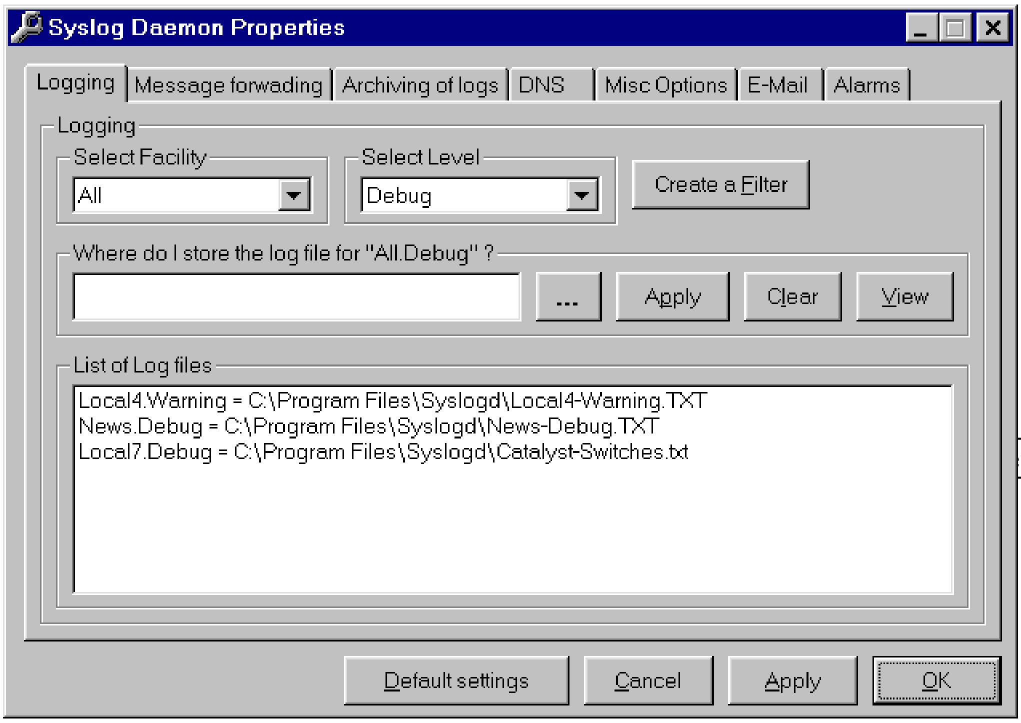
Once you have configured Syslog Daemon to your satisfaction you may want to backup the program settings to an INI file.
This is useful if you have to reinstall the operating system or you wish to use the settings on another machine.

To export the settings choose the File menu and then “Export Settings to INI or CFG file”
Or use the shortcut key Ctrl+E
Select a file name to export the settings to and press ‘Save’ or use the default file name “Syslog Daemon Settings.ini”

To Import the settings choose the File menu and then “Import Settings from INI or CFG file”
Or use the shortcut key Ctrl+I
Select a file name to import the settings from and press ‘Save’ or use the default file name “Syslog Daemon Settings.ini”
Details of the selected file will be displayed so you can confirm that this is the file you wish to import.
Once the settings are imported you may want to close and re-run Syslog Daemon to ensure all the new settings take effect.
Restarting is not really necessary but those who belong to the old school of computing may want to just to be sure.

Setting Syslog Properties

From the Syslog main display, choose the File menu then Properties or press Ctrl+P.
This will bring up the **Syslog Daemon Properties** window…



Select Facility: All

Select Level: Debug

Where do I store the log file for "All.Debug" ?

List of Log files

```
Local4.Warning = C:\Program Files\Syslogd\Local4-Warning.TXT
News.Debug = C:\Program Files\Syslogd\News-Debug.TXT
Local7.Debug = C:\Program Files\Syslogd\Catalyst-Switches.txt
```

faults.

