NotificationWorks™ User Guide

Providing Advance Notification Control for:

- HP's Openview Network Node Manager
- Cisco's CiscoWorks DFM
- CastleRock's SNMPc
- IP Switch's What's Up Gold
- Network Observer by Network Instruments
- Novell's ManageWise and ZENWorks
- and many others…

BEFORE YOU USE THIS PRODUCT, please read the Software License Agreement below. It tells you that this software is protected under U.S. copyright law: You may copy it only to make a backup copy. If more than one person needs to use this program, you must purchase a separate product for each user. This includes users on a network.
Be sure to fill out and send in the attached registration card. This establishes your warranty start date and lets us inform you of program upgrades.

90-DAY DISK WARRANTY: To the original purchaser only, Atlantis Software, warrants the magnetic disk on which the software is recorded to be free from defects in materials and faulty workmanship for a period of 90 days from the date the software is delivered. If a defect in the disk should occur during this period, you may return the disk to Atlantis Software for replacement at a nominal charge.

LIMITED WARRANTY AND LIMITATION OF REMEDIES: This program is provided “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The original purchaser assumes the entire risk as to the quality and performance of the program. This warranty gives you specific legal rights, and you may have other rights.
Your sole and exclusive remedy in the event of a defect is expressly limited to replacement of the disk as provided above. In no event shall Atlantis Software be liable for any direct, incidental, or consequential damages, such as, but not limited to, loss of anticipated profits, benefits, use, or data resulting from the use of the software, or arising out of any breach of any warranty.
Some states and countries do not allow the exclusion of implied warranties, or the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusions may not apply to you.
DISCLAIMER: The software and accompanying written materials (including instructions for use and this document) are provided “as is” without warranty of any kind. Atlantis Software, does not warrant, guarantee, or make any representations regarding the use, or the results of the use, of the software or written materials in terms of correctness, accuracy, reliability, correctness, or otherwise.

You assume the entire risk as to the results and performance of the software. If the software or written material is defective, you and not Atlantis Software, or its dealers, distributors, agents, or employees, assume the entire cost of all necessary servicing, repair, or correction. Atlantis Software, nor anyone else involved in the creations, production, or delivery of this product shall be liable for any direct, indirect, consequential, nor incidental damages (including damages for loss of business profits, business interruption, loss of business information, and the like) arising out of the use of or inability to use this products even if Atlantis Software, has been advised of the possibility of such damages.

TRADEMARKS and COPYRIGHTS:

1 Introduction

Thank you for choosing NotificationWorks from Atlantis Software. To get right to it, skip to the **Quickstart** section.

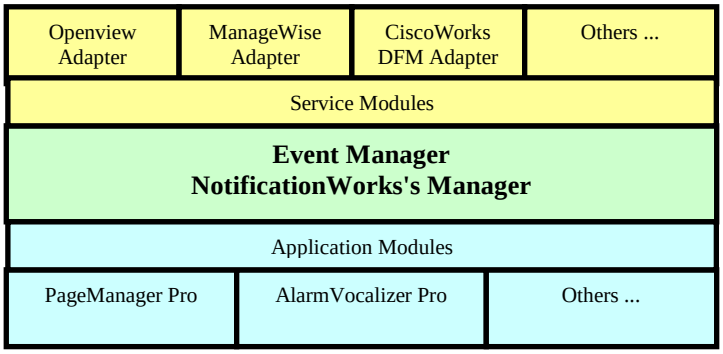
NotificationWorks is a collection of modules providing network management notification solutions that can be added to an existing network management environment or used as a stand-alone solution. The collection of modules can perform network monitoring, notification via pager/e-mail, response escalations, and reporting with astounding flexibility and detailed control. Using this modular solution provides users with the ability to build a custom network management solution that exactly fits their needs – nothing more, nothing less. Feel free to submit feature requests to asinfo@atlantissoftware.com

Operation

Event Manager is the main module manager that connects all the modules. It is included with NotificationWorks. There are two types of modules: Application modules and Service modules. Service modules are modules that connect to diverse environments and forward received events to Event Manager.

Note: Events, alarms, traps and messages are referred to as events in this manual

Event Manager forwards these events to the installed Application modules, e.g. PageManager Pro. Application modules process and perform an action based on the type of module. There are many Service and Application modules with many different functions.



Available Service Modules

- **Node Monitor –** If no device monitoring tool is already present, this provides a low-cost way to monitor the status of IP devices and ports/sockets. Set thresholds that trigger alarms for network latency, amount of time down/no responses, web pages, etc.
- **CiscoWorks DFM Adapter** – Processes SNMP events from CiscoWorks DMF and breaks them into over 50 specific events. The adapter can connect remotely.
- **HP Openview Network Node Manager Adapter** – Connects to the NNM console and processes all NNM events. The NNM console can be used on ANY Openview supported OS. The adapter can connect remotely.
- **CastleRock SNMPc Adapter –** Connects to the SNMPc management console and processes all events. The adapter can connect remotely.
- **AlarmGen Pro –** Consists of two parts: AlarmGen Pro Listener and the AlarmGen Remote. Install the AlarmGen Listener into Event Manager and copy the AlarmGen Remote called agremote.exe to ANY Windows based system. AlarmGen Remote can now be called from any local or remote application that supports the ability to run third-party applications. This provides the ability to create custom event messages and send them into the NotificationWorks system.
- **SNMPListener** – Listens for and processes all SNMP traps sent to the PC running NotificationWorks and SNMPListener. Comes with its own MIB compiler that supports MIB syntax v1 and v2. Can also customize event messages through a nice interface, eliminating the need to know MIB writing.
- **Novell ManageWise Adapter** - Hooks seamlessly into Novell's ManageWise console and forwards all events into NotificationWorks, providing a 16 to 32-bit connection bridge.

Available Application Modules

- **PageManager Pro –** Sends events to cell phones, pagers, web pages, and email. Supports escalation. The transport of the events can use SNPP, SMTP, HTTP web posting, and modem communication using TAP/UCP or ASCII Terminals. Can also be set to trigger applications. Each event can have its own assignments, filters and schedules.
- **Alarm Vocalizer Pro –** Each event can be vocalized using the built-in text-to-speech engine. Each event can be assigned to be vocalized, play a sound file, or be silent.

2 Installation

Preparing for Installation

This user guide requires knowledge of

- Microsoft Windows

System requirements are

- 32-bit Windows
- 800 x 600 minimum desktop size

Performing the Installation

Installing NotificationWorks™

Run the installation program. After answering the usual installation questions, two installation options are shown:

1. Wizard Installer
2. Expert Installer

Choose the Wizard installer for a guided NotificationWorks module installation. Choose Expert to manually select the modules to install.

After installing the desired NotificationWorks modules the installer presents the option to install licenses. Cick “Yes” ONLY if you have purchased licenses. Otherwise, select “No.”

Verify that all third party applications NotificationWorks will connect to are running, then launch NotificationWorks.

Note: Many additional installation tips can be found in the support forum on the Atlantis Software web site at http://www.AtlantisSoftware.com.

3
Configuring NotificationWorks

EventManager

All NotificationWorks modules are controlled through EventManager:

EventManager launches all NotificationWorks modules with the “Startup” setting set to “Auto” (default). All modules can be started and stopped from this screen (except Node Monitor) by double-clicking on the “Status” entry. Double-clicking one the module names shows or hides the module’s screen.

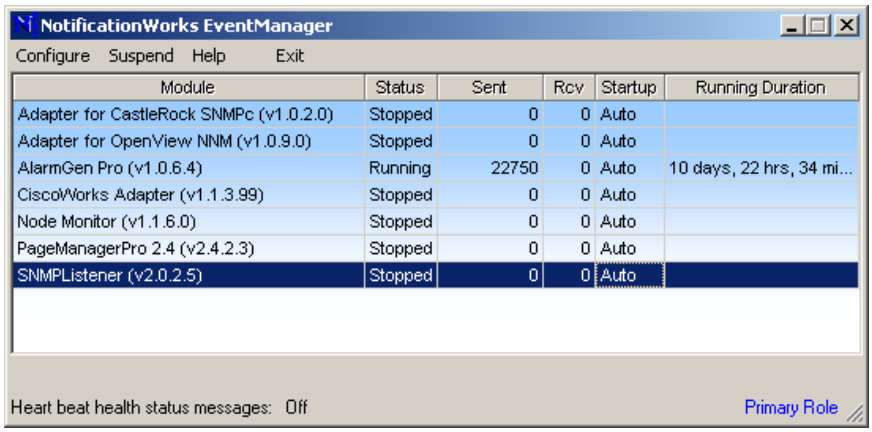


Figure 3.1: Event Manager

Reading in the Alarms/Events

The events need to be added into either PageManager Pro (PMPro) or AlarmVocalizer Pro (AVPro). Verify that all required third party applications are running and that any modules connecting to them show as “Connected” in the module’s screen. If using PMPro, click PMPro’s “Settings” tab, then click “Add new Alarms to DB”. This reads all of the available events into PMPro. If using AVPro, perform the same steps for it.

Please refer to the specific module sections in this documentation for further details.

Running NotificationWorks as a Service

To run NotificationWorks as a service: Click the Windows Start button and navigate to Programs >NotificationWorks > Register as NT-2000 Service

If running as a service, NEVER run a second instance of NotificationWorks from the desktop. This will lead to database corruption. Steps have been taken to prevent this but in some instances it still can occur.

EventManager Columns

The EventManager columns have the following functions:

- Module:
  Name of the installed module.
  Double-clicking here either shows or hides that module’s screen
- Status:
  Shows the running status of that module.
  Double-clicking here either starts or stops that module.
- Sent:
  Shows how many events were created and sent by that module. Note that only those modules that create events increase this number, e.g. AlarmGen Pro. But modules like NNM Adapter for OpenView will only “receive” events and not create them, leaving the “Sent” value always at zero.
- Rcv:
  Shows how many events that module received.
- Startup:
  Shows the startup behavior for that module. Options are Auto (starts when ever EventManager starts up) or Manual (has to be started by double-clicking on the status).
  Double-clicking here toggles between Manual and Auto modules.

Sending System Health Alarms or Heart Beats

EventManager can be configured to send out events that show NotificationWorks module status every 15, 30, 45, or 60 minutes, keeping you informed that NotificationWorks is still running. PMPro can be used to refine the time even further, e.g. once at 3:00 PM every day.

NotificationWorks can also be put into Redundancy mode, running two complete copies of NotificationWorks as primary and secondary. For more information on Redundancy mode read the “Running Redundancy Mode” section.

Open the Heart Beat Schedule dialog by selecting Configure >Heart Beat to enable or disable Heat Beat, and set how often to send the message. Use PMPro to fine tune when to receive the message.

Redundancy Mode

NotificationWorks™ can run in redundancy mode with a secondary instance monitoring the primary. If the primary stops responding to the secondary request for status, the secondary becomes “acting” primary until the primary is functioning again. At that time the secondary reverts back to its secondary monitoring role.

When secondary becomes “acting” primary, an event called “Event Manager: Acting Primary Role” is sent. When secondary relinquishes the “Acting Primary”, an event called “Event Manager: Relinquishing Primary Role” is sent to keep the administrator informed.

The minimum requirements for the secondary are EventManager and a 5-user copy of PMPro. For true redundancy run both NotificationWorks with the same modules and configure both identically.

To set up redundancy mode, install a second copy of NotificationWorks on a separate Windows PC which has IP access to the primary.

From the primary EventManager, select Configure > Redundancy Roles.
From the dialog select “Primary” and enter the IP address of the PC running the secondary instance. The port (default 9000) can be customized here as well. Use the Microsoft “netstat” command to locate available ports. Click “Ok” to close this dialog box.

From the secondary instance, follow the same steps and select “Secondary”, enter the same port, then click “Ok” to close the dialog.

All the modules run in the secondary copy need to be set to “Auto” startup mode by double-clicking on any modules set to “Manual” in the EventManager’s Startup column. Lastly, verify all of the secondary modules are not running (stopped). If the primary fails, the secondary starts up only those modules set to “Auto” startup mode.

To have complete redundancy configure any event sources to send their events to both the primary and secondary instance of NotificationWorks and ensure that the configuration for both instances of NotificationWorks are identical.

Tip: Assign and schedule those two EventManager event messages about redundancy roles.

Find additional failsafe options of NotificationWorks’ PMPro for event delivery and delivery confirmation later in this document.

Temporary Suspend Events

To suspend all events for a certain amount of time, for example while restarting servers, routers, etc. put EventManager into suspend mode for a specific amount of time. EventManager will automatically resume processing events after suspend mode time has expired.

To turn on suspend mode select Suspend > Suspend Processing Events. In the resulting dialog, specify the length of suspend mode or click “Resume.”

Uninstalling Modules

To remove a module from EventManager select the module from the EventManager list, then select Configure > Remove Selected Module.
Atlantis Software Product Manager appears. Select the module again then click “Uninstall Module”. This completely removes the module from the EventManager and Product Manager. If the module has licenses installed, they need to be removed first. Refer to the “Managing Licenses” section for details.

Managing Licenses

After installation, Atlantis Software products run 30 days in evaluation mode. In order to properly license Atlantis Software products, License IDs have to be installed which can be obtained through Atlantis Software’s online licensing system.

To obtain a License ID, the following items are required:

- Access ID – Provided at the time of purchase
- PC ID – Displayed in the License dialog
- Email address – A valid email address
- Internet connection – Required to connect to the license server

To manage licenses, either open EventManager and select Configure > Manage Licenses, or run as_prod.exe from the Windows directory.

Adding/Creating Licenses

If Product Manager is installed on a console with Internet access:

1) Launch Product Manager either by opening EventManager and selecting Configure > Manage Licenses or by running as_prod.exe from the Windows directory.

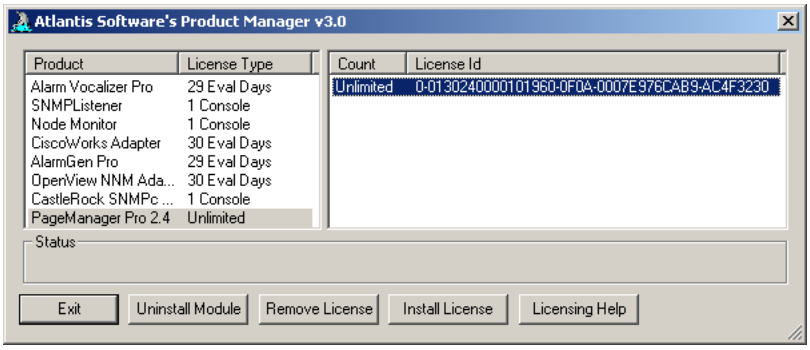


Figure 3.2: Product Manager

2) Click “Install License”. It is not necessary to select a module. The “Adding New License” dialog appears.

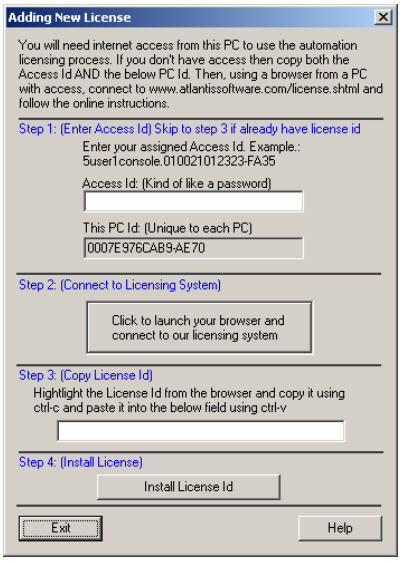
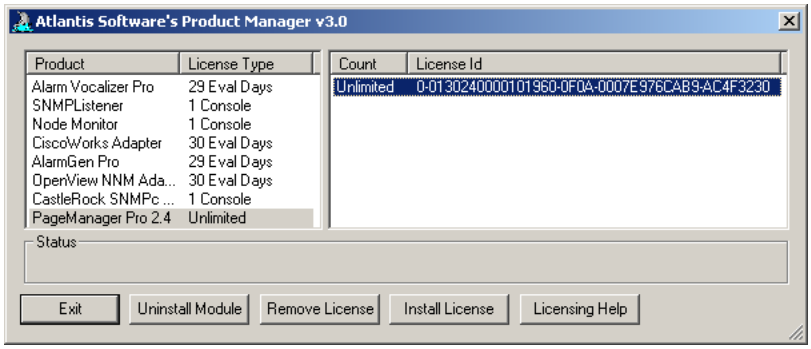


Figure 3.3: Adding New License

3) In Step 1, enter the Access ID that was provided at the time of purchase into the Access ID field.
4) In Step 2, press the button to launch a browser window and connect to Atlantis Software’s licensing server.
5) Follow the on-screen instructions to create a License ID.
6) If this step is performed for the first time, you will be prompted to enter an email address and fill out a customer form. It is very important to fill it out as completely and accurately as possible.
   Every customer has to go through this process only once. If the customer form has been completed previously, skip to the next step.
7) Copy the License ID from the browser window into the License ID field in Step 3 in the “Adding New License” dialog
8) Click “Install License ID” to apply the License ID
9) Repeat steps 2) through 8) for each Access ID
10) Click “Exit” to complete the process

Please make a note of the email address entered as it identifies your profile in the customer database. Keep it together with the Access IDs and License IDs in a safe place.

If Product Manager is installed on a console without Internet access:



1) Launch Product Manager either by opening EventManager and selecting Configure > Manage Licenses or by running as_prod.exe from the Windows directory.
2) Click “Install License”. It is not necessary to select a module. The “Adding New License” dialog appears.
3) Make a note of the PC ID shown in Step 1

Figure 3.4: Product Manager

4) On another PC with Internet access, launch a browser window and navigate to http://www.atlantissoftware.com/license.shtml.
5) Follow the on-screen instructions to create a License ID.
6) If this step is performed for the first time, you will be prompted to enter an email address and fill out a customer form. It is very important to fill it out as completely and accurately as possible.
   Every customer has to go through this process only once. If the customer form has been completed previously, skip to the next step.
7) Make a note of the new License ID. Go back to the PC running Product Manager and enter it into the License ID field in Step 3 in the “Adding New License” dialog
8) Click “Install License ID” to apply the License ID
9) Repeat steps 2) through 8) for each Access ID
10) Click “Exit” to complete the process

Please make a note of the email address entered as it identifies your profile in the customer database. Keep it together with the Access and License IDs in a safe place.

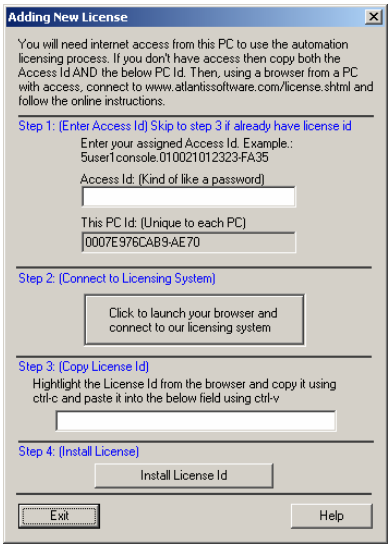


Figure 3.5: Adding New License

Removing or Moving Licenses

NOTE: Licenses do not have to be removed when performing a reinstall on the same computer.

