Enabling Syslog on TimeStep's Permit/Gate

One of the features of PERMIT/Gate you might wish to explore is the option to connect to a syslog server in order to capture all logging entries for subsequent evaluation.

The internal logs on PERMIT/Gate have limited capacity. In order to be able to preserve all logging information, the Gates are able to connect to a syslog server.

I am using Kiwi's Syslog daemon Version 6.2.9, which is a GUI based (runs on Windows 95, 98, ME, 2000 & NT) Logging Tool with a couple of great features, which I couldn't resist to list here.

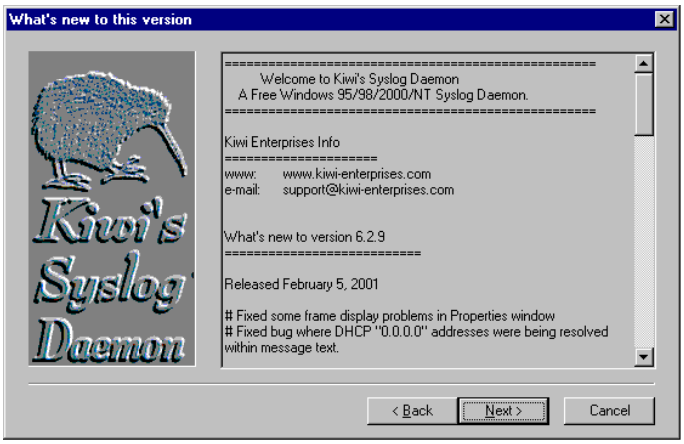
- Visual – you can watch the messages on screen as they are received
- NT and Windows 2000 Service edition available
- Message forwarding. (All or selected by priority)
- Automatic log file archiving (daily, weekly or monthly)
- Alarm notification (audible or via SMTP e-mail)
- Daily e-mailing of syslog statistics
- Up to 50 rows of scrolling display
- Minimizes to the System Tray to avoid task bar clutter.
- Maintains the original sender address when forwarding messages
- PIX Firewall support via TCP
- LinkSys home firewall support via SNMP
- Selectable Syslog listen port
- Cool Statistics display
- Selectable display wallpaper
- **Free to use for as long as you want**

You can download it from http://www.kiwi-enterprises.com/info_syslogd.htm

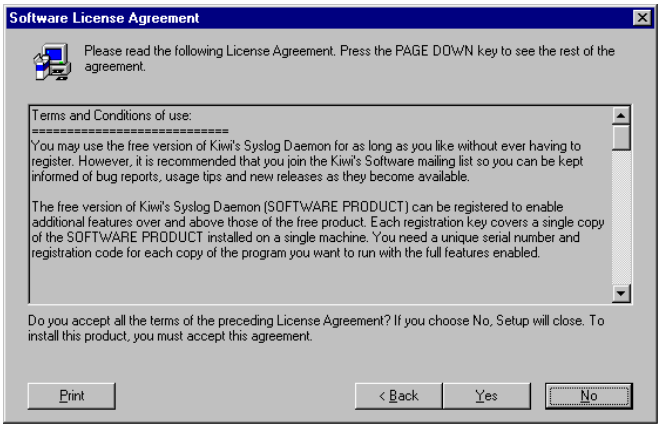
To install, execute kiwis_syslogd.exe

Welcome screen appears – Click **NEXT**

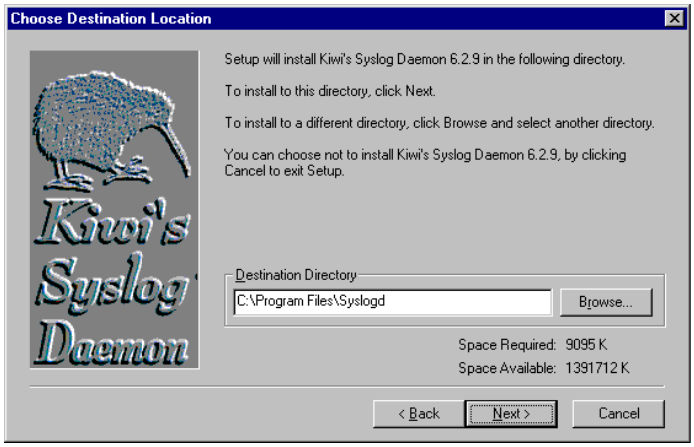
Information Screen on “What’s new to this version” - Click **NEXT**