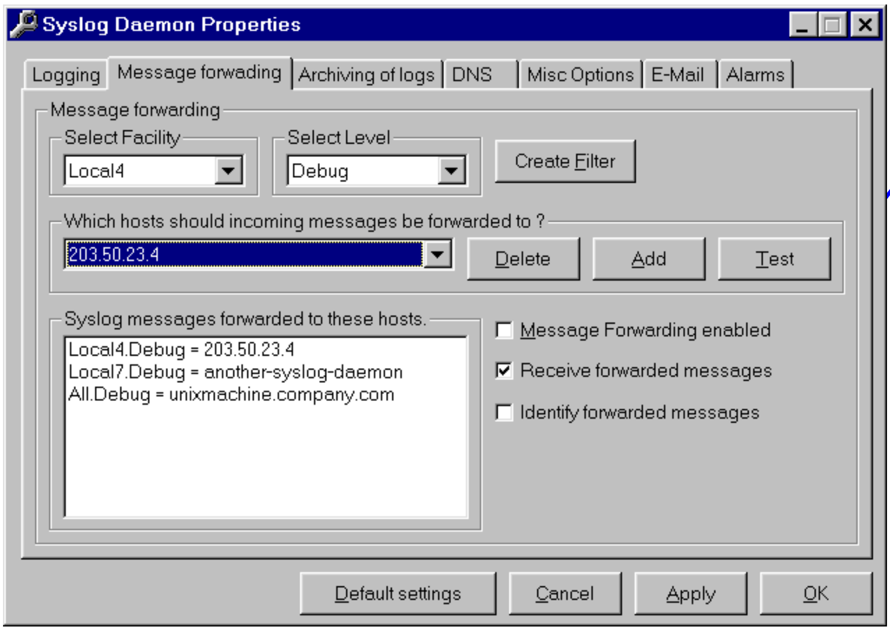
Logging Messages to disk

See guide to initial setup above first.

To setup logging for a facility and level…

1. Select the Facility from the dropdown list.
2. Select the Level from the dropdown list.
3. Type in a path and file name for the log file or choose the "**…**" button to browse for a file.
4. Apply this path and file name by pressing the "Apply button" (next to the "**…**" button)
5. Check the new entry appears in the "list of log files" list.
6. Repeat from step 1 until you have set a log file for all the facilities you expect to receive messages on.

Forwarding Messages to another Syslog Daemon



Message forwarding

Select Facility: Local4

Select Level: Debug

Which hosts should incoming messages be forwarded to ? 203.50.23.4

Syslog messages forwarded to these hosts.

```
Local4.Debug = 203.50.23.4
Local7.Debug = another-syslog-daemon
All.Debug = unixmachine.company.com
```

☐ Message Forwarding enabled

☑ Receive forwarded messages

☐ Identify forwarded messages

Globally enables or disables message forwarding.

Removes the "original address=" line from received Forwarded messages and uses the address to indicate the original sender not the address of the forwarding Syslog Daemon.

level…

1. …e
2.
3.
4. appears in the list of Syslog messages to be forwarded
5. Repeat from step 1 until you have set a host for all the facilities you want to forward messages on.

Note: you can forward messages to more than one host per facility and level, just keep adding hosts.

To test message forwarding for a facility and level…

Select a line from the list containing the Syslog messages to be forwarded.
Press the Test button.
A message will be sent to all the hosts that have been set for that facility and level.
The message reads "This is a test message generated by Kiwi's Syslog Daemon".