Licenses are tied to the MAC address of the Network Interface Card (NIC) of the computer the software is installed on. Therefore it is necessary to remove and recreate the license when replacing the NIC with a different one or installing the software on a different computer

To remove the license from the current computer:

1) Launch Product Manager either by opening EventManager and selecting Configure > Manage Licenses or by running as_prod.exe from the Windows directory
2) Select the module and the License ID to remove
3) Click “Remove License”
4) Follow the instructions that will appear
5) Email the uninstall license confirmation file C:\as_ulc.txt to asinfo@atlantissoftware.com with the subject line “unlock Access IDs”. After the file has been verified you will receive a reply containing your customer licensing record and notification that your Access IDs have been “unlocked”. This process can be as short as 15 minutes.

After removing the license(s), replace the NIC or reinstall the software on a different computer, then follow the instructions “Adding/Creating Licenses” to reapply the license(s).

Managing the Devices

EventManager uses Atlantis Software's Device Manager program to manage device host names and IP addresses. Devices are automatically added as new ones arrive with event messages. Device Manager also provides the ability to create groups, allowing the organization of devices into groups which can be assigned to PMPro for easier event managing.

To bring up Device Manager from EventManager, select Configure > Device List.

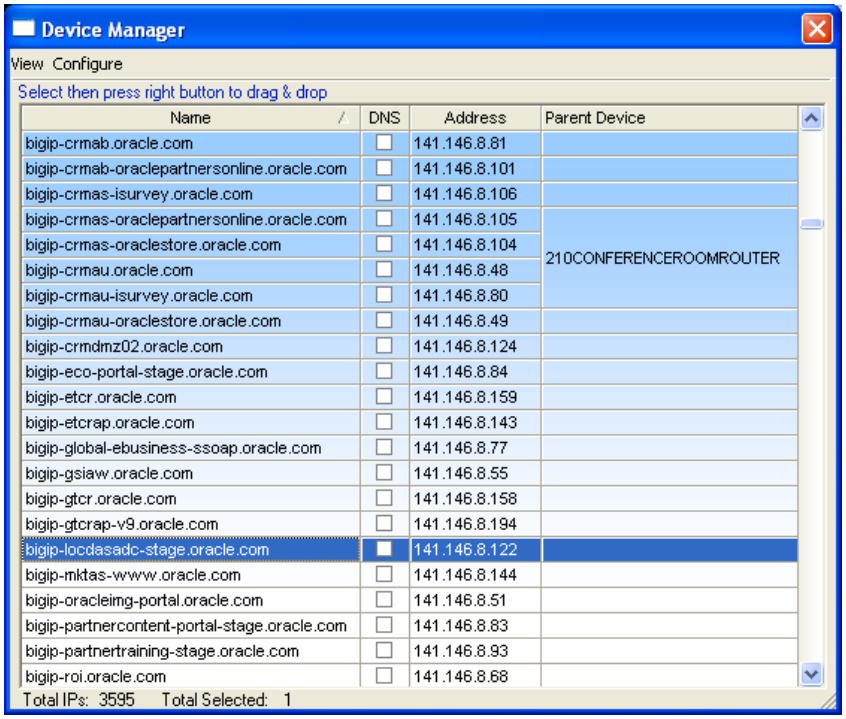


Figure 3.6: Device Manager

The screen and columns can be resized as needed. The device list contains three columns:

Name – Host name of the device
DNS – For future use, not currently used
Address – IP address of the device. A single device can have multiple addresses assigned.
Parent Device – This is used for the PageManager's "Upstream Failure" Filter. Which allows PMPro to ping the device's parent to see if it is responding. If not then PMPro's filter will nullify the alarm. See the PageManager Pro "Alarm Correlation & Downstream Filtering" section for more information. You can right mouse click and drag devices onto existing parent names to make fast assignments or double click on the device name.

The Device Views

The View menu allows filtering of devices into three categories:

All – All devices
User Configured – Devices manually entered through the "Manually add devices" option in Device Manager
Discovered – Devices that came into EventManager with an event or were discovered from the Auto Add Devices feature.

Configuring Devices

Select Configure > Device list to:

- export the device list
- import a device list from a delimited text file
- add devices manually
- automatically add devices from the Window's network neighborhood
- automatically add devices from a specific IP range
- resolve multiple device IP addresses

Instructions for these features are provided in their respective dialogs.

Configuring Device Groups

Device Manager provides the ability to create groups and assign devices to them. These groups can be assigned to profiles/personnel in PMPro which can greatly simplify managing devices.

To create a device group:

In Device Manager, select Configure > Groups > Configure List. This will "hide" the current device list and bring up two other dialogs, the Available Devices list and the Device Group list.

In the Group list dialog, select Groups > Create Group

Enter a name for the group and click "OK"

Select the new group name. From the "Available Devices" list, select one or more devices. Drag the devices with the right mouse button and drop them on the group name.

Remove devices from groups by selecting the device in a specific group, then selecting Devices > Remove Selected Devices from Group.

After the device groups have been created, click the "X" in the upper right corner of the Device Group list dialog to close it.

4
PageManager Pro 2.5

PageManager Pro 2.5 (PMPro) has many filters and delivery options which are detailed in this chapter. Skip to the quick start section to get up and running quickly.

PMPro is centered on Personnel profiles. Time schedules, event assignments, device filters, what couriers to use (how and where to send the events), and most filters are tied to profiles.

PageManager Pro's Page Layout

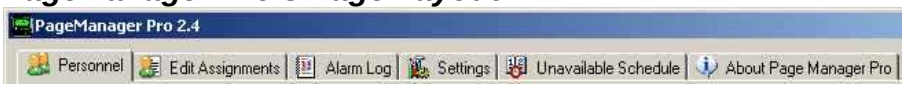


Figure 4.1: PageManager Pro's Page Layout

PMPro's screen layout is arranged by pages:

- Personnel - Set up/edit Personnel profiles, escalation control, nodes, and services
- Edit Assignments - Setup/edit alarm assignments and schedules
- Alarm Log - Logs all forwarded alarms
- Settings - Adjust couriers, alarm database, alarm filters, etc.
- Unavailable Schedule – activate or deactivate personnel
- About PageManager - Displays registered owner information and copyrights

Move from page to page by clicking on the page tabs.

Items to Configure

This section explains how to start PMPro 2.5, configure personnel profiles, couriers (how events are delivered), and alarm schedules. It is assumed that you have an installed and working modem and/or Internet connection and/or you have a working e-mail service that supports SMTP or ESMTP. The checklist below shows the recommended task order.

1) Setup your SQL connect string
2) Add personnel
3) Add and configure couriers
4) Assign alarms
5) Assign time schedules

Quick Start

Get you up and running as quickly as possible with the following steps. For a more in-depth description of the PMPro controls refer to the rest of this section.

1 **Starting PageManager Pro 2.5:**
- 1.1 By default PageManager will be started when Event Manager is launched. If this is disabled, select PageManager from the application module list in Event Manager and double-click the startup field.
- 1.2 When starting for the first time, a popup box will appear asking for information to connect to your SQL server. We have tried to make it as simple as we can but there are so many security concerns that we cannot make it automated. But if you have the SQL installed on the same PC as NotificationWorks then we try to create the connect string for you. The popup box will display a possible connect string, click the test button and if the success message box appears then click the OK button. If not then you will need to enter the connect that will work for your setup.

2 **Configure Personnel/Profile:**
- 2.1 From the Personnel page, click "Create". The creation wizard leads through the steps needed to create a new personnel/profile. A yellow task list appears showing the steps to be completed. Each task will be crossed out as it is completed. Placing the mouse arrow over any of the tasks displays a help box describing the task.
- 2.2 Enter a unique name for the new profile. Leave the "Profile Type" set to "Personnel". Click "Next". Item 1 has been crossed out on the yellow task list.

3 **Configure Alarms/Events:**

3.1 The alarm/event list is displayed. If new to NotificationWorks, it is recommended to select all events. Select the top event, scroll down to the bottom of the list, hold the Shift key, and click the last event.

3.2 Click the “Assign Alarms” button. By default, the events will be scheduled for all week and all 24 hours. Change the schedule from the PMPro’s Edit Assignment tab.

3.3 Click “Next”. The Device list manager appears.

4 **Assigning Devices:**

4.1 Filter alarms by devices so that only those assigned alarms will be sent when they are received from assigned devices. If new to NotificationWorks it is recommended to use the default of “Any device”. In this case close this dialog by clicking the “X” in the upper right corner. Courier manager appears.

5 **Configure Couriers:**

Click “Yes” in the “Bring up the Manage Courier” dialog. From the Courier dialog select the desired Courier transport type and click “Create”. Refer to the next section for the selected Courier transport type.

5.1 **Configure DOSCommand Courier Transport Type:**

5.1.1 Enter a unique name for the courier in the name field.

5.1.2 Enter the program to run, including its path in the command field.

5.1.3 Enter any program parameters to pass to the above program in the parameter field.

5.1.4 To see the program when it is run leave the “Hide Window” option unchecked.

5.1.5 Click “OK”

5.2 **Configure SMTP Email Transport Type:**

5.2.1 Enter a unique name for the courier in the name field.

5.2.2 The port number field should be set to 25. Enter a different port number if needed.

5.2.3 Timeout should be set to the default of zero in order to keep trying until a connection is made, unless the connection is not possible.

5.2.4 Enter the SMTP mail server’s name or IP address (preferred) into the Host Name field.

5.2.5 Enter an email address that is allowed to use the mail server into the Source Email Address field. This is the sender of the event message. Note: Some mail servers will only allow sending of email from known email accounts.

5.2.6 Leave the rest of the fields set to the defaults and click “Save”.

5.3 **Configure Text Msg via Modem Courier Transport Type:**

5.3.1 Enter a unique name for the courier in the name field.

5.3.2 Select either Text or Numeric pager type from the Service Type check boxes. Note that if Numeric type is selected all events and devices need to be changed to use numbers instead of text. Refer to the Numeric pagers section for details.

5.3.3 Select which Pager Service Protocol to use from the “Service Protocol” list. Note: To use the XML scripting to connect to a text terminal refer to the XML scripting section.

5.3.4 Enter the service’s terminal number in the “Service’s phone number” field. For text paging this will be answered by another modem and not just a couple of beeps.

5.3.5 Choose which modem driver to use from the “Modem/ISDN Device” list.

5.3.6 Most paging services use 7 data bits, even parity, and 1 stop bit, which are the default settings. Change only if required.

5.3.7 Click “Save”

Note: For numeric paging, please read the detailed section for Text Msg via Modem Courier

5.4 **Configure HTTP WebForm Courier Transport Type:**

5.4.1 This courier allows posting data to a web form. Enter a unique name into the name field.

5.4.2 Enter the whole URL for the result page (the URL that occurs when the web form’s submit button is pressed)

5.4.3 Enter the text that appears when the posting is successful or not into the results checking fields. Only one is needed.

5.4.4 Enter the web form’s variables into the variable list. Click the “Get Variables” button to retrieve all variables from the form’s page. Delete the variables not needed.

5.4.5 Right-click in the “Value” field to assign a value to that variable.

5.4.6 Click “OK” when done

5.5 **Configure SNPP Courier Transport Type:**

SNPP (Simple Network Paging Protocol) is now supported by many mobile services. Click the SNPP button to open a browser window showing a list of sites that support SNPP. Using SNPP is recommended, as it is more dependable than email.

5.5.1 Enter a unique name for the courier into the name field.
5.5.2 Enter the URL or IP address of the SNPP server into the Server Name field.
5.5.3 Enter server's SNPP port address (444 default) and the maximum length of the message the server can accept in the port and max length fields.
5.5.4 In the Msgs exceed max length field; configure how PMPro handles messages that exceed the Max Msg Length setting.
5.5.5 Seconds between retries field, 5 seconds is default.
5.5.6 The default for the Message Format field is: %msg%. This is the PMPro's variable for the event message. Right-clicking in the Message Format field brings up a list of possible PMPro variables to use in the message.
5.5.7 The Authentication Id fields should only be used in the rare occasion if the used service states that it uses authentication IDs.
Click "OK" when done

5.6 **Configure Mobile Messaging Courier Transport Type:**
Read the Mobile Messaging section for more details about support wireless devices. But basically, the mobile device should work if it supports the GSM AT+C command set.

5.6.1 Click the Add button from the Port tab and follow the wizard's instructions.
5.6.2 After completing the Port creation, select the Services tab then click the Add button.
5.6.3 Enter a unique name for the courier into the Name field.
5.6.4 Select the COM port from the drop down list.
5.6.5 Enter your SMSC (Simple Messaging Service Center) phone number into the SMSC field. Most of the time this number can be find in your phones settings, if not then contact your service to obtain this number. This is where all of your messages will be set to then rerouted to the final destination.
5.6.6 Click the OK when done.

6 **Select and Assign a Courier**
6.1 Select the new configuration name and click "Assign". Answer any fields that might appear.
6.2 Click "Done" in the Assigned Couriers dialog box.

If something was done incorrectly a "<WARNING>" will be displayed next to the profile name. Placing the mouse over this entry displays a message showing what is wrong.

Any received events are now sent to the profile that was created. See any received events with their sending status by clicking on the Alarm Log tab.

This concludes a quick overview of PMPro 2.5 setup. For more detailed instruction refer to the rest of the manual.

Personnel Page

This page provides the ability to add or edit Personnel/Profiles, create templates and assign node responsibilities.

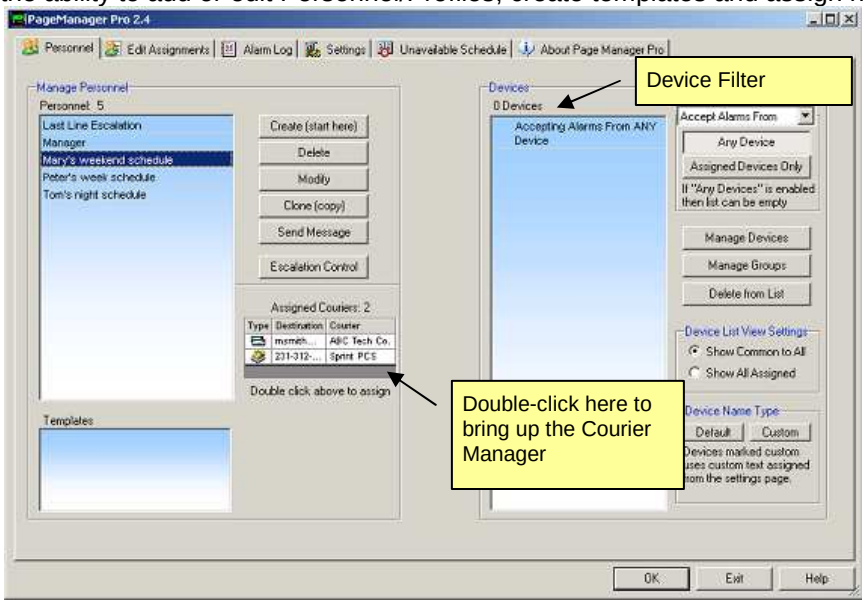


Figure 4.2: Personnel Page

Create (start here)

Use this option to create new personnel using the creation wizard. The wizard can be stopped at any time. It is explained in detail in the PMPro 2.5 quick start section above.

Clicking on the “Create” button brings up the following dialog:

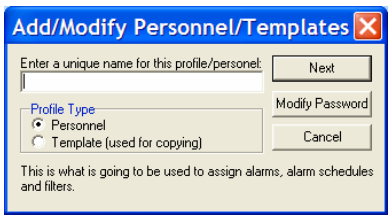


Figure 4.3: Add/Modify Personnel/Templates dialog

A yellow task list appears showing the steps to be completed. Each task will be crossed out as it is completed. Placing the mouse arrow over any of the tasks displays a help box describing the task.

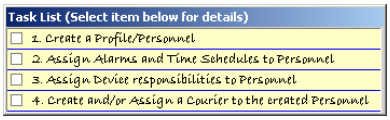


Figure 4.4: Task List

Use this function to create a profile or modify the password. Passwords are currently used for the web interface logon function.

There are two types of profiles: Personnel and Templates.

Personnel profiles are the main focus for most settings, assignments and schedules. Alarms (events), schedules, couriers (the how and where events are sent), and device filters are assigned to Personnel profiles.

Templates provide a convenient way of creating or changing personnel profile settings. Use a template to “clone” its settings, alarm assignments, and schedules to other personnel profiles.

The button labeled “Modify Password” is used to assign passwords to that profile. The password is required when logging on using the “Web Interface” which is described in later in the “Web Event Viewer” section.

Click “Next” to go to the next part of the creation wizard.

Delete

This option deletes the selected profile from either the Personnel or the Template list.

Modify

This option allows modifying the selected profile’s name and password. To modify a profile, select a profile name from either the Personnel list or the Template list and click “Modify”.

Clone Personnel

This powerful feature allows using the settings from one personnel or template profile to replace, add, or remove these settings in other personnel or template profiles.

To clone a profile:

1) Click “Clone”. The “Clone Personnel dialog appears.

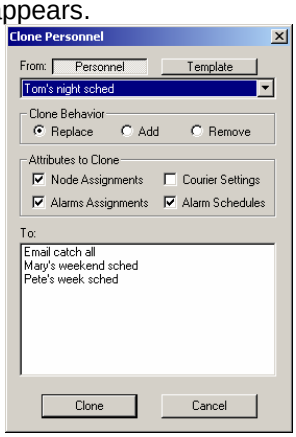


Figure 4.5: Clone Personnel dialog

2) Select the type of profile to clone (Personnel or Template)

3) Select the name of the profile to clone from the dropdown list

4) Select the type of clone behavior. The source profile is used as the source for these attributes:
   Replace - replaces all selected personnel with the selected attributes.
   Add – Adds the selected attributes to the selected personnel in addition to what they already have.
   Remove – Removes the selection from the selected personnel.

5) Select which attributes to clone. When choosing a template “Courier Settings” is unavailable because templates do not have assigned couriers.

6) Click “Clone” to start the process

Send Message / Testing Couriers

Messages can be sent to selected personnel. Select one or more entries from the personnel list and click “Send Message”. The “Send Message” dialog appears. Select how to send the message, either “Direct” (default) or via “Alarm Log”. “Direct” will send out the message without loggin. “Alarm Log” enters the message into the log showing when it was sent. Enter the message to send and click “Send”.

Output from the courier can be used to troubleshoot any problems. When using a courier that is a modem transport, e.g. TAP/UCP also enable “Log all communication after connection” from that courier’s configuration dialog to log the conversation that occurs after the modems have connected for more information. Refer to the “Managing Couriers” section for more details.

Device Filter

By default, profiles accept alarms from any device. To set up device filtering, read the “Manage Devices” section further down. When an alarm is received and it has been “assigned” AND “scheduled” AND the arrival time of the alarm is within the scheduled time, (additional optional filters are explained in the “The Alarm Filtering Process” section) it will be sent without care as to where it came from.

Each profile can have its own specific device filter settings. Selecting one profile shows its device filter settings. See what device filters multiple profiles have in common by selecting multiple profiles, then selecting the “Show Common to All” option in the “Device List View Settings” section.

Accept Alarms From / Exclude Alarms From

The dropdown list at the top of the right side of Personnel Page in the Device section is for setting the device filter behavior to include or exclude devices in the device list. Possible settings are:

- **Accept Alarms From (default):** Only events that come from devices in the device list or are members of a device group that is in the device list will be sent to the selected profile.
- **Exclude Alarms From:** Only events that do not come from devices or devices in device groups assigned in the device list will be sent to the selected profile.