Scan the License Agreement and accept the agreement by clicking **YES** in order to continue with the installation

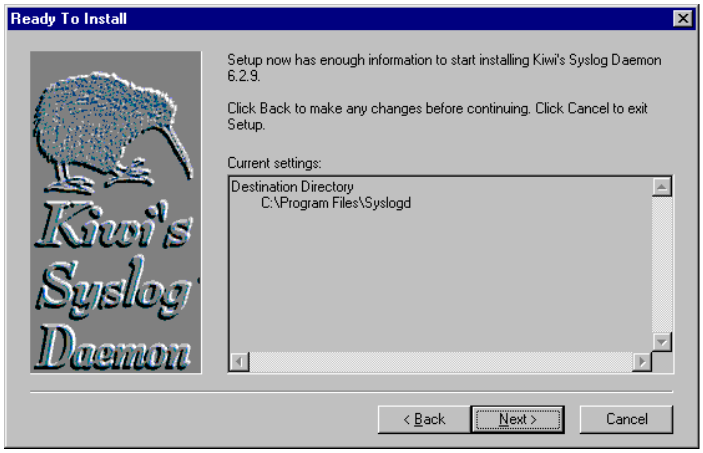


Accept the default Destination Directory and click **NEXT**

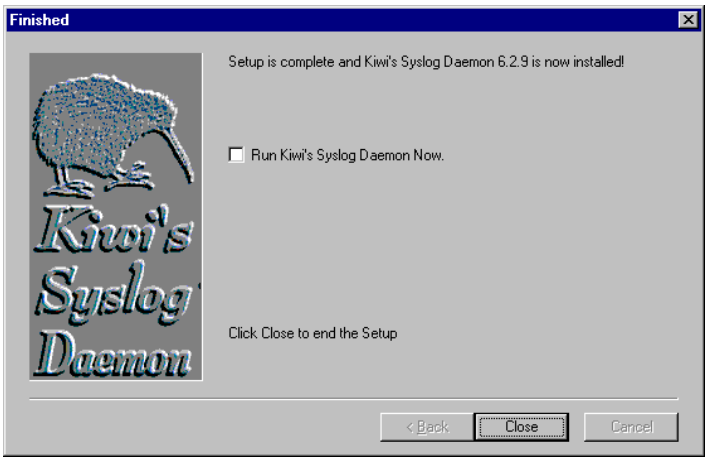


This technical document has been created and evaluated by myself with the purpose to help friends to get into new technology and installations. There is no financial interest, however, please respect the copyright.

You'll get an information windows that Kiwi's Syslog Daemon is ***Ready to Install***. Click on **NEXT**
(A progress bar appears)

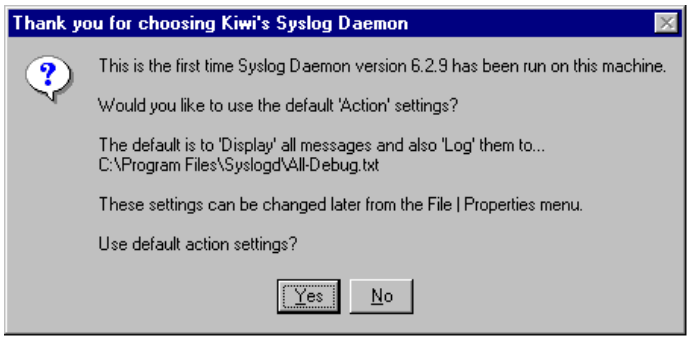


Once all files has been installed, you should get a Finished window. **Do not *Run Kiwi's Syslog Daemon Now***. Do a reboot of your PC first.