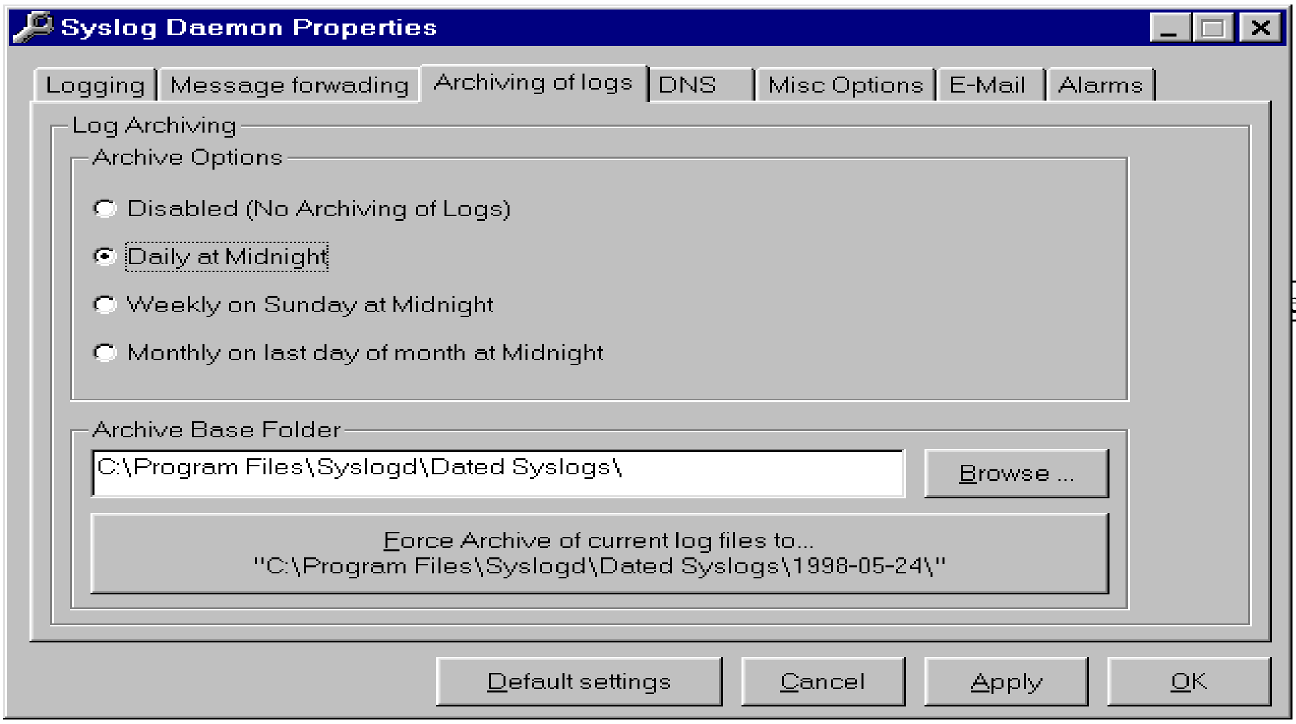
To remove a host from the message forwarding list…

Select a line from the list containing the Syslog messages to be forwarded.
Or select the facility and level from the dropdown lists.
Select the host (if there is more than one set for this facility and level) from the list containing the hostnames.
Press the Delete button, you will be prompted to confirm you want to delete this host.

How message forwarding works…

When a message is forwarded from Kiwi's Syslog Daemon the original address of the sending host is added into the message with the words "original address=aaa.bbb.ccc.ddd".
This allows a message to traverse many Syslog Daemons and still show the original address of the sending device.
If the "Receive forwarded messages" box is checked then if the message contains the line "original address=" the IP address following it will be used as the original sending device and the extra text ("original address=") will be striped from the message.

Automatic Archiving of log files



Log Archiving

Archive Options

○ Disabled (No Archiving of Logs)

● Daily at Midnight

○ Weekly on Sunday at Midnight

○ Monthly on last day of month at Midnight

Archive Base Folder: C:\Program Files\Syslogd\Dated Syslogs\

Force Archive of current log files to...
"C:\Program Files\Syslogd\Dated Syslogs\1998-05-24\"

ed on the se

How the log file archiving works…

If the log archiving is disabled (top option) then no archiving is done and the log files as specified under the “logging” tab will continue to grow in size as messages are received.