Any Device / Assigned Devices Only

When a profile is selected, choose one of these options:

- **Any Device:** The selected profile accepts events from any device.
- **Assigned Devices Only:** Devices and/or device groups in the device list will be included or excluded from the selected profile, depending on the Accept/Exclude setting described above.

Manage Devices

This button brings up the Device Manager which was explained in detail earlier in Event Manager’s “Managing the Devices” chapter. Click this button and select the desired devices. Drag them with the right mouse button and drop them on the PMPro24’s device list to assign them to the selected profile. It is also possible to drag and drop the selected devices from the Device Manager right on a profile name to automatically assign those devices to that profile.

Manage Groups

Like the “Manage Devices” button, it brings up the Device Manager but shows the Device Manager’s Device Groups instead. Assign device groups to the selected profile the same way as devices.

Device List View Settings

View what devices the selected profiles have in common or show all assigned devices for the selected profiles. It is a good way to find out if someone is missing a device from their assignment.

Device Name Type (Use custom device names)

PMPro 2.5 can use a customized name for a device which is very useful when using a numeric pager.

To enable this feature, select the device, then click the “Custom” button. A paper icon appears next to the device name indicating that the device has a custom name.

By default, device names have an associated number assigned to it which is the custom name it uses when enabling the option for the selected node. To change this custom text use the “Customize Text” option from the “Settings” page. For more information on changing this text see the “Customize Text” section.

Assigned Couriers

Bring up the “Assigned Couriers” dialog by double-clicking inside of the “Assigned Couriers” space.

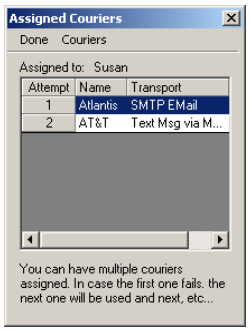


Figure 4.5: Assigned Couriers

Couriers are the means by which events are sent. Create a courier and then assign it to one or more profiles. During assignment the profiles are also configured to tell the courier where to send the event. Each profile can have multiple couriers assigned.

PMPro sends out an event “PMPro: Courier failed, attempting next” when a courier fails and attempts to use the next one. When PMPro has exhausted the list of assigned couriers it sends out an event “PMPro: Delivery failed, no other courier assigned”.

If multiple couriers are assigned they are listed in the order of which they are used. Change this order by selecting the courier and dragging it with the right mouse button to a new position.

To assign a courier to a profile and configure it select Couriers > Edit Assignments. The Edit Assignments dialog varies depending on the transport the courier is using. However, it always includes a destination field to specify where the event will be sent.

To create a courier bring up the Courier Manager by selecting Couriers > Manage Couriers.

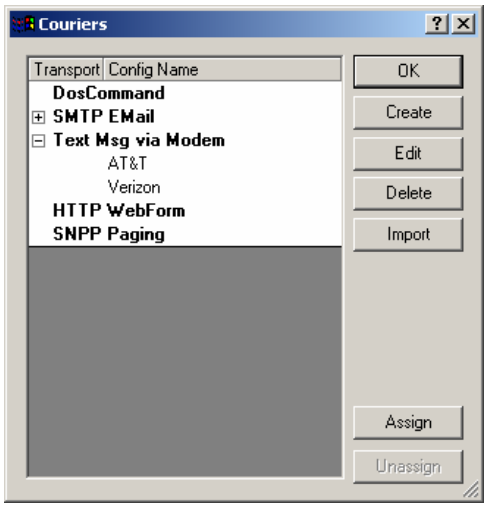


Figure 4.6: Courier Manager

Create a courier by following these steps:

1) Select a transport to use

2) Create a courier using that transport

3) Assign that courier to a profile and configure the profile to tell the courier where to send the message

Do not create more than one courier for a specific service. If multiple users use SkyTel paging service, create only one courier using the modem transport. When assigning that SkyTel courier to each user enter the information into the profile

that will tell the SkyTel courier where to send the message. This way PMPro is able to handle messages much more efficiently when they are going to the same courier even though they are going to different destinations.

PMPro currently offers 5 courier transports:

- **DOSCommand** – Launch another program.
- **SMTP Email** – Send events to an (E)-SMTP service via the Internet.
- **Text Msg via Modem** – Send events to another terminal using TAP, UCP, and ASCII terminal using a modem.
- **HTTP WebForm** – Send events to a web page via the Internet.
- **SNPP Paging** – Recommended if your mobile service supports it. More reliable than SMTP. Uses the Internet to send events.
- **Mobile Messaging** – By attaching one of the supported wireless modems or phones you can then send the events to other mobile phones by using your mobile's text messaging service. Keep in mind your service charges for text messaging.

The order of reliability is:

1. **Text Msg via Modem and Mobile Messaging**: Best since it does not rely on a good network connection, and receives confirmation from service that it will deliver the message.
2. **SNPP Paging**: Better than SMTP since it receives confirmation from the destination service that it will deliver the message.
3. **SMTP Email**: OK, it does receive confirmation from the SMTP service that it will deliver the message but offers no confirmation that the mobile service has received and will deliver the message.

All transports can be used with PMPro's escalation/conformation feature. This requires the recipient to reply when they receive the message, therefore providing the best level of delivery confirmation.

To view a specific transport dialog, select which Transport to use for the courier, then click "Create". Now skip to the section for the selected transport:

DOSCommand

Use this transport to run batch files and applications, or even send the events to a SQL database (see example below).

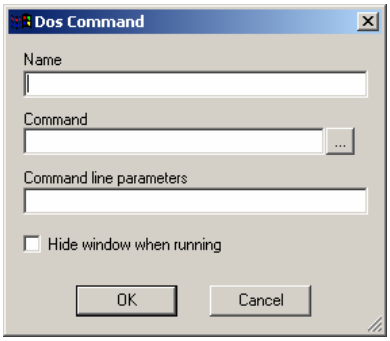


Figure 4.7: DOSCommand Dialog

It is recommended to create a batch file to run applications to provide the administrator with more control and flexibility.

Use PMPro 2.5 to launch another application and pass it parameters.

It is recommended to always run the DOS command interpreter (Windows 9x: command.com, Windows NT 4, 2000, XP, 2003: cmd.exe) and in the PMPro's "Parameters" field pass it the name of the batch file. Use the /k switch for debugging purposes and /c when debugging is completed. The /k switch leaves the DOS window open for the administrator to examine the results. The /c switch closes it after the command has completed.

The following PMPro variables are available and can be used as DOS environment variables in batch files or in the "Parameters" field. They need to be enclosed in percent symbols as shown:

Variable	Description
%site%	Name of the site that is running PageManager Pro
%date%	Configurable date string (See changing date/time format section)

%time%	Configurable time string. (See changing date/time format section)
%rawtime%	The number of seconds elapsed since midnight (00:00:00 GMT), January 1, 1970
%rawmsg%	The raw alarm messages without any pre-pended additions
%device%	The affected name of the device name
%ipaddr%	IP address of origin of the event
%profile%	The name of the Personnel profile.
%profileid%	ID of the Personnel profile
%alarmname%	Name of the alarm
%msg%	The formatted alarm message
%severity%	Alarm severity: Informational, Warning, Major, Critical
%logid%	ID of the log entry
%level%	Courier level used to send event
%dupmsg%	Message from the duplicate threshold field if valid
%cover%	Name of the covering profile if valid
%destination%	The destination assigned to the courier

Here is an example of a DOSCommand courier sending events to a Microsoft SQL server:

1) Create a batch file called “sqlbat.bat” containing the following commands:

   C:\MSSQL7\Binn\osql -E -d DataBaseName -Q "insert TableName (nodes,message) values ('%Device%','%Msg%')"

   The above is all one line. Change the DataBaseName to the actual SQL database name and change the TableName to the actual SQL database table. In the example, the values of the variables Device and Msg are passed into the two fields “nodes” and “messages”.
   Osql.exe is a Microsoft SQL server utility that allows sending SQL commands via the command line.

2) Enter SQL into the Name field

3) Enter c:\winnt\system32\cmd.exe

4) Enter sqlbat.bat including locations into the parameter field i.e.
   /k c:mssql7\binn\sqlbat.bat

5) Leave the “Hide Windows” option unchecked for debugging

6) Click the OK button to close the DOSCommand dialog

7) From the Courier Manager, click “Assign” to assign this courier to the selected profile

SMTP (Email)

This transport provides the ability to send events to anything that supports SMTP (Simple Mail Transport Protocol), including mobile phones, pagers, PCs, PDAs, etc. It is recommended to check with the service to see if it supports SNPP as it is far more reliable than using email to send SMS messages.

PMPro 2.5 supports multiple mail servers, mail servers with authentication (Auth Login), and email templates (discussed later). Please refer to the “Quick Start” section for creating a Courier using SMTP as a transport.

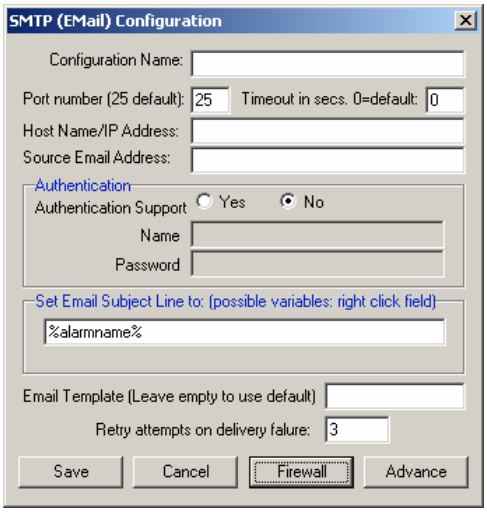


Figure 4.8: SMPT Configuration

The subject line can be used to send PMPro values using variables. To get a list of possible variables, right-click in the subject field. When using escalation, it is recommended to use the following text in the subject line:

%alarmname% pid=%profiled% logid=%logid%

The reason for this is discussed in detail in the “Escalation Control” section.

Email Templates

When using email delivery messages can be formatted based on a pre-defined template. This is useful when sending to automated email processing services. The template can also contain PMPro variables.

Example template format:

Event Name: %alarmname%
Event Message: %msg%

Text Msg via Modem

This method uses the modem as the transport and supports 3 protocols: TAP, UCP, and Text (ASCII) Terminal using XML scripting.

TAP (Telocator Alphanumeric input Protocol) is the most modem type paging protocol used in North America.

UCP (Universal Communication Protocol) is mostly used in Europe.

If a XML script for a Text Terminal has been created it will be listed in the “Service Protocol” drop down list. How to create a script is covered in another document located at:
http://www.atlantissoftware.com/help/XLMScripting.pdf

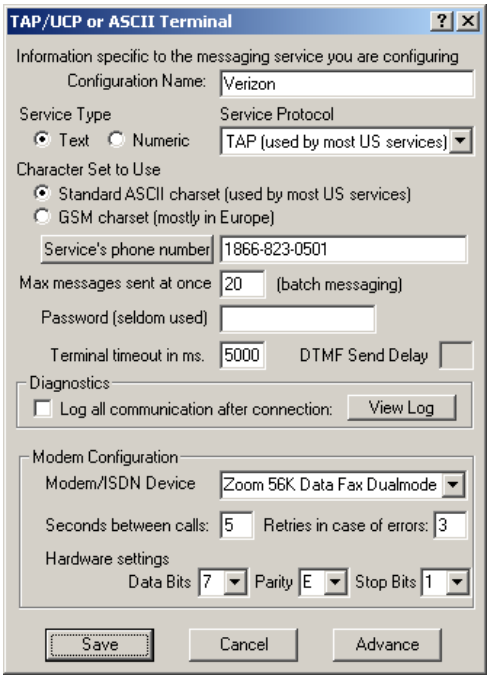


Figure 4.9: TAP/UCP/ASCII Terminal Dialog

Service Type:
This has two options: Text or Numeric. Select “Text” when using TCP, UCP, or ASCII Terminal. Select “Numeric” when using a numeric pager. Certain fields in this dialog deactivate depending on which type is selected.

Service Protocol:
Choose the communication protocol (this is not a modem protocol) to use. Options are TAP or UCP, and XML scripts if present.

Character Set to Use:
Configures which character set to use. Standard ASCII is used by most US services. GSM is mostly used in Europe.

Service’s Phone Number:
Enter the terminal’s phone number in the field next to this button. Click this button to launch a browser window to connect to www.AtlantisSoftware.com and display a list of known terminal numbers.

If “Service Type” is set to “Text” this number needs to be for a terminal with a modem connected and not the one used when sending a page from a phone. These phone numbers are only used when “Service Type” is set to “Numeric”.

Max messages sent at once:
This option is extremely useful when using text service type. It allows multiple messages to be sent during a connection instead of just one for each connection.

Example: Five events arrive and need to be sent to four users using SkyTel service. If Max messages are set to 20 then PMPro will need to only connect once to send all 20 messages (4 users x 5 messages = 20). Most services support batch messaging but the max amount differs. If the max is unknown, perform some testing to determine it.

Password
Rarely used but specified in the UCP spec. Enter here if the service requires it.

Terminal timeout in ms:
Maximum amount of time (default is 5000 milliseconds) PMPro will allow for no reply after connecting to a service before it errors and closes the connection.

DTMF delay in sec:
For numeric service types. Specifies how long in seconds PMPro will wait until it begins sending the touch tones to the paging service. Set the time high enough for PMPro to have enough time to dial the modem and the paging services to answer and get ready to receive the tones. 30 seconds is a good place to start. Turn the modem volume to high to hear when it is appropriate to start sending.

> **NOTE:** For numeric paging, sometimes modems will not hang-up in a timely meaner. This is due to the modem not being able to tell that the answering site has hung-up. So, to force PMPro to hang-up the modem after delivering the numeric page add the following to the PMPro24 section in the EventMan.ini file located in your winnt folder. This is ONLY for numeric paging.
>
> **[PMPro24]**
> DTMF=2
>
> 2 is the number of seconds to wait before hanging up after delivering the message.

Diagnostics:
Used when encountering issues sending to a service like the modem hanging up after the modem has connected and completed synching. Enable the “Log all communication after connection” to create a log that shows all communication between PMPro and the service. An empty log indicates the modem is disconnecting from the service’s modem due to a modem configuration issue.

Modem/ISDN Device:
Use this option to select which modem driver that this courier should use. It displays all Windows modem drivers that are installed.

Seconds between calls:
Increase this number if the modem does not have enough time to reinitialize between calls. Some modems require more than 5 seconds between calls to hang up and reset.

Advanced
Not normally needed. Advance configuration options are:

General
All of these settings have already been covered above.

Additional
Screen to provide further parameters for the current service.

In the Terminal Number field, enter the number to dial for the paging service for modem or ISDN access. This is not the PIN number itself. The PIN number is entered when assigning this courier to a profile.

Below that, enter the maximum length for a notification message. Messages longer than this will be split up.

Enter the dial-in password required by some service types.

For mobile transmission services (such as D2), enter the corresponding prefix without leading zeroes in the Standard Prefix field. For pager services, optionally enter the value for the calling area.

In the last field specify how many notification messages are accepted by the service during a single connection session.

Most pager services only permit a single notification message, i.e. each dispatched notification message requires a separate connection session.

Type
Specify the kind of service: Alphanumeric, Numerical or Audio-only. Usually this is Alphanumeric.

During the application of the UCP protocol specify the kind of protocol operation that should be used. The base operation, which is supported by nearly all UCP-based services, specifies a value of 01. Use this if all else fails. Additionally, the operation types of 30 and 51 are also supported.

Several services (e.g. Skyper) also include the pager number when dialing into the terminal number and establishing a connection. Specify the pager number here if desired.

Activate the “Max word wrap” option to split up messages that might otherwise be too long to send in a single call. This option splits long messages into smaller parts, and sends them out in incremental dispatches.

The “Breakup larger messages automatically” parameter indicates the maximum number of characters in one word which should be pushed to the next partial message where the effect would otherwise be a split word. This improves the readability of texts on the receiver in cases where the message is sent in either a group dispatch or in individual parts.

Country Codes for International Dialing
Because mobile transmission services, for example D1 and D2, support the broadcast of notification messages to so-called roaming partners, these services may be configured with the standard Country Codes used for international dialing. For example, to transmit a notification message to a subscriber on a German mobile transmission service, specify the Country Code for Germany (49). To transmit messages to subscribers on other networks, enter the corresponding country code here.

Notes:

- The Country Code for a particular subscriber remains the same even if the subscriber travels outside their home country, as long as the subscriber does not change his or her mobile transmission service. Only change the Country Code in cases where a subscriber switches to a mobile transmission service located in another country.
- Several mobile transmission services require that telephone numbers be entered using the following syntax: **00[Country Code][Prefix][Number]**. Establish here whether to enforce this syntax or not.
- In general, pager services do not require a Country Code.

Terminal Access
Configure the parameters for the terminal access in this dialog. Most services use either the combination 8N1 or 7E1.

HTTP WebForm

This uses the Internet as a transport and will post events to a web site. Usage includes posting events to a company web site that might be part of a trouble ticketing system, sending to a database using a web front-end, or sending to mobile devices using that service’s web page (like Arch).
The web page must support the “post” method and this courier is configured to post the information to the action page that would normally be shown in the HTML <form> tag. i.e.:
<form name=test method="post" action=”results.phd”>
It is recommended that only administrators with a good understanding of HTML create a courier using this transport.

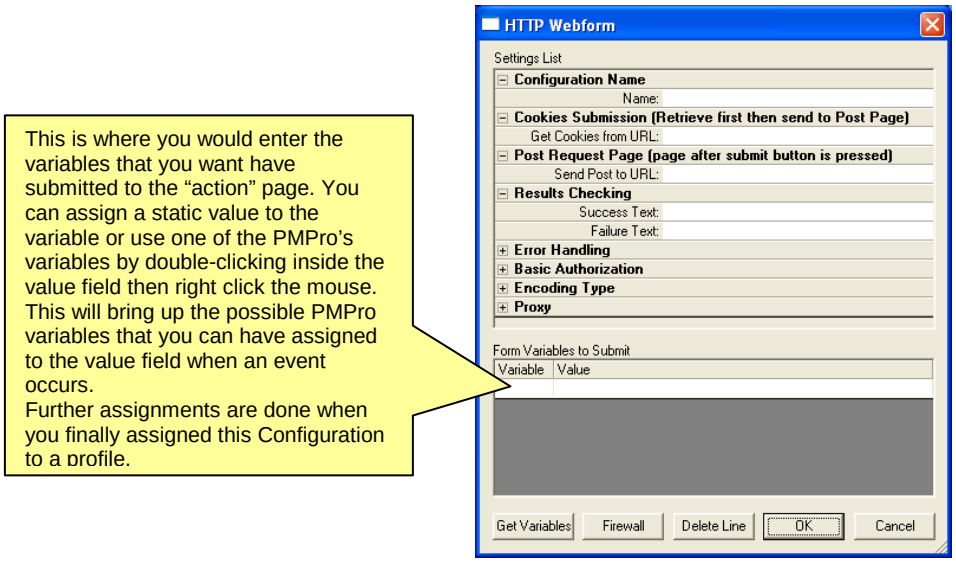


Figure 4.10: HTTP Webform

Configure Name:
Name of the courier

Cookies Submission:
Some sites have cookies (variables) that are needed to read and sent to the Post Page, if this is the case then enter that URL here.