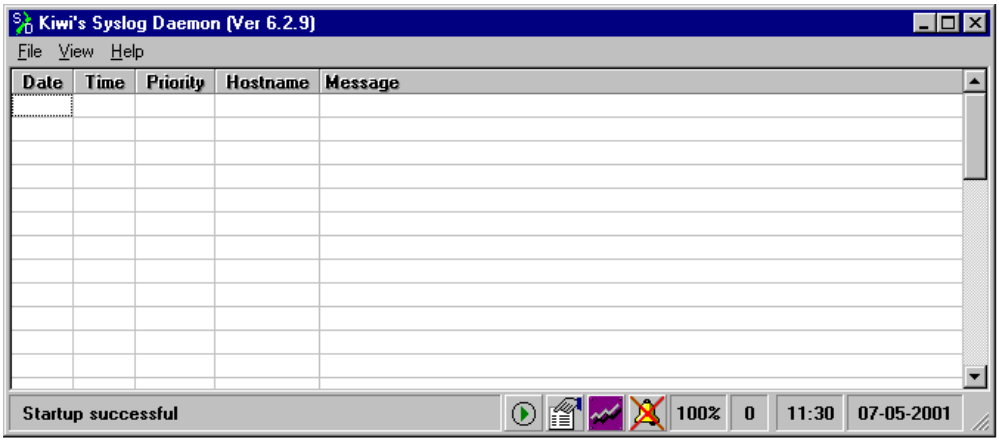


When the PC has been restarted you could run Kiwi's Syslog Daemon by Start ⇨ Programs ⇨Kiwi's Syslog Daemon ⇨ Kiwi's Syslog Daemon

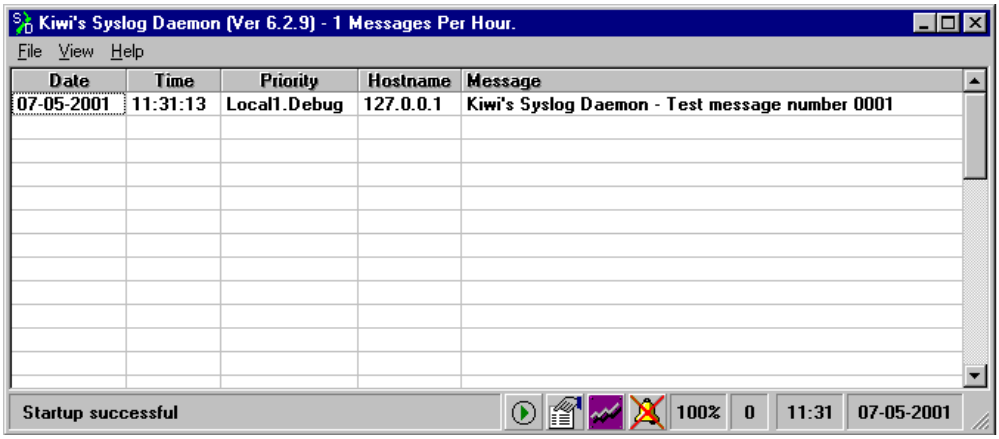
As this is the first time Syslog Daemon ir running on this PC, you will be asked to choose Default Action setting. Click on **YES**



Now you are ready to receive syslog messages. But to be sure if this service is really running you should do one more thing.