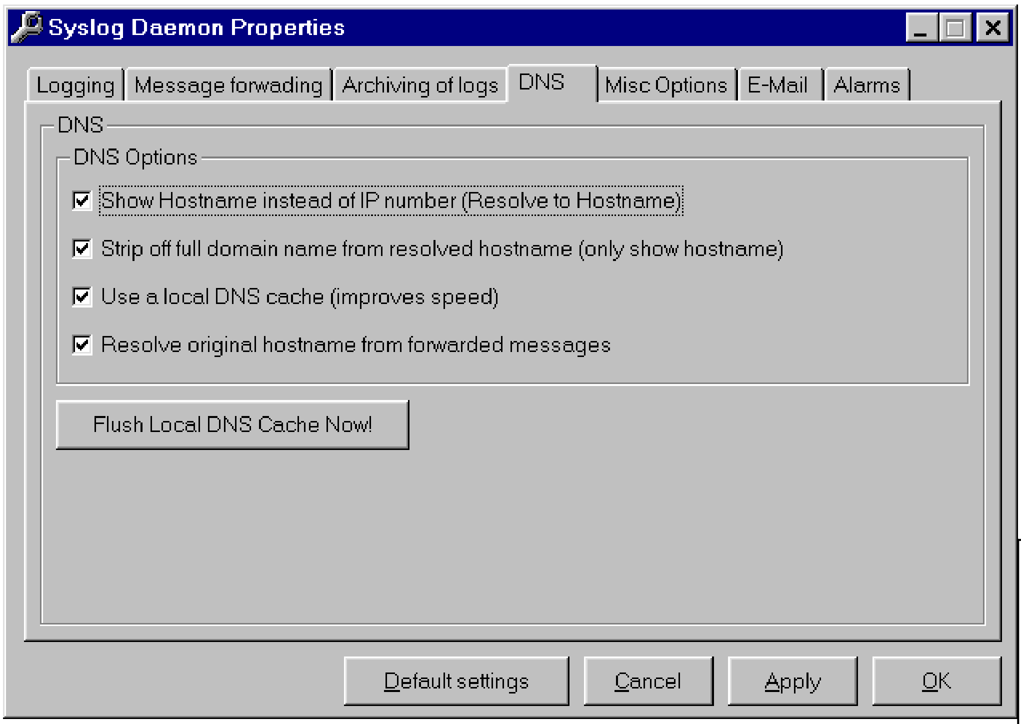
If an archiving option has been chosen (daily, weekly or monthly) then at that time all the individual log files for each facility and level are moved into a new dated archive folder.

The folder that is created is the “Archive Base Folder” plus the current date.
Ie “C:\Pogram Files\Syslogd\Dated Syslogs\1999-02-03\”

This has been checked to work for the year 2000 and beyond.

All the individual log files are moved into this one new folder, therefore make sure you use unique file names if your individual logging files are stored in different folders to each other.

Setting the DNS Options



☑ Show Hostname instead of IP number (Resolve to Hostname)

☑ Strip off full domain name from resolved hostname (only show hostname)

☑ Use a local DNS cache (improves speed)

☑ Resolve original hostname from forwarded messages

Show Hostname instead of IP number

This converts the IP address of the sending device into a more meaningful hostname.
Instead of 203.50.23.4 you will see something like "sales-router.company.com"

If hosts on your network have changed you may want to clear the local DNS cache so Syslog Daemon can relearn the new addresses and hostnames.

Strip off full domain name from resolved hostname

If the "Show hostname instead of IP number" option is checked then this will remove the trailing domain name from the resolved hostname.
Instead of "sales-router.company.com" you will see "sales-router"

Use a local DNS cache

Every time an IP address to hostname resolution is needed the DNS server is queried. This can be an extra overhead on Syslog Daemon and the DNS server, especially if you get lots of messages.
To avoid this extra traffic it is better to enable the local DNS cache so that when hostname has been resolved once the result is stored locally. Next time that address needs to be resolved the result is taken from the cache instead of making another DNS request.

Resolve original hostname from forwarded messages.