Post Request Page:
In the "Send Post to URL" field, enter the location of where the post action should go, where the information is sent.

Results Checking:
Enter text that will show whether the post was successful or not. Either the Success or the Failure field must be used. If the success field is used and that text is not found then it is assumed that the operation failed and vice versa.

Basic Authorization:
If the site requires authorization enter it here.

Encoding Type:
The following three encoding types are supported:

- **URL Encoding:**
  This is the most common encoding for HTML form contents.
- **MultipartFormData:**
  This is MIME encoding allowing transmission of binary data.
- **QueryString:**
  An older form of encoding where the actual parameters are appended to the URL query string.

Proxy:
If a proxy server is used, enter its information here

Form Variables to Submit:
Enter the variables to submit to the action page. Assigned a static value to the variable or use one of the PMPro's variables by double-clicking inside the value field then right-clicking. This brings up the possible PMPro variables that can be assigned to the value field when an event occurs.

Get Variables Button:
This brings up a dialog to enter an URL (website). It will try and parse out the variables on that page, like a form page.

Here is a example of creating a HTTP WebForm that sends messages to Arch pagers using the Arch website:

1) Select the personnel to assigned the new courier to and create a HTML Form called Arch

2) Enter the following information into the WebForm:
   Name: Arch

Send Post to URL:
http://www.arch.com/cgi-bin/wwwpage.cgi
Success Text: Page Sent

Form Variables to Submit:

Variable:	Value:
PIN	%destination%
MSSG	%msg%
Q1	1

3) Click “OK” to get back to the courier list

4) Select the new WebForm courier “Arch” then click "Assign" and enter the pager number into the first field.

SNPP Paging

SNPP (Simple Network Paging Protocol) is recommended if the service supports it. SNPP receives confirmation that the service has received the message and will deliver. If confirmation of delivery is needed as well, use the PMPro escalation feature.

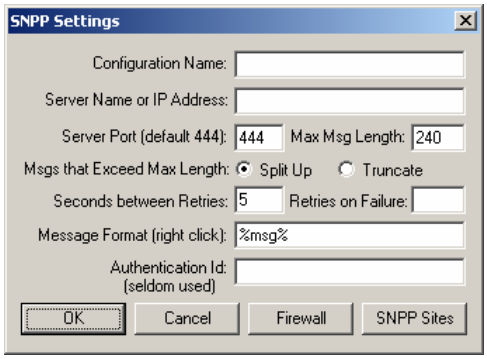


Figure 4.11: SNPP Settings

Configuration Name:
Name of the courier.

Server Name or IP Address:
The address of the host providing the SNPP service. Use the IP address if possible since it is quicker.

Server Port:
The port address for the service, usually 444.

Max Msg Length:
Maximum message length that the service can accept.

Msgs that Exceed Max Length:
Can do two things if message is too long: Split the message into multiple parts and send each one, or truncate the message at the maximum length.

Seconds between Retries:
The number of seconds to wait before resending after receiving an error.

Retries on Failure:
Number of retries after receiving an error on sending. Zero means no retries.

Message Format:
The format of the message. The default is %msg%. Right-click to bring up the possible PMPro variables.

Authentication Id:
Rarely used but specified in the SNPP spec.

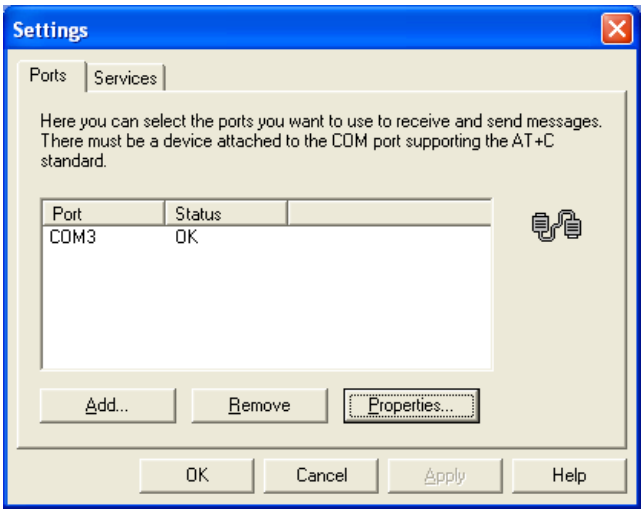
SNPP Sites Button:
Launches a browser window, connects to www.AtlantisSoftware.com, and displays a list of known SNPP sites. Contact your service provider directly if not listed.

Mobile Messaging

You can send out the alarms (events/alerts) using any wireless device connected to the COM port that supports the GSM AT+C command set. Here is a small list of supported wireless devices with their initialization strings:

Falcom A2 Modem: 9600 bps, 8N1 Initialization: AT+CMGF=0	Nokia Communicator Modem: 9600 bps, 8N1 Initialization: AT+CNMI=1,2 The COM port speed of the device and the PC must be configured to be the same.	Siemens M1 Modem: 19200 bps, 8N1 Initialization: AT+CMGF=0 Attention: The option to encode the SMSC in the PDU must be switched off in the software.
Nokia 30 GSM Connectivity Terminal Modem: 9600, 8N1 Initialization: AT+CMGF=0 AT+CNMI=1,0,0,1 AT+CPMS="SM","SM"	Nokia Data Suite Modem: 9600 bps, 8N1 Initialization: AT+CPMS="SM","SM" AT+CMGF=0 AT+CNMI=1,0	Siemens M20 Modem: 19200 bps, 8N1 Initialization: AT+CMGF=0
Nokia 7110, 6210 with DLR-3 data cable Modem: 19200 bps, 8N1 Initialization: AT+CMGF=0 AT+CNMI=1,0,0,1 AT+CPMS="SM","SM"	Siemens S45,M45,S55 Modem: 56000 bps, 8N1 Initialization: AT+CMGF=0 AT+CMGF="ME","ME"	Siemens TC35 Modem: 19200 bps, 8N1 Initialization: AT+CMGF=0
		Wavecom Modem: 9600 bps, 8N1 Initialization: AT+CMGF=0

The **Ports page** is where you can edit the settings for the ports, which are to be used by the mobile device, which support the AT+C-Standard.



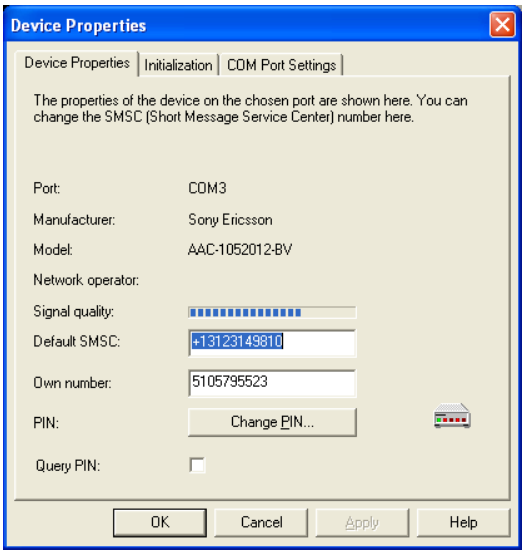
Add:
Here you can add a port. The Add Mobile Device dialog box will be shown.

Remove:
Click here to remove the selected port.

Properties:
Click this button to show the properties of the device on the chosen port. The Device Properties dialog box appears. In this dialog box you also can edit some properties like the number of the SMS-Center and the PIN (Personal Identification Number) for the SIM Card in the device.

By clicking on the Properties button you will see the Device Properties dialog as shown below.

In this dialog box you can see the properties of the device on the specified port. Some of them you can edit.



Port:
The chosen port.

Manufacturer:
The device manufacturer.

Model:
Model name of the device.

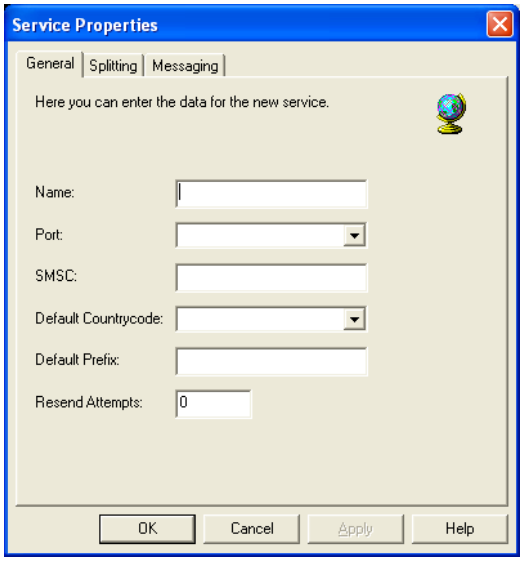
Network Operator:
The network operator.

SMSC-Number:
The number of the used SMS-Center.

Own number:
Here you may enter the number of the connected device. This number will be used to identify the device when messages come in. This number has no effect on the number that will be transmitted when sending messages.

PIN:
Here you can change the PIN (Personal Identification Number) for the SIM Card in the device on the specified port. After clicking the Change PIN button the Change PIN dialog box appears.

Query PIN:
Under Query PIN you can determine whether or not message master SMS SDK GSM/PCS should query the PIN (Personal Identification Number) for the SIM Card. In most cases you should activate this query because otherwise the device cannot be used. However, some devices do not support the command for querying the PIN. In these cases you can deactivate the query. This is possible especially for mobile phones with PCMCIA-Cards.



Name:
The Name of the service.

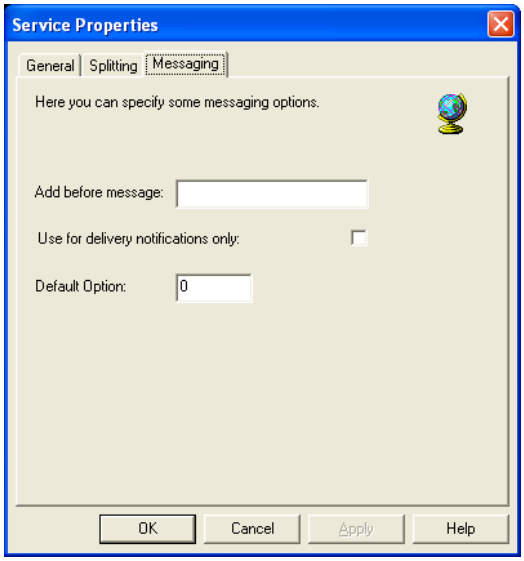
Port:
The port that where the device is connected.

Default Contrycode:
The default countrycode. (May be empty.)

Default Prefix:
The default prefix. (May be empty.)

Resend Attempts:
Number of attempts to resend the message in case of an error.

Add before message:
Here you can enter a text that should be inserted before the message text of each message.



Use for delivery notifications only:
Here you can specify that the string above should be inserted only if the software requests a Notification.

Note: Some carriers provide delivery notifications if the message begins with a special string, e.g. ”*N#”. Here you can activate this option by automatically insert such a string before the message text. Also, please, note that the maximum number of characters for the message text could decrease accordingly.

Default Option
Use this value to define the default options for sending a message.
Possible values are the following:
0: No further options
2: Enable GSM delivery notifications
4: Direct display (the message immediately appears on the display of the mobile phone)
8: Enable 8bit messaging (the message text should be in hexadecimal format in this case)
16: Enable 8bit messaging with UDH (e.g. for sending logos and ringing tones)
64: UNICODE (UCS2) encoding

128: EMS (Enhances Messaging Service) messages (7bit messages with UDH)

Escalation Control

Escalation provides accountability for delivery of events by requiring event recipients to reply within a specified amount of time. Failure to respond causes the events to be escalated and sent to the next level. An optional close timer escalates the event even though a reply may have been received and will continue to escalate it until the event has been closed.

Escalation replies can be received by email or web page. The web interface requires the installation of either Apache 2.0 or Microsoft IIS on the same PC as PMPro. To enable email reply, create an account that PMPro can use to receive emails. This is the email account that users will reply to after they have received an event. It is used only for receiving replies, not sending events.

Disabled for now

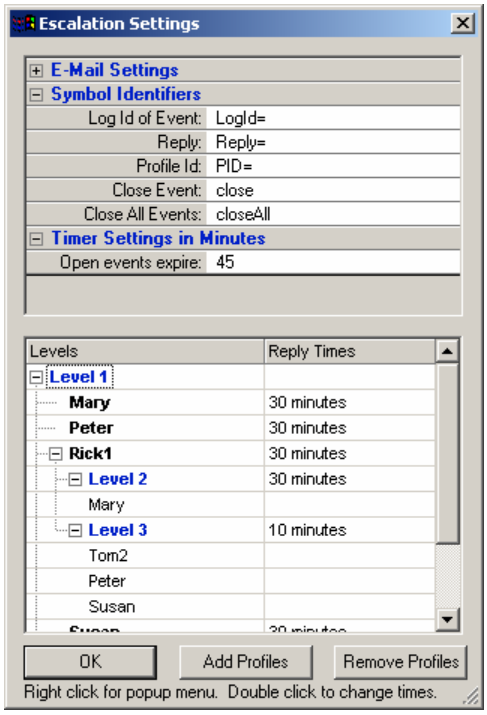


Figure 4.12: Escalation Settings

Configuring Email Replies

Click on the + symbol in front of the E-Mail Settings to expand the following fields:

- **E-Mail Type**: Select the mailbox type (POP3 or IMAP)
- **Server**: Enter the IP address or server name PMPro downloads the email replies from
- **Account Name**: Enter the account name PMPro logs in to the email service with
- **Password**: Enter the password assigned to the account

Leave the Server field empty to disable the PMPro email checking feature.

Symbol Identifiers

Symbols tell PMPro what event is being replied to, who is replying, what to do with the event, and more. Symbols have default values but they can be changed.

Symbols are only used for email replies. Skip this part when only using web replies or phone/fax replies.

Disabled for now

- **Log Id of Event**: The number following this symbol is used to locate the event by the log id. The default is “LogId=”. For example, if “LogId=4356” is placed in the email reply PMPro knows that the reply pertains to the event with the log ID of 4356.
- **Reply**: All text following this symbol is saved as the reply and can only be viewed in the web report. The default is “Reply=”. For example, if the reply message body is: “System is down. Reply=I’m working on this right now”, the saved reply is “I’m working on this right now”. If no reply symbol is found the whole reply message is saved.
- **Profile Id**: The number following this symbol tells PMPro who is replying. The default is “PID=”. For example, if PMPro finds the symbol PID=114 it looks up the profile with the ID of 114. The best use for “Log Id” and “Profile Id” is to assign these two symbols inside the email courier’s subject line. The default for the subject line is “%alarmname%”. Edit the email courier and change the subject line to: “%alarmname% pid=%profiled% logid=%logid%”
  The variables between the “%” signs are PMPro variables. See all of the possible variables by right-clicking on the email subject line. By setting the subject line this way, the receiver of the emailed event can reply without typing any of the event specs since the email subject already has the information PMPro needs.
- **Close Event**: If the close feature is enabled PMPro closes the event specified by the Log Id symbol when it finds this symbol. The event will not be escalated when the close timer has expired.
- **Close All Events**: If the close feature is enabled PMPro closes ALL events that have been sent to this profile/personnel when it finds this symbol. Useful when many events have been sent to a specific personnel. Keep in mind though that if this option is enabled (making the field empty disables close all) it is not possible to ensure that the profile has indeed read and/or received all of those events.

Timer Settings in Minutes

“Open events expire” timer: The time is specified in minutes and defaults to 45. Set to zero to disable the close feature. The close timer starts as soon as the event has been sent out. After someone has replied to an event it can still be escalated if the close timer expires before someone has closed it. Closing the event can be done via the web page or by sending the close symbol that has been assigned to the Close Event field in the email reply.

The close feature provides the ability to make PMPro similar to a trouble ticket solution. See how long it took for the issue to be resolved from the web reports. See the Web Interface section later in this doc for more information.

Disabled for now

Assigning Escalation Levels and Reply Times

The lower half of the Escalation Settings dialog is for creating and assigning escalation levels. All profiles/personnel are at level 1. Escalation will only be enabled for those profiles that have levels assigned to them. If a profile has escalation levels assigned, any event sent to that profile is escalated if

a) No one replies before the reply timer expires or
b) if close is enabled and the event is not closed before the close timer expires.

To assign a new level, right-click a Level 1 profile, then select, “Insert Next Level”.

To assign profiles to the new level, right-click the new level, then select “Assign Profiles”. A list of profiles that have not already been assigned to that level 1 profile appear. Double-click on the profiles to assign to that level. Multiple profiles per level are possible as well as an unlimited number of levels.

To change the Reply time, double-click on the time and enter the new time in minutes. Each level (other than 1) can have its own time. Empty levels are not allowed

Escalate on Delivery Failure

If a profile has a courier delivery failure, it has exhausted all fallback assigned couriers, and it has escalation enabled, it will escalate the event base on courier delivery failure.

Web Event Viewer

Web Interface

The web interface uses the Microsoft ISAPI calls, allowing the use of any web server that supports ISAPI. The two tested and approved by Atlantis Software are Apache 2.0.48 (download from http://www.apache.org), and Microsoft IIS (included with Windows). Apache 1.3 is not supported.

The web interface provides the ability to view the event/alarm log in any browser as well as the ability to reply and close escalated events.

Disabled for now

1) Install a supported web server on the PC running NotificationWorks PMPro.
2) Edit the eventmgr.ini located in the Windows directory and add the following to the PMPro section:
   [PMPro24]
   WebTemplates = c:\Program Files\NotificationWorks\web
   PMProRemoteLocation = c:\Program Files\NotificationWorks\web
   WebSessionMaxMin = 10
   EscalationLoopWaitTime = 30

WebTemplates:
Set to the directory location where the PMPro html files are located
PMProRemoteLocation:
This is the directory/folder location of the PMProRemote.dll file
WebSessionMaxMin:
This is the maximum minutes before the user's web session times out
EscalationLoopWaitTime:
This is how many seconds PMPro waits before each email and escalation check. Set this to zero to disable the escalation feature.

To Use Microsoft IIS

First off, make sure the the “/” characters have been removed from the following two files located in the NotificationWorks/web folder:
Edit “eventFilter.html” and “logon.html”. Remove the ”/” character from all src=”/something” entries. For example, change src="/calendar.js" to src="calendar.js”

Configure the virtual directory:
For IIS v4.x and v5.x

1. Run the Internet Services Manager by navigating to
   Start > Settings > Control Panel > Administrative Tools > Internet Services Manager
2. Expend the tree then right click on the "Default Web Site" and select New > Virtual directory. The Virtual Directory Creation Wizard appears
3. Click “Next”, then enter a name for the virtual path. For example, if you enter the name “NotificationWorks” and if you installed NotificationWorks using the default path then the URL to access the PMProRemote web features would be http://127.0.0.1/NotificationWorks/pmproremote.dll
   Click “Next” when finished
4. Enter the path of the directory the PMPro web files reside in and click “Next”. The default is: c:\Program Files\NotificationWorks\Web
5. From the Permissions screen enable “Read”, “Run”, and “Execute”, then click “Next” and “Close.”
6. Right-click the newly created Virtual Directory and select “Properties”. For IIS 5.0: Change the “Application Protection” to “High (Isolated)”.