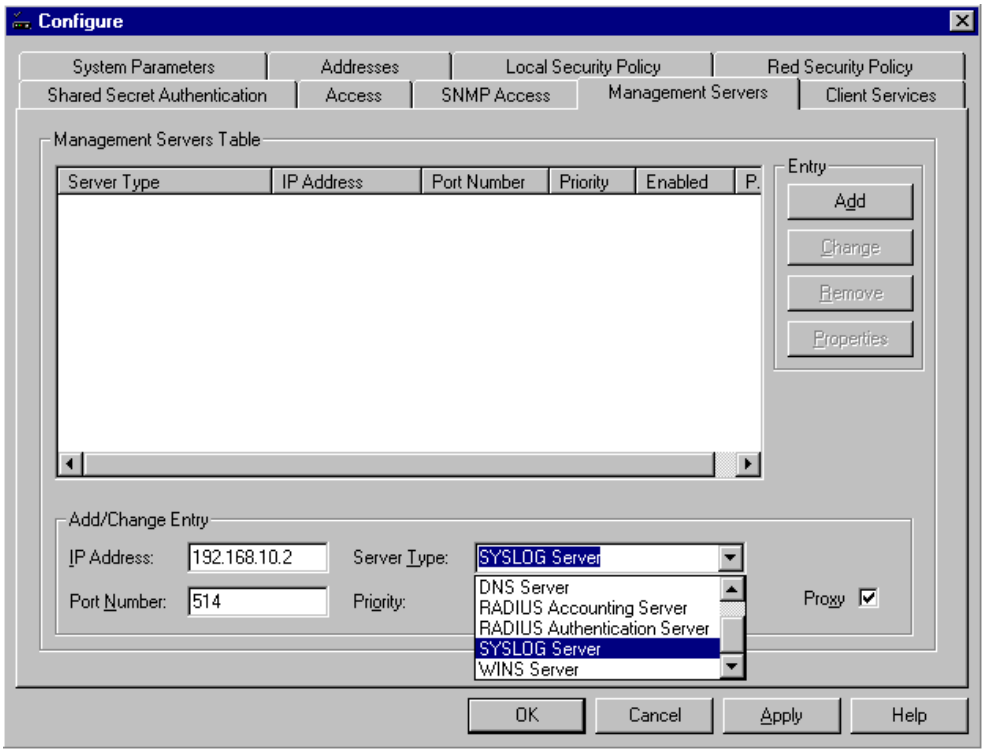
Test the server with **CTRL+T**
You should see an entry in the log



Finally, we need to configure the VPN Gateway to send messages to the Syslog services.

Use PERMIT/Config to connect to the Gate and open the Configuration Window

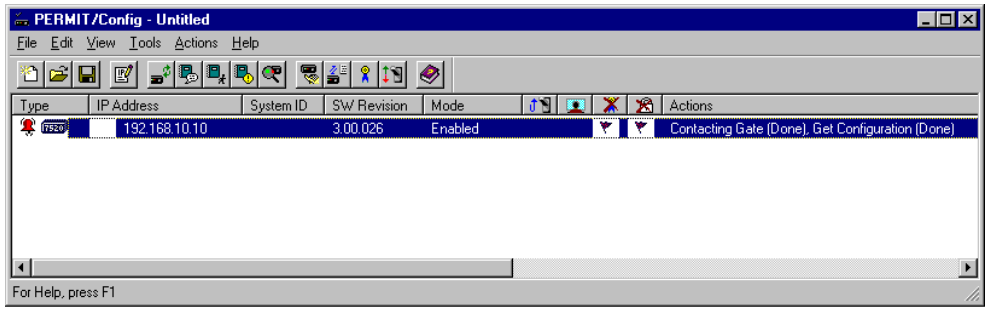
Click the ***Management Servers*** tab



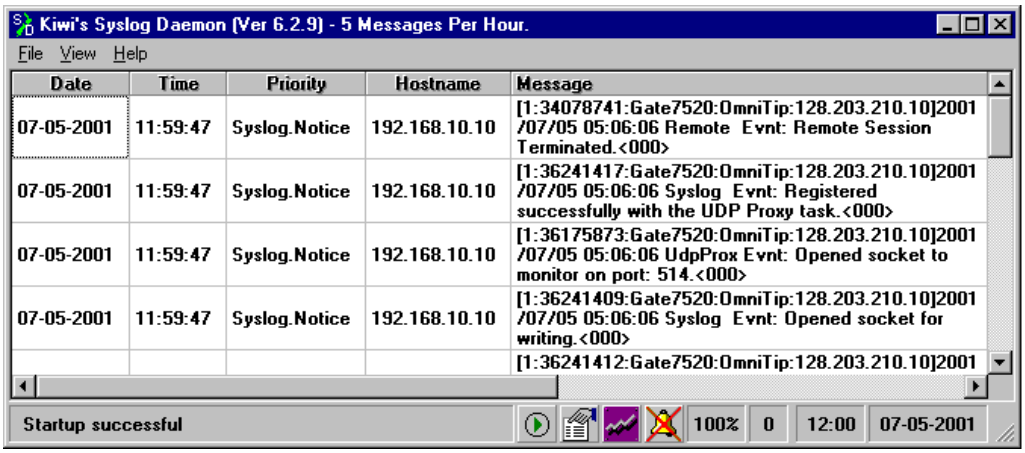
Type the **IP Address** of the desired server in the IP Address.