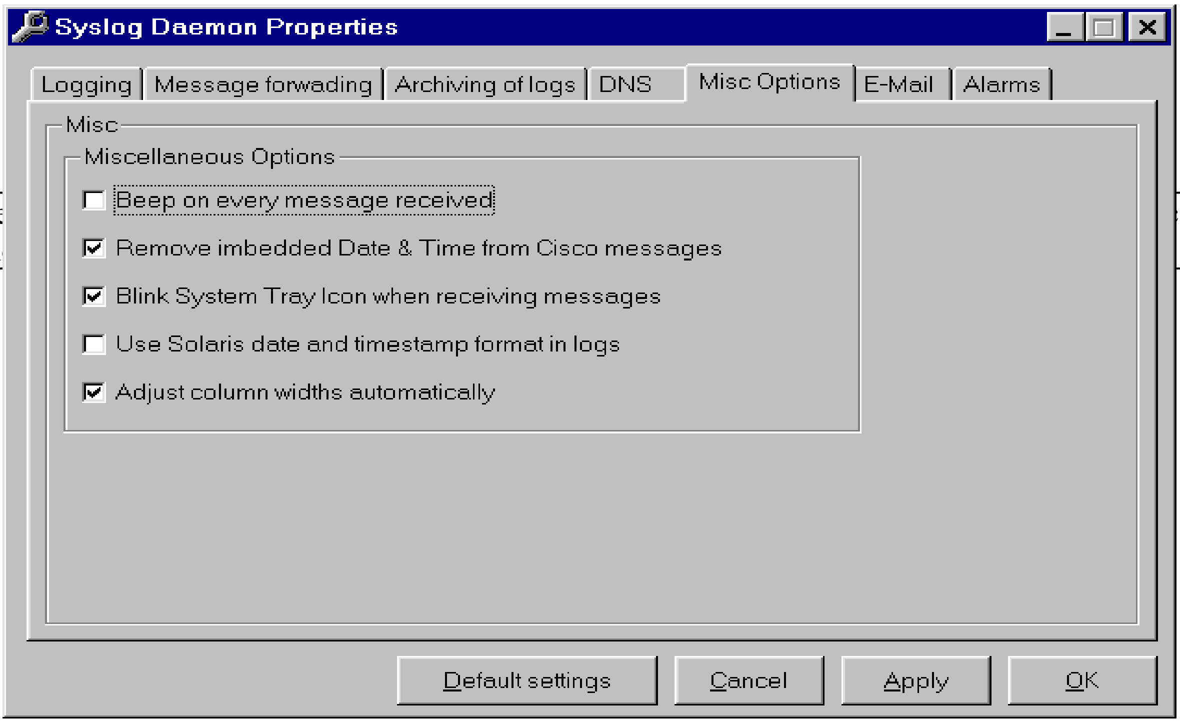
When a forwarded message is received the original IP address is taken from the "original address=" text in the message.

Enabling this option converts the IP address of the original device into a more meaningful hostname.
Instead of 203.50.23.4 you will see something like "sales-router.company.com"

This may have a speed impact if your DNS is unable to resolve these IP addresses.
Ie. If the original sending device is so remote that it is not linked to your local DNS.

Misc Options

Message ally stamps the incor
Time an



☐ Beep on every message received

☑ Remove imbedded Date & Time from Cisco messages

☑ Blink System Tray Icon when receiving messages

☐ Use Solaris date and timestamp format in logs

☑ Adjust column widths automatically

Use Solaris date and timestamp format in logs

Check this box if you want to use the Solaris UNIX style date format in the log files.
The Syslog format is…
“Sep 7 18:00:03 203.50.23.4 Message text here”

Kiwi’s Syslog Daemon logging format is…
“05-24-1998 TAB 21:43:22 TAB News.Emerg TAB sales-router TAB Message text here”

You will find that the Solaris logging format is lacking a lot of info but you may want to enable it if other parsing programs are looking for that particular format.

Kiwi’s format has the following TAB delimited fields

- Month-Day-Year
- HH:MM:SS
- Facility dot Level
- IP address or hostname, with or without domain name depending on DNS options set.
- Message text

TAB delimited fields allow easy parsing with spreadsheets or database applications.