Disabled for now

For IIS v6.0 on Windows 2003

IIS v6.0 2003 Server

1. First we need to change the security rights for the NotificationWorks web folder so open the folder properties on the NotificationWorks Web folder e.g.:
   \Program Files\NotificationWorks\web
   Click on the "Security" tab and add "Full Control" to the user called "Users"
2. Open Internet Information Services manager
   Select the "Application Pools"
   Right click on "Application Pools" then select New->Application Pool. Now from the "Add New Application Pool" dialog, enter "NotificationWorks Pool" into the field.
   Select the "Use existing application pool as template"
   Click the OK button.
3. Select the new Pool you just created, "NotificationWorks Pool" and right click then select properties.
   From the properties dialog click the "Identity" tab, then select the "Local System" option for the "Predefined" security account.
4. From the Internet Information Services manager select "Default Web Site" (under the "Web Sites" branch) then Right click on the "Default Web Site" and select New->Virtual Directory
   Enter NotificationWorks (or some other name that you want to use to access the web page) into the Alias field in the "Virtual Directory Create Wizard" then click the next button. Now enter the path to the NotificationWorks web folder then click next e.g. c:\program files\NotificationWorks\web Select the following Access Permissions, Read, Execute, then click next button.
5. Right click on the NotificationWorks entry you just created and select Properties From the Properties dialog, "Virtual Directory" tab, change the Application Pool to be the "NotificationWorks Pool" then click Apply.
6. Click the "Documents" tab and add pmproremote.dll to the default content page, this provides the ability not to have to add the prmproremote.dll to the URL entry when accessing the web site.
7. Now LEFT click on the "Web Service Extensions", and select the "All Unknown ISAPI Extensions" then click the "Allow" button.

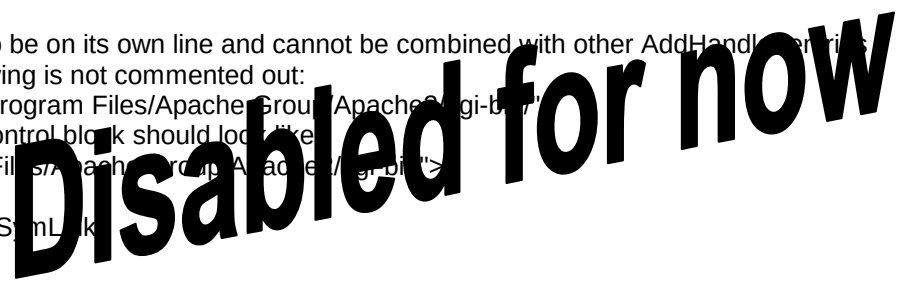
Then to access the web page using the above entries and step 6 above open a browser window and enter:
http://127.0.0.1/NotificationWorks/
or if not used step 6 above then you will have to also enter the dll name:
http://127.0.0.1/NotificationWorks/pmproremote.dll

To Use Apache version 2.0.48 or Higher

Assuming that Apache was installed to the directory
C:/Program Files/Apache Group/Apache2

Make the following changes to the file httpd.conf:

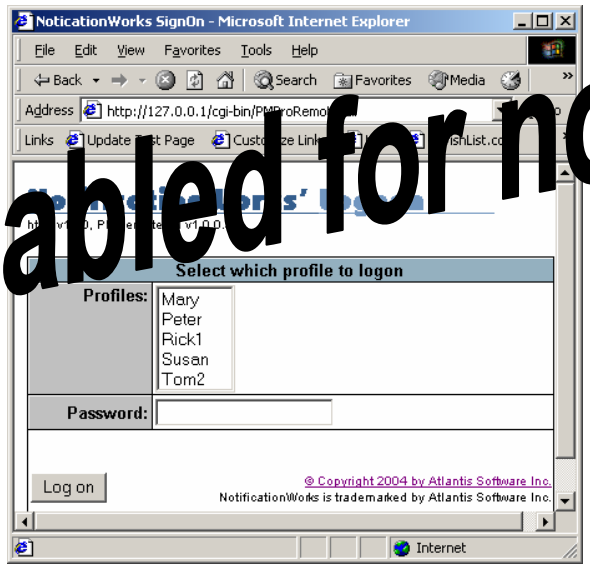
1. Add the following into the AddHandler section:
   AddHandler isapi-isa .dll
   Note: This entry needs to be on its own line and cannot be combined with other AddHandler entries.
2. Make sure that the following is not commented out:
   ScriptAlias /cgi-bin/ "C:/Program Files/Apache Group/Apache2/cgi-bin/"
3. The CGI-BIN directory control block should look like:
   <Directory "C:/Program Files/Apache Group/Apache2/cgi-bin">
   AllowOverride None
   Options ExecCGI FollowSymLinks
   Order allow,deny
   Allow from all
   </Directory>
4. Add the following below the above block:
   ISAPIAppendLogToErrors on
5. Do NOT enable the ISAPICacheFile for our DLL, it crashes the system.
6. Copy PMProRemote.dll into C:/Program Files/Apache Group/Apache2/cgi-bin/
7. Copy the remaining the support files into C:\Program Files\Apache Group\Apache2\htdocs
8. Edit “eventFilter.html” and “logon.html”. Add the ‘”/” character to all src=”/something” entries. For example, change src="calendar.js" to src="/calendar.js”



Open a browser window and enter the IP address of the PC running the web server along with the virtual directory <name>/pmproremote.dll
For example:
http://127.0.0.1/cgi-bin/pmproremote.dll

Web Pages

The start page is the logon page. Select the profile to log on as and enter the password (if one was assigned in PMPro). The password is encrypted before it is sent to the web server. After logon is completed a session is established that expires when the WebSessionMaxMin is reached as described earlier.



Disabled for now

Figure 4.13: NotificationWorks Logon Page

After clicking “Log On” the Menu page appears. Click on the “Event Viewer” option to go to the Even Viewer filter page and select what events to view.

Select multiple Profiles by holding down the Ctrl key while clicking on profiles and multiple escalation flags. Clicking the calendar icon displays a popup calendar to select dates.

To select all, disregard this page and click “Get Events” to see all of PMPro’s events.

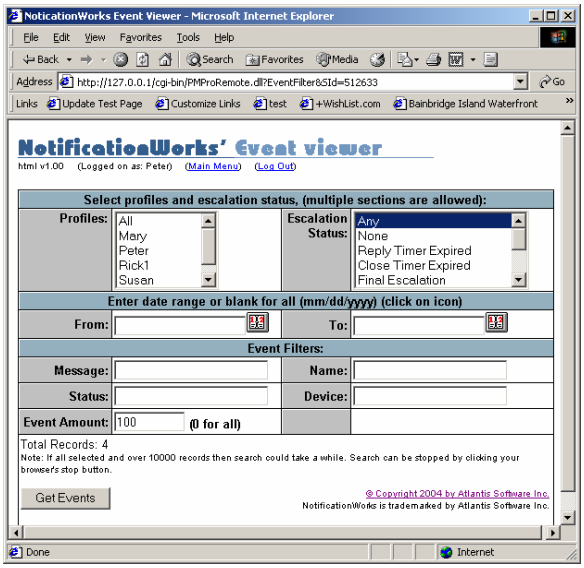


Figure 4.14: NotificationWorks Event Viewer Filter Page

The Escalation Report refreshes every 5 seconds. See the “Changing Web Refresh Interval” section for how to change the refresh interval.

If the Escalation Report Event ID has a link clicking that link brings up the Event Details report. This report shows all activity for that event. Use this page also to enter information, view replies, and close events.

Edit Assignments Page

The “Edit Assignments” page is used to assign alarms and time schedules for profiles (personnel and templates):

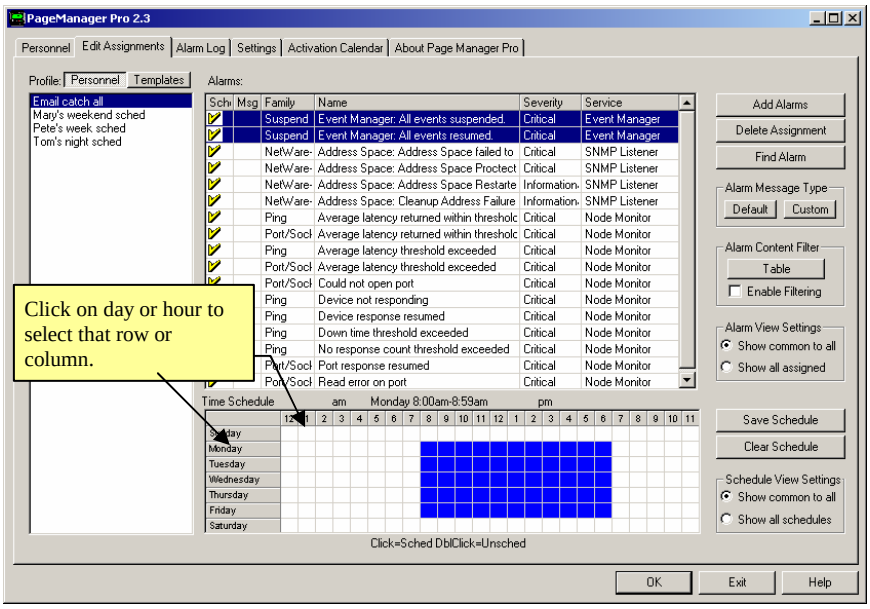


Figure 4.15: Edit Assignments Page

Profile Personnel / Template

The profile list box displays either personnel or templates depending on which radio button below the box is selected.

Alarms

The “Alarms” table shows the list of alarms that have been assigned to the selected personnel and has the following 4 columns:

“**Schd**” - A check indicates that this alarm has been scheduled
“**Msg**” - A doc icon indicates that this alarm uses custom text
“**Family**” - This is the name of the family of alarms it comes from
“**Alarm Name**” - This is the name of alarm not the alarm message
“**Severity**” - The severity of this alarm
“**Service**” – The service this alarm is from

Note: All 5 columns can be resized with the mouse. Alternatively, double-clicking the bar between columns auto resizes them. Select multiple non-adjacent alarms by holding down the Ctrl key while left-clicking. Select adjacent alarms by holding down the Shift key while left-clicking.

Time Schedule

The “Time Schedule” table shows when the selected personnel are available to receive the selected alarm. This schedule is divided in 7 day 24 hour time blocks. To select individual time blocks, click the desired time block. To select a group of time blocks, hold down the left mouse button and drag through the group of desired time blocks. Double-clicking on an assigned block removes the selection.

Special commands:

To quickly select the entire table, click in the top left corner of the timetable. Double-click to clear the timetable.
To select a whole day, click the name of the day. Double-click to clear the day.
To select an hour for all 7 days, click the hour. Double-click to clear.

Note: Remember to click “Save Schedule” after making modifications; otherwise all changes are lost.

Add Alarms

Clicking this button brings up the alarm list. The list shows the remaining unassigned alarms for the selected personnel.

1. Select one or more in the personnel list

2. Click “Add Alarms”
3. Add the desired alarms. Click “OK” when finished
4. Sort this list by double-clicking on the column name.

Sort most lists in PMPro 2.5 by clicking or double-clicking on the name of the column.

Delete Assignment

This deletes the selected alarm(s) assignments from the selected personnel.

Find Alarm

Find a particular alarm quickly by using this option. It searches through the alarm names while typing. This option is also available from the “Add Alarm” list.

Alarm Message Type

By default, PMPro 2.5 sends the alarm message that is received. However, it is possible to send a custom message. Select the alarms to change then click “Custom”. A document icon appears next to the selected alarms indicating that they are now set to send the assigned customized message.

Configure what message to send from the “Settings” page in the “Customize Text” section. By default, numbers have been assigned to each alarm for easier numeric pager support.

Alarm Content Filter

Set up an alarm content filter for each personnel. This is useful to include or exclude specific alarms based on their message content. To enable this feature, click the table button, then enter the text to search for into either the “Include” or “Exclude” column. Each line (row) is considered a “or” condition. To have “and” conditions, separate the praises with the “&” and to have spaces or whole praises then bracket them with quotes, for example:
“system down “ & interface
The above with be true if the praise “system down “ is found along with the word interface.

You can have multiple personnel selected when added or deleting. The # column shows the order of precedence, which can be changed by selecting the order and clicking either the up or down buttons. Once again, multiple rows can also be selected when making precedence changes.

To sort, just click on any of the column names.
To edit, double click in the field that you want to change and you will then be able to make any changes.

If have a need to have a filter to affect only specific alarms then you could just create another personnel (profile) and assign those specific alarms and create a filter for it.

Note: The window can be resized.
Note: Remember to enable the “Enable Filtering” option from the “Edit Assignments” page.
Note: The filter will affect ALL alarms assigned to these personnel or global to that personnel.

Save Schedule

Click on this button to save any schedule changes.

Clear Schedule

This provides a quick way of clearing time schedules. Clear an individual or group of alarm schedules. To save the cleared schedule, click “Save Schedule”.

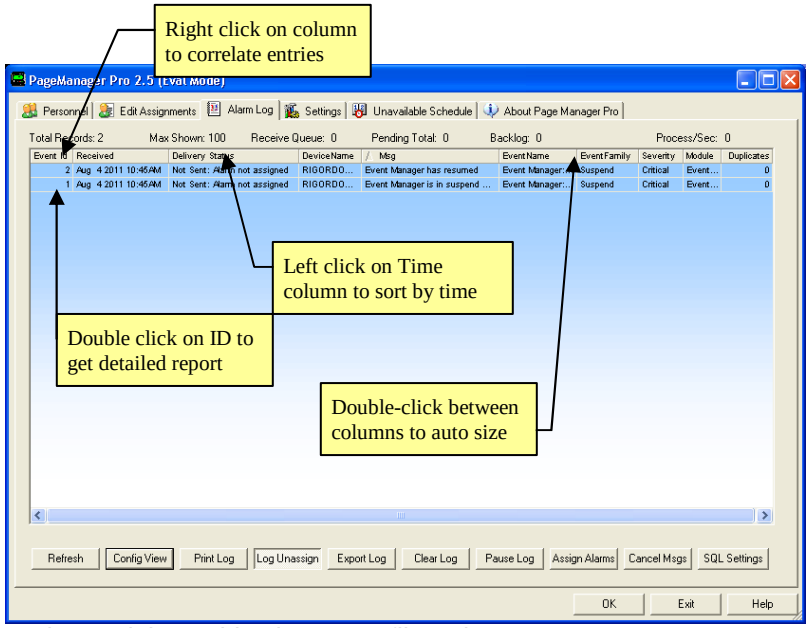
View Settings

Allows you to see what alarms or schedules the selected personnel have in common.

Alarm Log Page

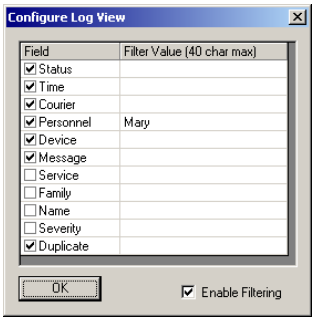
This page shows the alarms that have been sent by PMPro 2.5. This page provides the ability to create greatly customizable reports. By default, only those alarms that have been assigned are saved. To save all alarms PMPro 2.5 receives check the “Log Unassigned Alarms” option. Be aware that doing so increases the size and the growth speed of the log. This screen only reads into memory what is currently being shown. The size of the log files does not affect the memory of the system. Note: Double clicking on ANY item text will give you a report for that item.

Alarm Log Columns



- **Event Id** – The ID for this specific event. Double click on the ID for a detailed report showing where the event message was sent.
- **Recevied** – Time alarm was received.
- **Delivery Status -** Shows the delivery status of the alarm. If any errors occurred in delivery the error message appears here.
- **DeviceName –** Device alarm is about.
- **Msg** – The alarm message
- **EventName –** Alarm/event name
- **EventFamily –** The alarm/event family
- **Severity** – Severity level of the alarm
- **Module –** The NotificationWorks module that received and forward the alarm/event to PMPro.
- **Duplicate –** If the filter duplicate feature is enabled from the “Settings” page this will show the total times this alarm was filtered.

Config View



Select which columns are displayed in the log, and configure filters to show only matching entries. **Note:** The filter is applied only to existing entries. New entries show as normal. Remove the check from the fields not to be displayed.

To show only those entries that contain specific text, enter the text into the Field’s Filter value field. It is case insensitive.
Select the “Enable Filtering” option to turn on filtering.

Print Log

The print feature provides options to change the header, footer, and the fonts used. Also provides a preview mode, which allows for multiple view types as well as printer configuration.

Log Unassigned - If depressed then even alarms/events that have not been assigned will be saved into the log.

Export Log - Exports the alarm log to a delimited file, which can then be imported into a report.

Clear Log - Clears the alarm log.

Pause Log - Good thing to do are searching the log.

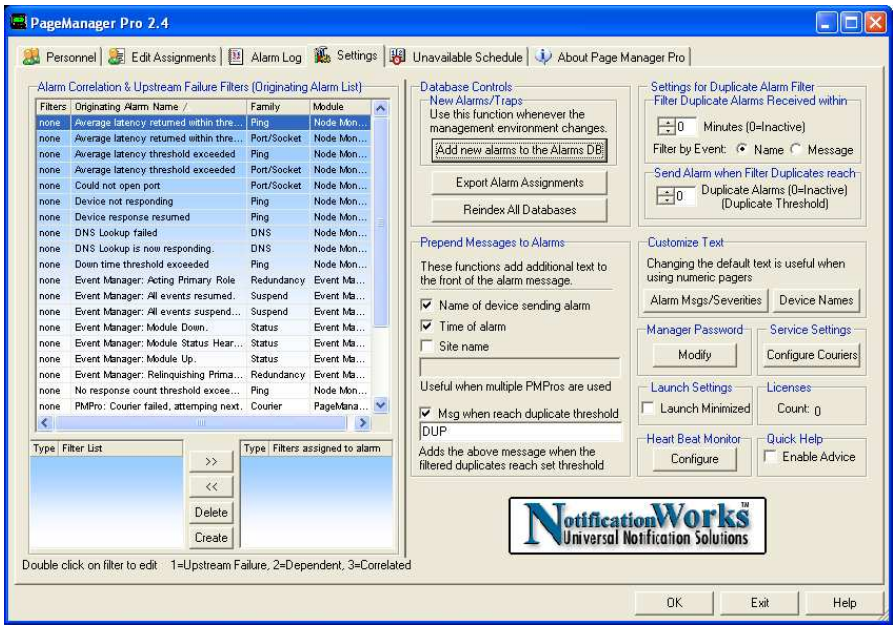
Cancel Msgs - Cancels any pending or processing alarms.

SQL Settings

This provides you will the ability to create your own log view using SQL commands. After the “Load SQL Settings” dialog appears, click the New button, then double click in the name field and give your view a name, then click the “Edit SQL” to enter your SQL commands. Please look at our existing tables and views to get the names of what you might want to use.

Settings Page

The “Settings” page provides the ability to configure many of PMPro’s settings. The left side of the Settings page is the Alarm correlation/Downstream filtering section. Notices the two panels on the bottom left side. The left panel will show and filters not assigned to the selected alarm, the right showing those that are assigned. Read the “Alarm Correlation & Downstream Filtering” for more information about filters. The right side shows PMPro 2.5 general settings.



Add New Alarms to Database

Clicking this button synchronizes any new alarms that were added to the management console with PMPro. This should be done when changing or adding to the management environment after installing PMPro. Note that alarms from services not running will not be added.

Deleting Alarms from PMPro

Alarms/events can be removed from PMPro simply by selecting the alarm from the left side of the “Settings Page” then pressing the “Delete” key.
Note: This will remove the alarm from PMPro and from all profiles and filters it is assigned to.