Select ***Syslog Server*** from the Server Type list box

Click **Add**
Click **OK**
Refresh the status of the main display



Observe the entries in the Syslog server



Establish a VPN Security Association (out of Kiwi's Syslog)

07-05-2001 12:06:14 Syslog.Notice 192.168.10.10 [1:33947680:Gate7520:OmniTip:128.203.210.10]2001/07/05 05:12:35 Isakmp ScSA: AddSa: SPIs:45401EEC/73F3F1DA Loc:192.168.10.* Rem:192.168.10.200 (128.203.210.2) Prot:ESP-DES[56] Exp:5:00:00<000>
07-05-2001 12:06:14 Syslog.Notice 192.168.10.10 [1:35913740:Gate7520:OmniTip:128.203.210.10]2001/07/05 05:12:34 Par Evnt: Request for IP address 192.168.10.200 from 128.203.210.2<000>
07-05-2001 12:06:13 Syslog.Notice 192.168.10.10 [1:33947685:Gate7520:OmniTip:128.203.210.10]2001/07/05 05:12:34 Isakmp ScSA: Notify from 128.203.210.2: Initial Contact<000>
07-05-2001 12:06:13 Syslog.Notice 192.168.10.10 [1:33947703:Gate7520:OmniTip:128.203.210.10]2001/07/05 05:12:34 Isakmp ScSA: AddPhase1: Rem:128.203.210.2, ID:"128.203.210.2", Cookies: 5DD64DE34C41FB35/2929B5220B677F39 Prot:DES[56]-MD5, Exp:23:59:49<000>
07-05-2001 12:06:02 Syslog.Notice 192.168.10.10 [1:34930700:Gate7520:OmniTip:128.203.210.10]2001/07/05 05:12:23 ShSecrt ScSA: Found PW for: 128.203.210.2.<000>
07-05-2001 12:06:02 Syslog.Notice 192.168.10.10 [1:33947698:Gate7520:OmniTip:128.203.210.10]2001/07/05 05:12:23 Isakmp ScSA: Got policy for peer:128.203.210.2, I am responder, authentication: shared<000>

Release of VPN Security Association (out of Kiwi's Syslog)

07-05-2001 12:09:56 Syslog.Notice 192.168.10.10 [1:35979273:Gate7520:OmniTip:128.203.210.10]2001/07/05 05:16:17 ParPool Evnt: Releasing IP Address 192.168.10.200.<000>
07-05-2001 12:09:56 Syslog.Notice 192.168.10.10 [1:33947704:Gate7520:OmniTip:128.203.210.10]2001/07/05 05:16:17 Isakmp ScSA: DelPhase1: Rem:128.203.210.2, ID:"128.203.210.2", Cookies: 5DD64DE34C41FB35/2929B5220B677F39, peer initated delete<000>
07-05-2001 12:09:56 Syslog.Notice 192.168.10.10 [1:33947705:Gate7520:OmniTip:128.203.210.10]2001/07/05 05:16:17 Isakmp ScSA: Rekey Phase 1: Rem:128.203.210.2, ID:"128.203.210.2", Cookies:5DD64DE34C41FB35/2929B5220B677F39<000>
07-05-2001 12:09:56 Syslog.Notice 192.168.10.10 [1:33947698:Gate7520:OmniTip:128.203.210.10]2001/07/05 05:16:17 Isakmp ScSA: Got policy for peer:128.203.210.2, I am initiator, authentication: shared<000>