E-Mail Setup

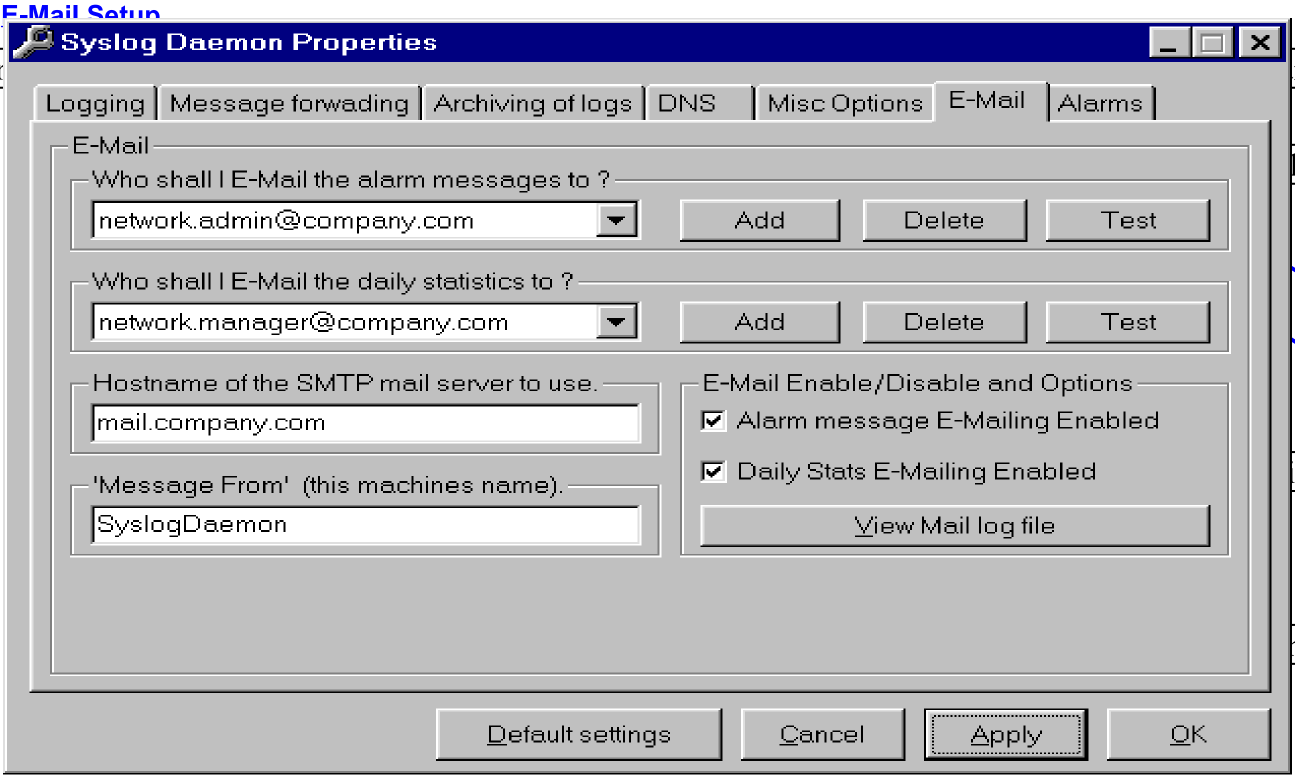
E-Mail addr

in for the sp

l message to

ing of E-Ma

n your recei



Who shall I E-Mail the alarm messages to ? network.admin@company.com

Who shall I E-Mail the daily statistics to ? network.manager@company.com

Hostname of the SMTP mail server to use. mail.company.com

'Message From' (this machines name). SyslogDaemon

E-Mail Enable/Disable and Options

☑ Alarm message E-Mailing Enabled

☑ Daily Stats E-Mailing Enabled

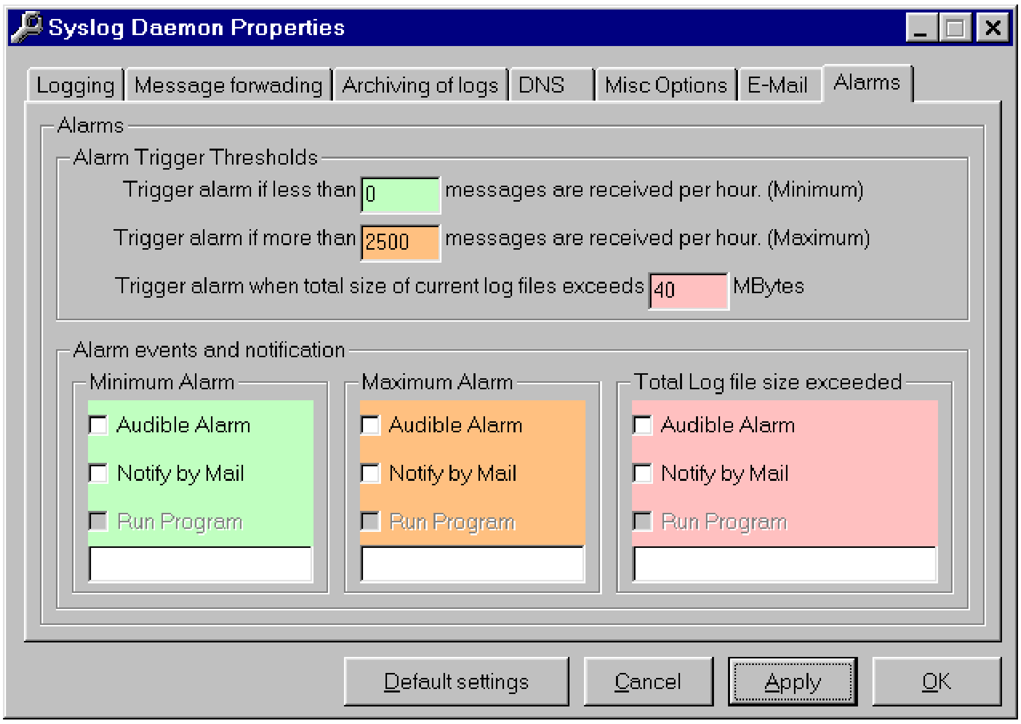
Alarm messages…

Alarm messages will be E-Mailed out when the Alarm thresholds have been exceeded

Daily Statistics…

A daily statistics message is mailed out every midnight and contains information on log file size, disk space remaining on the archive drive, number of total messages and a breakdown of where the messages came from and on what facility and level.

Setting the Alarm thresholds



Alarms

Alarm Trigger Thresholds

Trigger alarm if less than 0 messages are received per hour. (Minimum)

Trigger alarm if more than 2500 messages are received per hour. (Maximum)

Trigger alarm when total size of current log files exceeds 40 MBytes

Alarm events and notification

Minimum Alarm	Maximum Alarm	Total Log file size exceeded
□ Audible Alarm	□ Audible Alarm	□ Audible Alarm
□ Notify by Mail	□ Notify by Mail	□ Notify by Mail
□ Run Program	□ Run Program	□ Run Program

Notify by Mail…

If a Min or Max threshold is exceeded a mail message is send to all the recipients in the “Alarm notification” list. The message states the alarm message, the threshold exceeded, the threshold value etc.

Audible Alarm

If a Min or Max threshold is exceeded Syslog will beep once a second until the alarm is cancelled by pressing the “Cancel Alarm” button that appears in the middle of the main Syslog Daemon display.

Run Program

Runs an external program of your choice if a Min or Max threshold is exceeded.