Launch PMPro Minimized

Checking the “Launch Minimized” checkbox in the “Launching Settings” group will cause PMPro to be minimized after it launches. Unchecking this box will cause PMPro to launch in full screen mode.

Prepend Messages to alarm

This section provides the ability to add additional information to the beginning of the alarm message.

Filter out Duplicate Alarms Received within

A filter can be set to prevent the same alarm from being sent multiple times. This filters out any alarms that have already been sent within the set number of minutes. For instance, if “Minutes” is set to 5 and PMPro receives the alarm “NLM Unloaded from server SALES” it checks the alarm log to see if this alarm has already been sent within the last 5 minutes. If not then it will be sent otherwise the alarm is ignored. Setting the “Minutes” to 0 deactivates this filter.

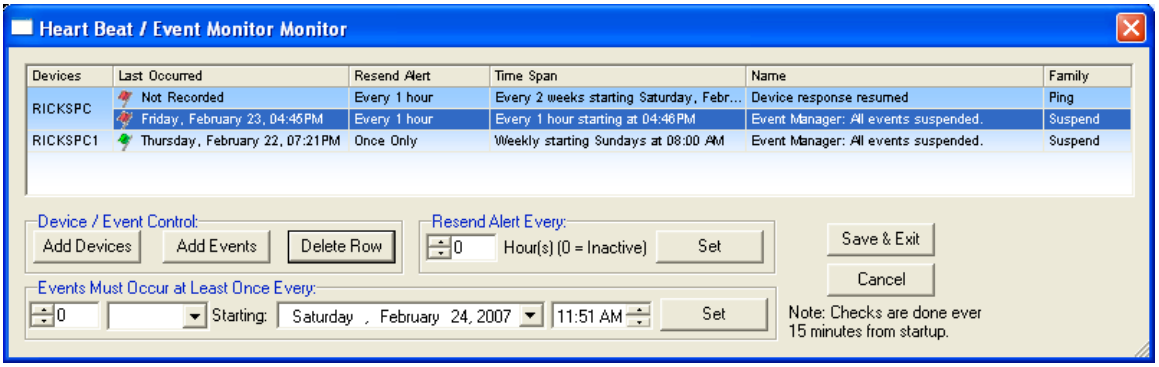
This filter can be used on either the event name or the event message. Using the event name is useful when the message contains text that changes e.g. time stamp, etc. This filter is currently global and applies to all events. It will be assignable to specific events and profiles in a future release of PMPro.

Send Alarm when Filtered Duplicates reach

If the duplicate filter is active it is possible to be notified if a certain amount of alarms have been filter out on a per alarm & server basis. Setting the “Duplicate Alarms” counter to a number other than zero activates this option. For example, the counter is set to 8. If the duplicate filter filters out 8 “NLM unloaded” alarms from a specific server PMPro sends out an alarm. This alarm states that the alarm “NLM unloaded” has reached this filtered threshold. PMPro keeps track of how many times each alarm has been filtered out.

Heart Beat Monitor

The Heart Beat / Event Monitor feature will monitor specific alerts coming from specific devices that have to occur within a specified time span. If not meeting the time span then PMPro will issue an alert describing the situation.
So, if you have applications and/or devices that send out "Heart Beats" on a scheduled bases, you no longer have to personally arrange to receive them, you can now have PMPro automatically monitor them and let you know if they fail to meet their configured schedule.
The events configured in this Monitor do not need to be assigned to any profile nor do they need be saved in the PMPro's alarm log. The monitor listens to ALL events that are received by PMPro.
Clicking on the "Configure" button will bring up the following dialog:



In the "Last Occurred" column a flag will be shown. The colors of the flags show the following:
Red - means that the event has not occurred within the configured time span.
Green – means that the event is in good standing, has occurred within the time span.
White – has not be completed configure yet.

The status is not "Real Time", meaning that the flags will not change while this dialog is up. You must close then reopen this dialog to reflect any events that may or may not have occurred within scheduled time spans.

To configure the Monitor:

1) Click the "Add Devices" button then from the "Device Manager" dialog, left select the desired devices then click and hold the right mouse button and drag and drop the devices on to the Monitor screen.
2) Select the devices that are now shown in the Monitor dialog and click the "Add Events" button. Select the events that you want to have monitored then click the "Assign Events" button then click the "Close" button when done.
3) Select one or more events on the Monitor dialog then using the "Resend Alert Every" control, choose how often you want PMPro to send out it's "PMPro: Event Monitor, did not received scheduled event", alert. If set to zero then PMPro will send the alert only once. Click the "Set" button to set the time.
4) Now use the "Events Must Occur at Least Once Every" control and select the time span for how long the Monitor wait for the event and when the time span begins. Then click the "Set" button to assign the setting to the selected events.

After you have anything set to your liking click the Monitor's "Save & Exit" button.
Note: This dialog can be resized to fit you viewing options just by dragging the dialog's edges.

Alarm Correlation & Downstream Filtering

These controls provide the ability to create three alarm-filtering types: Upstream Failure, Dependent, and Correlation. There are two places with alarms are “Attached” to the filters. When assigning filters to alarms from the “Settings” page (read the section under the “Settings Page” in the section above) these are called, Originating alarms/events, alarms assigned “inside” the filter are called, correlated alarms.

Filter precedence is “Upstream Failure”, “Dependent”, and then “Correlated”.

Upstream Failure: This filter will verified if the alarm is valid (and not due to the inability to reach the device that the alarm is about) by sending a (ICMP) ping to the affected device’s parent (the device “upstream/above”). If no response is received then the originating alarm (the alarm this filter has been assigned to) is nullified, then for the next (n) minutes, any additional alarms matching the entries in the “Nullify Alarm List” (the correlated list) are also nullified having the same originating affected device. You don’t have to have additional alarms in this list if not needed.
This filter is very useful if you receive “device down” alarms from devices that are below a router but it’s really the router that is down and not the devices below it.
Note: Read the “Managing the Devices” section for more information about assigning parents to devices.

Dependent: Used to cancel a received alarm when a dependent alarm has or has not happened yet (depending on the found/not found selection). For example: Sometimes HP OpenView Network Node Manager sends a “Node Up” alarm when started, resulting in a barrage of “Node Up” alarms even though they were never down. For this example to create a dependent filter that says, “If the “Node Up” alarm is received AND a “Node Down” alarm was not received within the past 5 minutes then cancel the “Node Up” alarm”. Then assign the “Node Down” alarm inside the filter list then assign this filter to the “Originating” alarm called, “Node Down” from the PMPro’s Settings page.

Correlation: This filter type is used to cancel alarms that are tied to or paired with another alarm. For example, cancel a “node down” alarm if a “node resumed” alarm is received within 5 minutes of receiving the “node down” alarm.
To create a filter, click “Create Filter”.

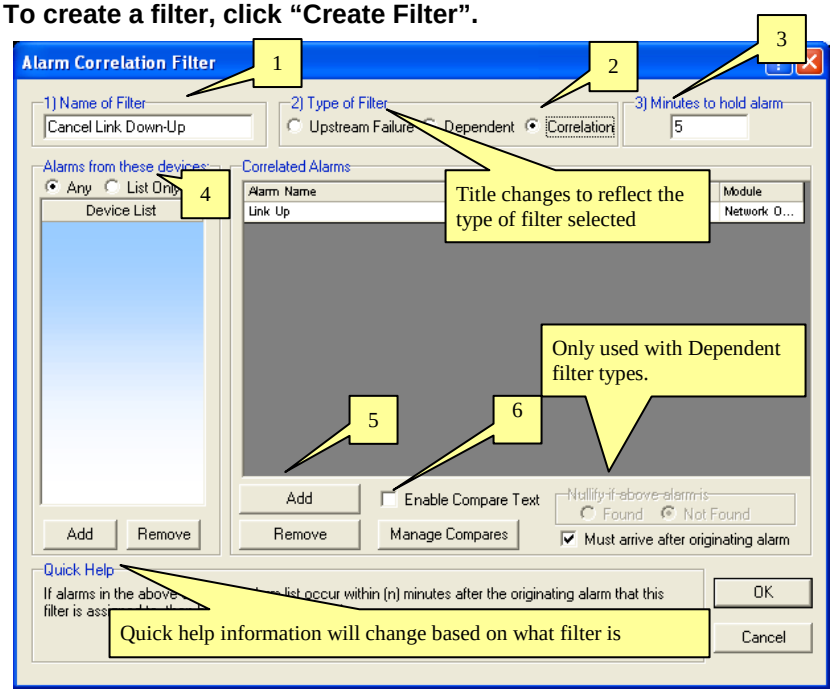
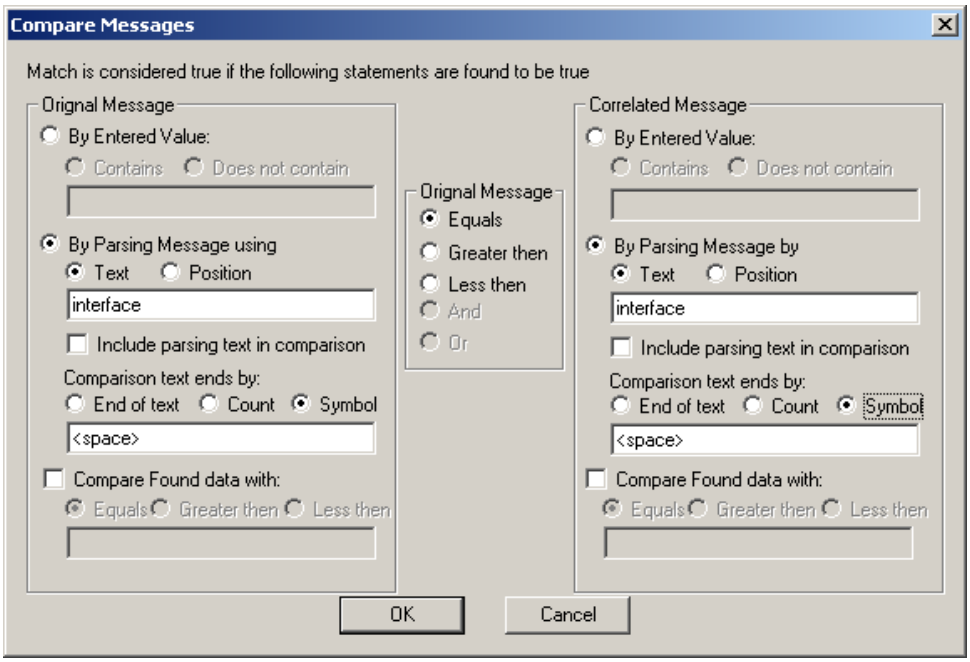


Figure 4.16: Alarm Correlation Filter

1) Enter a name for the filter
2) Select the filter type.
3) Enter the number of minutes to wait before sending the originating alarm. Filters are assigned to originating alarms. Alarms shown in the filter’s “Correlated Alarm” list are correlating alarms, not originating alarms.
4) You can limit the filter to be only applied to specific devices, the default is “Any”.
5) Add the correlating alarms here. For correlated filter types the alarm in the correlating list is normally different from the originating alarm the filter is attached to. For example, add the “Link Up” alarm to the correlated list. Save the filter then assign this filter to the originating alarm called “Link Down”.
6) Enable or Disable the Compare Text function based on your needs. Most of the time you will disable this option since most events are matched up by their event names. The “Enable Compare Text” option provides the ability for PMPro to search the original and correlated received events for a specific value and compare those values (text or numeric) using equals, greater then or less then, logic. This feature becomes VERY useful when you need to compare certain parts of the event text. For instances, the “Link Down” and “Link Up” events contain the interface names, so matching the interface names become very important since you could receive more then one “link down” event from a device that has more then one interface.



The options on the “Compare Messages” feature are:

- **By Entered Value** - Searches the event text for the entered value, if the “Contains” option is selected and the value is found then it will return true. If the “Does not contain” option is selected and the value is not found then it will return true.
- **By Parsing Message using** – Use this option when the value in the event is not static. A good example is the “Link Down” and “Link Up” event. The message would be, “Interface Serial2/1/5:0 Link Up Trap”. The part that we want is “Serial2/1/5:0” so we choose the “Text” option since the text “Interface” never changes. The function will search for the word “interface” (not case dependant) and if found it would then skip any spaces and find the next text part, “Serial2/1/5:0”. Since the first part of the message up to the text “Serial2/1/5:0” does not change we could also us the “Position” option and put the number 10 in the text field (which is the count of characters where this text starts) and we would still get the “Serial2/1/5:0” value. The downside of using the “Position” option is that it would always return true, so using the “Text” option ensures that you are finding the information that you need. How long the found text is will depend on what option is selected in the “Comparison text ends by” option.
- **Include parsing text in comparison** – This option is used with the “By Parsing Message using” option when parsing by “Text”. Using the example above, if this option is enabled the return value would be “Interface Serial2/1/5:0”, notice that it “Includes” the text entered into the field IF the text is found. Not sure when anyone would ever use this option but it is here anyway
- **Comparison text ends by** – This is how you inform the “By Parsing Message using” option to end the found text. We will use the above “Link Up” event message has an example:
  “**End of text**” - means to the end of the message, e.g. “Serial2/1/5:0 Link Up Trap”
  ”**Count**” - Set to length of the value you are looking for, e.g. 18 would return: “Serial2/1/5:0 Link”
  ”**Symbol**” – Set to any text that would end the found text, if set to a space, e.g. “Serial2/1/5:0”
  Note: When space bar is pressed the space character will be replaced with the word “<space>”. This makes it easier to know that you have a space entered into the field.
- **Compare Found data with** – This option provides the ability to compare the found text will a static value that you enter into this field. We are not sure when you would ever use this option because most of the time you would want to compare the found data in the “Originating” event message with the found data in the “Correlated” event message. But we knew that if we did not have this feature that someone would ask for it.

The logic in the middle of the above dialog is used for comparing the values of the “Originating Message” with the “Correlated Message”. So if you have the “And” logic selected then both sides must be true for the two events to be cancelled, (nullified). If “Equals” is selected then the value found in the “Originating Message” must be the same as the value found in the “Correlated Message”, etc…

As you can see this feature is very powerful providing all kinds of filtering abilities.

Activation Calendar Page

PMPro 2.5 activation calendar provides the ability to make someone unavailable on a specific day and time and assign other personnel to provide coverage for the unavailable person.

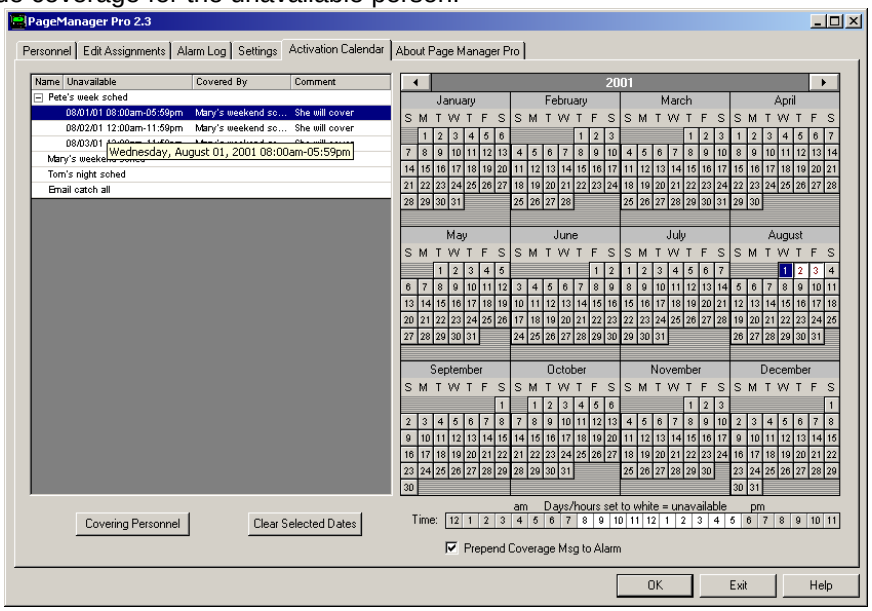


Figure 4.17: Activation Calendar

To schedule unavailable dates:

1) Select personnel
2) Click the dates to make unavailable, then click “Clear Selected dates”
3) By default, the unavailable time is the entire day 12:00am to 11:59pm. To change this use the time bar and left-click on the start time then drag to the desired end time.
4) To assign personnel to provide coverage, click “Covering Personnel” then select the personnel to provide coverage. Add a comment if desired then click “OK.”

If the option “Prepend Coverage Msg to Alarm” is enabled, the person receiving the covered alarm knows who they are covering for. The message looks like this: “[Cover for Pete] System Atlantis is down”

Previous 2.3 Features

- New database engine
- Database ODBC Compatible
- Database FoxPro compatible
- Add or remove node assignments from multiple selected personnel
- Full multiple node assignment management
- Cloning Personnel now includes the ability to add, replace or remove the Alarm or node assignments from the target personnel
- Alarm list now allows selecting multiple, non-adjacent alarms
- Can now see assigned alarms that multiple personnel have in common and their common time schedules
- Can now assign someone else to take over personnel's assignment when they are not active for that day
- Personnel names can now be renamed on the fly
- PMPro is now about 10 times quicker
- Alarm log filtering
- Alarm log view can be changed
- Hundreds of files less

New 2.5 Features

- Escalation support via email or web verification
- Heart Beat / Event Monitoring
- Courier failure recovery
- Wireless Modem support
- HTTP courier delivery support via web posting

- SNPP (simple network paging protocol) support
- Text Terminals using modem and XML scripting
- Customizable notification messages
- Event escalation reports
- Screen is now resizable
- Profile creation wizard
- Profile problem indicator
- Notification on courier failures
- Device group support
- Clone from templates to profiles and back
- Upstream Failure Verification event filters
- Event correlation filters
- Event dependency filters
- Event Message Content filters
- Multiple unavailable time frames per day now supported

File Layout

After the installation has been completed, a new directory "PMPro24" appears in the NotificationWorks directory. Most of PMPro's files are kept there. The following is a list of files that are installed or created at runtime:

File	Purpose	Location
eventman.ini	NotificationWorks settings file	C:\Windows or C:\WinNT
messagemaster.dll	Pager services library	NotificationWorks\shared
*.dbf	NotificationWorks databases	PMPro24\database
*.cdx	NotificationWorks databases indexes	PMPro24\database
Escalation.cfg	Escalation configuration file	PMPro24\database
Excludes.ini	Alarm message content filter	Pmpro24
Includes.ini	Alarm message content filter	Pmpro24
Pmpro24.dat	PMPro's settings	Pmpro24
Couriers.ini	Courier manager settings	PMPro24
CustomDeviceNames.ini	Custom device names	PMPro24
Exclude.ini	Message content filter	PMPro24
Include.ini	Message content filter	PMPro24
LogStatusMsgs.*	Static messages for log status	PMPro24
Pageman.exe	PMPro24 program	PMPro24
DosCommand.dll	Dos command courier	PMPro24
SMTP.dll	Email courier	PMPro24
SNPP.dll	SNPP courier	PMPro24
TAP_UCP.dll	Tap/Ucp courier	PMPro24
WebHttp.dll	Web Form courier	PMPro24

Modifying Date and Time Format

* Date and Time strings are configurable using the Ansi C api strftime() flags. Default for date is %x representation for current locale date. Default for time is %X representation for current locale time. To change these defaults add an entry in the PMPro24 section in the EventMan.ini file located in the Windows directory. The entries are:

DateFormat=%x
TimeFormat=%X

Change %x to any of flags below:

%a	Abbreviated weekday name
%A	Full weekday name
%b	Abbreviated month name
%B	Full month name
%c	Date and time representation appropriate for locale
%d	Day of month as decimal number (01 – 31)
%H	Hour in 24-hour format (00 – 23)
%I	Hour in 12-hour format (01 – 12)
%j	Day of year as decimal number (001 – 366)
%m	Month as decimal number (01 – 12)
%M	Minute as decimal number (00 – 59)
%p	Current locale's A.M./P.M. indicator for 12-hour clock
%S	Second as decimal number (00 – 59)

%U	Week of year as decimal number, with Sunday as first day of week (00 – 53)
%w	Weekday as decimal number (0 – 6; Sunday is 0)
%W	Week of year as decimal number, with Monday as first day of week (00 – 53)
%x	Date representation for current locale
%X	Time representation for current locale
%y	Year without century, as decimal number (00 – 99)
%Y	Year with century, as decimal number
%z, **%Z**	Time-zone name or abbreviation; no characters if time zone is unknown

Troubleshooting:

Getting Help

All forwarded alarms are logged into the Alarm Log page along with their status codes. For help see “Contacting Atlantis Software” in the “Troubleshooting” section of this user guide.

Database issues

Click “Reindex All Databases” from the PMPro’s setting tab. If that does not resolve the issue shut down PMPro and delete all cdx files in the PMPro24\database directory. Start PMPro again. It rebuilds all indexes.

Contacting Atlantis Software

Contact Atlantis Software at:

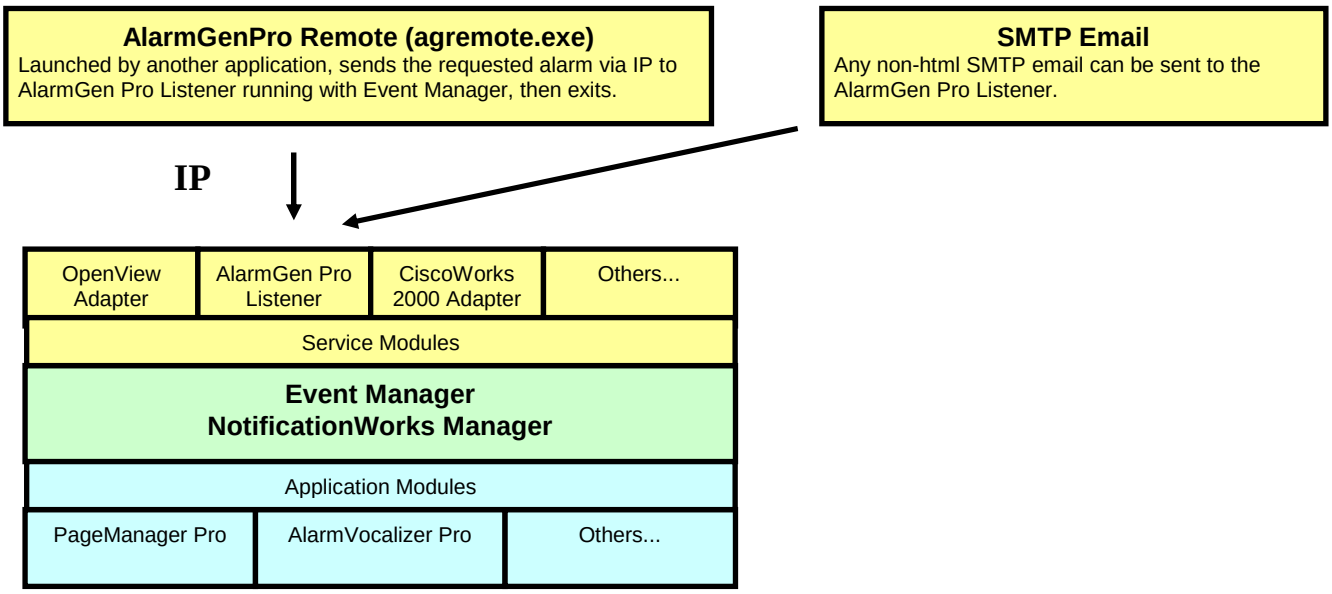
Atlantis Software
34740 Blackstone Way
Fremont, Ca. 94555-3209
Email: asinfo@atlantissoftware.com
Voice: 510-796-2180
Fax: 510-796-8476
Web: http://www.AtlantisSoftware.com

5
AlarmGen Pro

AlarmGen Pro is one of the NotificationWorks Service Modules. It provides the ability to create and send user defined alarms from any SMTP email software or using the AlarmGen Remote (agremote.exe) from the command line from anywhere as long as it has the ability to reach the PC running NotificationWorks via IP. AlarmGen Remote can be ran in many ways: It can be launched from other programs, DOS batch files, a command prompt, etc. from anywhere on the intranet or Internet. AlarmGen Pro can passed additional messages to be added to the original alarm message. It consists of two components: AlarmGen Pro Listener and AlarmGen Remote. The remote program named agremote.exe can be run from any PC running Windows with an IP connection.

Operation

AlarmGen Pro Listener runs from Event Manager which launches AlarmGen Pro Listener automatically by default. Its purpose is to provide the connection from the AlarmGen Remote to the Event Manager.



Items to Configure

This section explains how to start AlarmGen Pro, create alarm messages, and send them using AlarmGen Pro Remote. An installed and working Application Module and understanding of how Event Manager works if required. The checklist below shows the recommended task order.

1) Start AlarmGen Pro Listener
2) Create alarm messages
3) Configure IP and Port Addresses
4) Configure some other program to launch AlarmGen Pro Remote

Starting AlarmGen Pro

Bring up the Event Manager screen, then double-click the AlarmGen Pro entry. This either starts AlarmGen Pro and brings up the AlarmGen Pro Listener dialog or, if already running, just brings up the dialog.

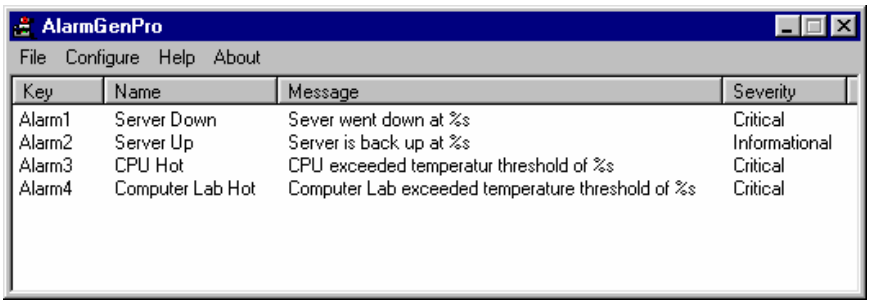


Figure 5.1: AlarmGen Pro Dialog

Creating Alarm Messages

Creating alarm messages is very easy. From the AlarmGen Pro configuration menu click "Add Alarms" menu item and fill in the fields.

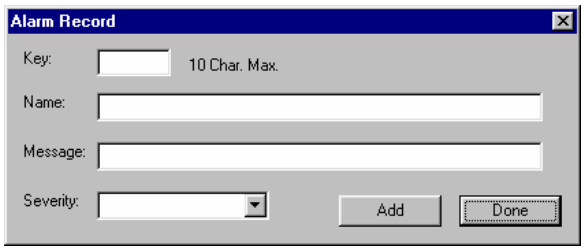


Figure 5.2: Alarm Record Dialog

Key: This has to be a unique name by which the alarm message is called up.
Name: Name of the alarm
Message: The alarm message to be sent. It is possible to imbed "tokens" or variables to be filled in when AlarmGen Pro Remote is launched by using the "%s" token in the message string.
Severity: Choose a severity from the dropdown list to assign to his alarm

Configuring the IP and Port Address

AlarmGen Pro Listener has to be configured what port to listen on and AlarmGenPro Remote what IP and port address to send alarms to. To configure the port address for AlarmGen Pro Server click Configure > Change Listening Port. By default it uses 32032. Change it to any unused port address if desired.

AlarmGen Pro Remote needs to be configured with AlarmGen Server's IP address and port. To configure these, run agremote.exe without command line parameters to bring up the help box. Click "Configure" and fill in the fields.

Configuring the Remote Command Line Parameters

In order for AlarmGen Pro to function, AlarmGen Pro Listener must be running at all times as it receives the AlarmGen Pro Remote or SMTP Email messages.

The following parameters are also the same for SMTP Email.

When configuring another program to launch the AlarmGen Pro Remote executable agremote.exe, it requires certain command line parameters, e.g. agremote /k=alarm1 /n=Accounting /p1=4:02pm

Agremote.exe sends the string, "/k=alarm1 /n=Accounting /p1=Accounting /p2=4:02pm" to the specified IP address and port of the AlarmGen Pro Listener. When AlarmGen Pro Listener receives the messages it locates the alarm by the key "alarm1" (/k=alarm1) and identifies the node "Accounting" (/n=Accounting). AlarmGen Pro loads this alarm and replaces any tokens with the /p(n) parameters.

Example: An alarm is configured with the message "Server %s went down at %s".
The /p1=Accounting parameter goes into the first "%s" (token). The parameter /p2=4:02pm goes into the 2nd "%s" to form this message:
"Server Accounting went down at 4:02pm"

AlarmGen Pro Listener then forwards it along to the EventManager for dispatching.

Possible command line parameters are:

/k= Alarm's key name, required
/n= Affected node name, optional
/pn= other values to insert into the alarm message, where n can be
1 or higher, E.g. /p1=system /p2=computer /p3=harddrive
/list Retrieves the list of configured alarms from AlarmGen Pro Server, (Not available via using Email).
/ip Allows configuring of AlarmGen Pro Server's IP and Port address, (Not available via using Email).
No Switches Help Box

There is no limit of how many parameters to pass into the message other than the Windows command line character length limit of 256.

Configuring the Email Message

The above switches are still the same except the /IP and /LIST is not supported via Email. Currently, only the Email message body is used, the subject line it ignored. Using the above example for sending an Email to the AlarmGen Pro listener from the same PC is:

To: anyone@127.0.0.1
From: anyone
Subject: Test message
Body:
/k=alarm1 /n=Accounting /p1=4:02pm

Let us know if you have any feature ideas and we will try our best to add them.

6
AlarmVocalizer Pro

AlarmVocalizer Pro provides verbal alarm monitoring and notification capabilities.

Using text-to-speech technology from Microsoft, any alarm/event message can be verbalized. An alarm message is divided into 3 parts: Node/device sending the alarm, severity, and alarm message. Each of these parts can be set to either verbalize, play a sound file, or remain silent.

Operation

AVPro is an Atlantis Software NotificationWorks Application Module and therefore requires a NotificationWorks Service Module to receive alarms. There are many Service Modules available with more being developed.

System requirements are

- EventManager and a NotificationWorks Service Module.
- All Windows versions
- 800 x 600 minimum desktop size
- Sound Card and Speakers

Memory Usage

AVPro uses different amounts of memory depending on which of its two modes is currently active, minimized or non-minimized. The minimized mode uses less memory and is the preferred mode when not modifying any of the AVPro's sound depositions or other settings. The non-minimized mode uses much more memory. The amount depends on the number of compiled MIBs in the ManageWise console.

- Minimized Mode approx. memory usage: 1.2Mb.
- Non-Minimized Mode approx. memory usage: 1.2Mb + (512 bytes x Alarm Total)

Disk Usage

AVPro uses 2MB. The alarm database, ALARMS.DAT, uses (4Kb x Alarm Total). This makes Total AVPro disk usage 2MB + (4KB x Alarm Total).

AVPro Page Layout

AVPro's screen layout is arranged in pages. Move from page to page by clicking on a page tab.

- Alarm Settings - Manage alarm settings
- Global Settings - Set up default settings and node list
- Recorder Log - Logs all alarms that have been received
- About AVPro - Displays registered owner information and copyrights

Items to Configure

This section explains how to start AVPro, assign sound dispositions, node filtering, and alarm repeat attributes. An installed and working sound card is required. The checklist below shows the recommended task order.

1. Add and configure alarms and their sound dispositions
2. Configure alarm repeat attributes
3. Add nodes to the global list
4. Assign Node Filtering

Quickstart

The quickstart guide only describes the steps needed to get up and running as quickly as possible. For a more in-depth description of the AVPro controls see later in this section.

1) **Starting AVPro:**
   a) By default AVPro is started when Event Manager is launched. If this is disabled, select AVPro from the client list in EventManager and press the startup button.
2) **Adding Alarms:**
   a) From the "Global Settings" page click "Add New Alarms to DB"
3) **Configure Sound Dispositions:**
   a) From the "Alarm Settings" page, select one or more alarms.
   b) Click the desired sound disposition from the lower right side of the screen, i.e. None, Verbalize, or Sound File.
4) **Testing the assignment:**
   a) Select an alarm.
   b) Press "Test"

Alarm Settings Page

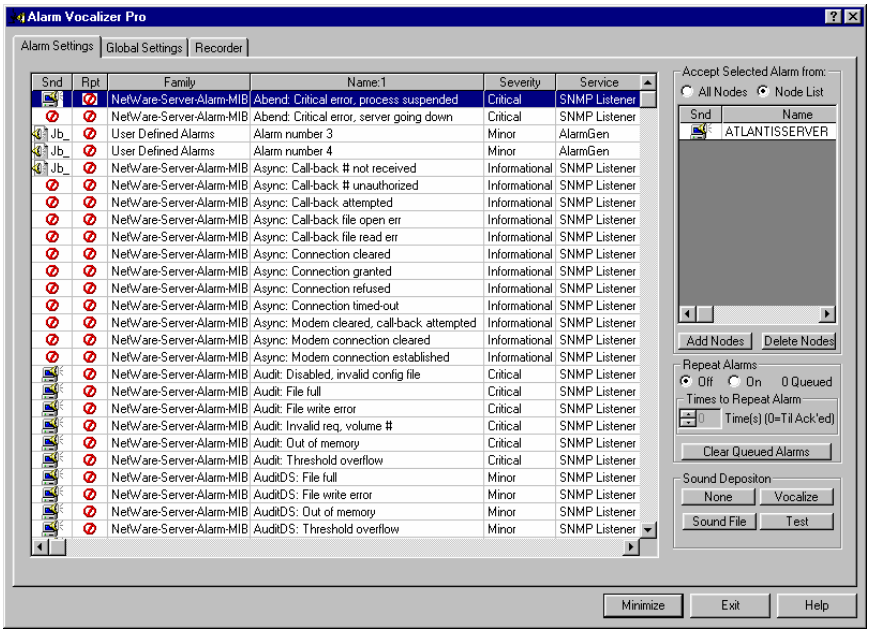


Figure 6.1: Alarm Vocalizer Pro

The "Alarm Settings" page contains two tables: the alarm table and the node assignment table. See below for table descriptions. From this page, assign sound dispositions to alarms, assign alarm filtering by nodes, assign repeat attributes, and see how many alarms are in the sound queue waiting to be played.

Sound Disposition

These 4 buttons assign sound dispositions to the selected alarm(s).

- "None": silent
- "Verbalize": verbalize the alarm
- "Sound File": Play the assigned sound file
- "Test": Test the assignment

Assigning Sound Disposition to Alarms

1) Using the mouse, select the alarm(s) to assign to a sound. If there are no alarms displayed in the alarm table use the "Add New Alarms to DB" option from the "Global Settings" page.
2) Click on the sound disposition button to assign
3) Notice the changed icon for the selected alarms in the "Snd" column

Note: When using sound files, all sound files must be in the same directory. If an alarm is assigned to a sound file in a different directory all previous sound file assignments are removed.

Assigning Node Filtering

In the control section "Accept Selected Alarm(s) from" choose to accept selected alarm(s) only from nodes in this node table. First create a master node list by choosing the "Manage Node List" option from "EventManager". Then from AVPro's "Global Settings" page click "Add Nodes". This installs the master node list into AVPro. The "Global Settings" page is also where sound dispositions are assigned to the node names.

1) From the "Alarm Settings" page, select the alarm(s) to filter
2) Click "Node List" to move the selection from "All Nodes" to "Node List"
3) Click "Add Nodes" and select the nodes to accept the selected alarms from

To delete a node from the node table, select the node(s) then click "Delete Nodes".

Note: Sound dispositions cannot be assigned to the nodes from the "Alarm Settings" page. It needs to be done from the "Global Settings" page. Since node sound dispositions assignments are global, any changes made affect all currently assigned nodes.

Assigning the Repeat Feature

The Repeat feature makes an alarm repeat its sound assignment for an infinite amount of time or for a set number of times. After the "Hot Key" is pressed, the alarm is then acknowledged and ceases to repeat for that received alarm instance.

1) Select the alarm(s) to repeat
2) Enable the repeat feature by clicking "On"
3) Choose how many times to repeat the alarm(s) by entering an amount into the "Time to Repeat Alarm" field. A value of zero repeats the alarm(s) indefinitely until the "Hot Key" is pressed.

The Alarm Sound Queue

Since alarms can arrive faster than AVPro can play them, a separate thread is created to listen and save alarms into a queue called a sound queue. This status number shows how many alarms are currently in the sound queue waiting to be played. Clicking "Clear Queue" removes all alarms in the queue and stops playing the current alarm.

Stopping the Currently Playing Alarm

Press the assigned "Hot Key". By default, this key is the F11 key. Change the "Hot Key" from the "Global Settings" page.

Sorting Items in the Tables

Sort any items in all tables by double-clicking on the column title. Sub-sort by holding the CTRL key down while double-clicking on another column title. A number appears next to the column title name indicating the sort order.

Note: No number will be shown on the "Snd", and "Rpt" column

Alarm Table Column Meanings

Name	Meaning
Snd	Shows an icon representing the sound assignment.  Verbalize  Play sound file  No sound
Rpt	Shows an icon representing the repeat setting  Repeat infinite until acknowledged Repeat (n) times or until acknowledged

	Don't repeat
Family	The family of alarms this alarm belongs to
Name	The name of the alarm
Severity	The level of severity
Service	The "Service Module" responsible for this alarm

Global Settings Page

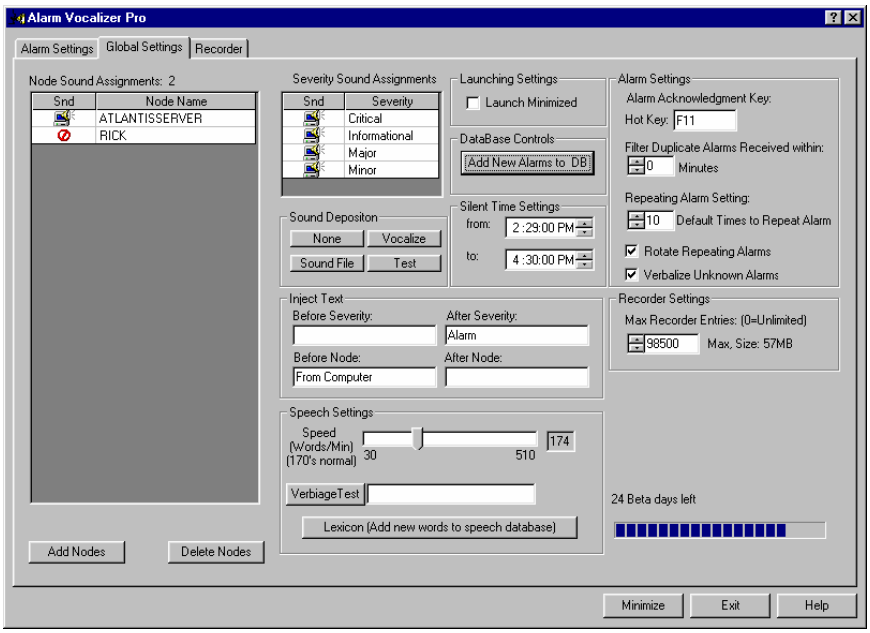


Figure 6.2: Global Settings

Building Master Node List

To filter alarms by nodes it is necessary to build a master node list. Clicking "Add Nodes" from the "Global Settings" page brings up a list of nodes to choose from.