Note. This feature is only available in the registered version.

Configuring a Cisco Router to send Syslog messages

Enter the following commands from the enable prompt on the router.

```
Config term

Logging on

Logging Facility Local6 (or any other facility you want to allocate for this router.)

Logging [IP Address or Hostname of machine running Kiwi’s Syslog Daemon]

End
```

Configuring a Catalyst 2900 series or 5000 series Switch to send Syslog messages

Enter the following commands from the enable prompt on the switch

```
Set logging enable

Set logging level all 7 default (this will set all facilities with a level of debug)

Set logging [IP Address or Hostname of machine running Kiwi’s Syslog Daemon]
```

Configuring a Unix box to send Syslog messages

Enter the following commands from a privileged account. Ie root or a su/sudo account.

```
cd /etc

vi syslog.conf
```

Then modify the file with vi to forward the various facilities and levels to the IP address or hostname of the machine running Kiwi’s Syslog Daemon.

If in doubt resort to ‘man syslogd’

Error and Sendmail logs

If Syslog is unable to write a message to a log file or has a problem archiving the log files an error will be logged in the file “Errorlog.txt” in the directory that Syslogd is installed. (Usually C:\Program Files\Syslogd”)

To view the error log file…

From the Main Syslog Daemon display…
Choose the View menu then Error log file or press Ctrl+R.
This will open the errorlog.txt file with notepad if there have been errors logged.

Every time an alarm notification is mailed out or the daily statistics are sent the E-Mail details are logged in a file called “SendMaillog.txt” in the directory that Syslogd is installed. (Usually C:\Program Files\Syslogd”)

To view the Sendmail log file…

From the Main Syslog Daemon display…
Choose the View menu then Send mail log file or press Ctrl+M.
This will open the errorlog.txt file with notepad if there has been any mail activity logged.