Note: If the popup node list is empty run the "Manage Device List" option from the "EventManager" program.

Assigning Sound Dispositions to Nodes and Severity

Assigning sounds to node and severity names uses the same process as described in the "Assigning Sound Disposition to Alarms" section above.
Click the node or severity name(s), then click the desired sound disposition type.

Insert Text Option

This control allows inserting any text to be verbalized when verbalizing the severity and/or node name.
The text can be inserted before and/or after the node and severity name. This provides a better sounding transition when the node and severity names are being spoken. For instance, without the inserting option the alarm might be:
"Critical" "Sales" "Volume low on disk space"
With the default insertions it is:
"Critical alarm" "From server Sales" "Volume low on disk space"

To use this option, enter any desired text into the "Insert Text Option" fields.

Speech Settings

These settings provide control over the speed the words are spoken with and adding or changing how words are pronounced.

Word Spoken Speed
To adjust how fast words are spoken, click and hold the mouse down while dragging the speed slider left or right.

Adding New Words, Changing Pronunciation
To add additional words or change how a word is pronounced click "Lexicon" to display a popup dialog wizard that steps through the process.

To test words or sentences type in the words into the "Verbiage Test" field then click "Verbiage Test".

Launching Settings

It is recommended to start up AVPro minimized. This mode uses far less memory than running non-minimized. To do this, use the mouse and put a check mark in the "Launch Minimized" option under the "Launching Settings" controls.

Database Controls - Adding Alarms to AVPro

When adding alarms to the management system it is necessary to have AVPro request the list. To do this, verify that all Service Modules are running then click "Add New Alarms to DB".

Silent Time Settings

Use this option to schedule a time period in the day during which all alrms will be muted.

Alarm Settings

This group of controls provide the ability to change the "Hot Key", duplicate filters, the default repeat amounts, turn on/off the rotate feature, and turn on/off the verbalizing of unknown alarms.

To Change the Acknowledgment Hot Key
Click in the Hot Key field, then type the key sequence to use, e.g. CTRL-F11, ALT-F12, ALT-5, etc... The default is F11

Duplicate Alarm Filtering
A filter can be set to prevent the same alarm from being sent multiple times. This filters out any alarms that have already been sent within the set number of minutes. For instance, if “Minutes” is set to 5 and AVPro receives the alarm “NLM Unloaded from server SALES” it checks the alarm recorder log to see if this alarm has already been sent within the last 5 minutes. If not, it will be played, otherwise the alarm is ignored. Setting the “Minutes” to 0 deactivates this filter.

Rotate Repeating Alarms
When checked, any alarms set to repeat will be rotated. For instances, if alarm 1 and alarm 2 are set to repeat and rotate is off (not checked), alarm 1 keeps playing until it has reached its repeat condition, then alarm 2 starts. With repeat on (checked), alarm 1 plays, then alarm 2 then alarm 1, etc. until the repeat conditions have been reached.

Verbalize Unknown Alarms:
When checked, any alarms not found in the Alarm Vocalizer Pro's database is played.

Setting the Maximum Recorder Size
This allows setting the maximum size of the recorder file. When the maximum is reached, the oldest alarms are deleted to allow the new ones to be saved.

Recorder Page

This page shows the alarms that have been received by AVPro. The log table contains 8 columns:

Alarm Log Columns

- **"Status" -** Shows the status of the alarm. If any errors occurred in delivery the error message appears here.
- **"Time" -** Displays the time when AVPro received the alarm
- "**Affected Node**" - The node the alarm came from
- **"Message" –** The message that was sent
- **"Alarm" -** The name of the alarm that was sent
- **"Family" -** The name of the MIB
- **"Severity"** – Severity level of the alarm
- "**Service**" – The service the alarm was received from

Delete All

Clears the alarm log.

Print Log

Prints the alarm log.

Export Log

Exports the alarm log to a delimited file which can be imported into a report.

1) Click "Export Log".
2) Choose the delimiter flag to use.
3) Select the file to export to, then click OK

7
CastleRock SNMPc Adapter

Atlantis Software's CastleRock SNMPc Adapter (Service Module) connects and receives all events from CastleRock's SNMPc console. Each alarm can then be handled using any of our Application Modules like PageManager Pro and Alarm Vocalizer Pro.

Items to Configure

There are only a couple of things to configure:

1) Configure the Adapter with the SNMPc console's IP address or 127.0.0.1 if on the same system
2) Configure the Adapter with the SNMPc remote poller password if one was configured, otherwise just leave it empty

That is all there is to it. If the configuration is correct then the Adapter's dialog shows the message "Connected" in the Connection Status line.
If for some reason the connection is dropped, the Adapter will keep trying to reconnect showing the attempts in the "Reconnect Trys" line and the amount of reconnects in the "Reconnects" line.

8
CiscoWorks Adapter

Atlantis Software's CiscoWorks Adapter (Service Module) receives and converts the two SNMP traps from CiscoWorks 2000 and translates them into over 50 specific alarms. Each alarm can then be handled using any of the Application Modules like PageManager Pro and Alarm Vocalizer Pro.

Operation

When the CiscoWorks Adapter receives the SNMP event it uses the translation file called cwadapter.ini to translate the event into a more meaningful and useful event message (the Cisco's CiscoWorks SNMP agent must be enabled), then forwards the message to PMPro or AVPro through EventManager.

Items to Configure

1) Install and enable Microsoft SNMP Trap Services
2) Enable CiscoWorks Trap Notifier Adapter
3) If running CiscoWorks on the same PC as NotificationWorks change the Microsoft SNMP Trap port and configure the CiscoWorks SNMP Trap agent to send to the new port

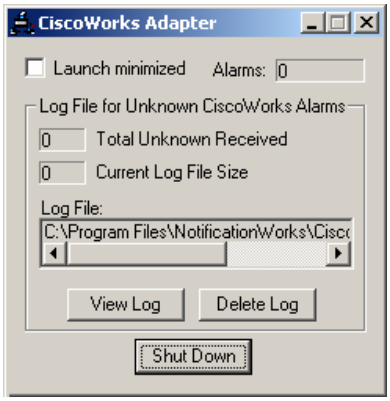


Figure 8.1: CiscoWorks Adapter

To install and enable MS SNMP Trap services:

1) Navigate to Control Panel > Add/Remove Programs
2) Select "Add/Remove Windows Components"
3) Select "Management and Monitoring Tools"
4) Click "Next" and follow the onscreen instructions
5) After installation is complete verify SNMP Trap Services is running
6) Enable Cisco CiscoWorks Trap Notifier. For instructions refer to http://www.atlantissoftware.com/support.shtml and click the link "Configuring Cisco's CiscoWorks 2000 Cisco Trap Notifier Adapter" to be taken to Cisco's website showing detailed instructions on how to configure the Trap Notifier Adapter.

To run NotificationWorks on the same system as CiscoWorks, it is necessary to change the Microsoft SNMP Trap Service port (port Windows is listening on for SNMP Traps) and the Cisco Trap Notifier Adapter port to something other than 162 because CiscoWorks is also using port 162 to receive SNMP Traps and Cisco wont share.

To change the destination port number for CiscoWorks Trap Notifier please refer to the above mentioned URL. To change the Microsoft SNMP Trap port edit the file C:\winnt\system32\drivers\etc\services.

Change the port in the entry

snmptrap 162/udp snmp-trap #SNMP trap

to the same number assigned earlier to the Cisco's Trap Notifier Adapter. Be sure to use an unused high port, e.g. 3232.

Removing Event Family Name from Device Name

CiscoWorks by default prepends the event family name to the device name. To have the Adapter remove the event family and leave just the device name add the following to the CiscoWorks Adapter section in the EventMan.ini file:

RemoveFamilyFromDevice=1

Use Device Short Names

The Adapter by default strips device name given to it by CiscoWorks to be just the short name. For example, if it receives fremont.california.us.atlantissoftware.com it will shorten it to atlantissoftware.com

To make the adapter use the name it was given add the following to the CiscoWorks Adapter section in the EventMan.ini file:

UseShortNames=0

9
HP OpenView™ NNM Adapter

Introduction

The Adapter for HP OpenView NNM is a service which connects to HP's OpenView Network Node Manager (NNM). NNM can be running on any HP supported OS such as Solaris, HP-UX, AIX, Unix, or Windows.

Run NotificationWorks including the NNM Adapter on Windows, configure it with the IP address of the system running NNM, and provide a copy of NNM's trapd.conf file. The Adapter then receives every event NNM receives or creates. The received event is processed by using the rules in the NNM trapd.conf file and forwarded along to NotificationWorks' PMPro or AVPro. Knowlegde of NNM and its trapd.conf file is assumed.

Items to Configure

1) Configure the Adapter with the IP address of the system running NNM
2) Configure the Adapter with the location of the NNM trapd.conf file

The "trapd.conf" file is NNM trap configuration file that tells NNM how to process the received event. NotificationWorks NNM Adapter also uses this file for the same purpose, therefore the Adapter needs to have access to this file. If installing NotificationWorks on the same system as NNM (if using the Windows version of NNM) this process is automatically done during installation. If connecting remotely it is necessary to either map a Windows network drive to the remote system's folder where the trapd.conf file is located, or copy the file to the PC running NotificationWorks and configure the Adapter with the folder location.

To configure the IP address click Configure > Set Address of OpenView.
To configure the location of Trapd.conf file click Configure > Set Trapd.conf location

Logging

To save the received events into a file add the following to the EventMan.ini file (located in the Windows folder) in the NNMAdapter section:

[NNMAdapter]
Log=1

Event Device Source

All events come by default from the system running NNM, but this is not necessarily the actual system the event is about. The NNM Adapter makes many attempts to discover where the event really came from or what device it is about. Each event can have one or more variables and each variable can be addressed by index starting with 1 to the max total of variables that are contained in that event. Most of the time one of these variables is the name or IP address of the affected device. The Adapter goes through all of these variables and tries to determine which one to use as the affected device. This is done using the following rules:

1) If the event name is an OpenView event, “OV_” the default index used is 2 since the second variable in almost all OpenView events is the affected device.
2) If it is not an OpenView event each variable is examined. If it is a IP address it is used as the address of the affected device.
3) The Adapter can be forced to use a specific variable index for a specific event by editing the Trapd.conf file, locating the event block to modify, then adding –source=index to the last line of that event block. Example:
   #
   EVENT OV_Network_Critical .1.3.6.1.4.1.11.2.17.1.0.58916869 "LOGONLY" Major
   FORMAT Network critical
   SDESC
   This event is generated by HP OpenView when it detects the
   status of a network has become critical (all connectors and
   segments in the network are in an abnormal state).
   --source=3
   EDESC
   #

If no device can be found it defaults to the device running NNM.

Event Correlation Streams

By default the Adapter will receive ALL events from the OpenViews NNM. If you would like the Adapter to switch from All and use the Correlation Stream then add the following to the EventMan.ini file located in the WinNt folder:

```
[NNMAdapter]
ConnectFilter={CORR}.*
```

Make sure you enter the above text exactly as shown, including the braces. You can also include OID filters, here are some examples:

Filter which defines what events (if any) the session wants to receive, which will be forwarded to it by the pmd process. A value of NULL or "" (empty string) is interpreted as a no-receive filter. In this case the session will be used to send events only; pmd process will not forward any events to it.
A non-empty filter defines a list of the events which should be forwarded to the application. The filter specifies event types only, using the following syntax.

```
filter  ::=  [constraintList] eventList
constraintList  ::=  "{" constraintKeywordList "}" " "
constraintKeywordList  ::=  constraintKeyword  |
                        constraintKeywordList ","
constraintKeyword
constraintKeyword  ::=   "NO_FORWARDED" |  flowType
flowType  ::= "CORR" ["{" streamName "}"] | "ALL" | "RAW"
streamName  ::=  character string of length 1...255.
            Valid characters are alphabetic {a-z, A-Z},
```

numeric {0-9} or "_".
eventList ::= eventSpec | eventList ";" eventSpec
eventSpec ::= "." eventComponent | eventSpec "."
eventComponent
(128 eventComponents maximum)
eventComponent ::=value | eventComponent "," value
(first value must be less than second value)
value ::= number | range | "*"
range ::= number "-" number
(first number must be less than second number)

number ::= 0-4294967295

In summary, a filter contains a list of constraints and a list of events. The constraint "NO_FORWARDED" specifies that no event from remote pmd will be forwarded to the application. The key words "CORR", "ALL", "RAW" specify the type of event flow from pmd (see ov_event man page for details). It is not allowed to specify more than one flow types in the filter. If none of the three key words is specified, the application will get the "RAW" event flow. The token streamName specifies the name of a stream the application connects to. It is only valid when the keyword "CORR" is specified. The streamName has to match the stream name inside the ECS engine (see ecsmgr for details). If no streamName is specified for the "CORR" event flow, the application connects to the "default" stream. The list of events can be specified using wildcards and/or ranges. For example:

".1.3.6.1.4.5-11,13,40-55.*"
".*" (all events from "RAW" event flow)
"{NO_FORWARDED,CORR{myStream}} .*"
(all local events, no forwarded events, from
"CORR" event flow with the stream name "myStream")

"{NO_FORWARDED} .1.3.6.1.4.*;.1.3.6.1.5.7.*"
".1.3.6.1.6.3.1.1.5.*"
(all standard SNMP traps)

The values within an eventComponent must be in increasing order. (The eventComponents ".1.3-7,5" and ".1.3.5,4" are not valid.) If a filter passed to NNM is invalid, pmd process will disconnect the application with an error message in trapd.log.

10
Node Monitor

Introduction

Node Monitor is a Service Module and a member of the NotificationWorks suite. Node Monitor monitors the status of IP devices and ports/sockets . It allows setting thresholds that trigger alarms for network latency (how busy), amount of time down, amount of no responses, service errors, etc.

Memory Usage

Node Monitor (NodeMon) uses about 4.5MB of memory and creates two threads for each monitored node, using an additional 17k of memory for each node, for a total approx. memory usage of: 4.5Mb + (17k x number of monitored nodes

Items to Configure

This section explains how to start NodeMon, create, configure and save a node listing. A node listing is a list of nodes to monitor. It is possible to create multiple listings resulting in the ability to separate monitored nodes into groups. For instance, separate web servers from routers. Node Monitor monitors each listing separately by running another copy of Node Monitor. The checklist below shows the recommended task order.

1) Add nodes to monitor
2) Configure polling settings
3) Configure alarm settings
4) Configure setup settings

Quickstart

The quickstart guide only describes the steps needed to get up and running as quickly as possible. For a more in-depth description of the NodeMon controls see later in this section.

1) **Starting Node Monitor:**
   a) Node Monitor is started by default when Event Manager is launched. If this is disabled, select Node Monitor from the list in Event Manager and press the startup button.
2) **Adding nodes/devices to monitor:**
   a) Navigate to Configure > Add Nodes
   b) Either double-click the node to add or highlight multiple nodes then click “Add Node“
   c) When finished click “Done”
3) **Configuring Polling Times:**
   a) Navigate to Configure > Settings
   b) From the “Misc.” tab highlight the nodes to change
   c) Click the left or right arrow buttons under the Poll Intervals to decrease or increase the time between polls for the selected nodes.
   d) Click “OK” when finished
4) **Resizing the Node Monitor Display:**
   a) Place the mouse pointer on the right edge of the first column called "Name" so it changes to a double arrow cursor.
   b) Hold the left mouse button down and drag the width of the column to the desired size, then release the mouse button. Notice that all columns called "Name" have been resized to match the first one.
   c) Now place the mouse on the bottom right corner of the Node Monitor display so it changes to a double arrow cursor.
   d) Hold the left mouse button down and move the mouse to resize the whole Node Monitor display. Notice that while increasing the height and width of the display, the cells within the display are re-stacked to match the new size. This allows changing the amount of columns and rows that are displayed.
5) **Saving Listing:**
   a) From the File menu, select Save As.
   b) Enter the desired name for the group of monitored nodes
   c) Choose which service to use from the Service’s drop down list.
6) **Starting the Monitoring:**

a) From the Configure menu, select "Start Monitoring All" Notice that the background color changes from gray to white indicating that it is currently being monitored. Gray means not monitored. Each time the node is pinged an arrow appears next to the Ping icon in the Ping column. This indicates that a ping was just sent to that device. The arrow clears when a response is received or an error occurs.

File Menu Option

Below are the details about each option under the File menu.

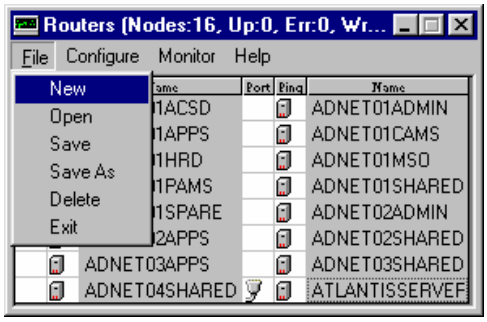


Figure 10.1: File menu

New

The new option loads another copy of NodeMon into memory. This provides the ability to set up multiple node lists and a copy of NodeMon monitoring each list simultaneously, allowing for great flexibility on how to organizing node lists.

Open

This option opens a list of previously saved Group files (*.grp). Double-click on a group file to load the new group list into NodeMon.

Save

This option saves the currently displayed list of nodes to the currently opened group file. If one is not currently open a prompt appears to enter an new name for this group list. It is recommended to use descriptive names for the list of nodes, e.g. “Web Servers”, or “NT Servers in Sales Dept”, etc.

Note: It is recommended to keep the group files in the NodeMon directory, otherwise NodeMon's autoload feature is unable to load them.

Save As

Saves the currently displayed list into a different group file name.

Exit

Close and exit NodeMon. NodeMon saves its current screen size and placement if that option has been enabled in the Settings Menu Options.

Monitor Menu Option

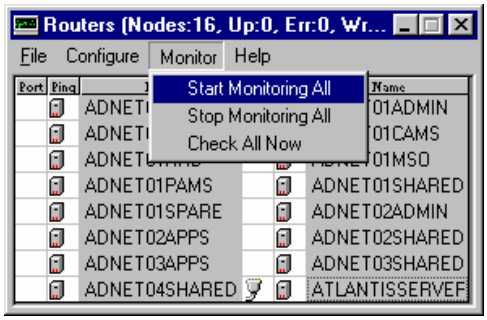


Figure 10.2: Monitor menu

Start Monitoring All

Selecting this option starts monitoring/polling all the nodes in the list.

Note: If a node has both components (Ping and Port) disabled, then even though the node is now being monitored, no checks are performed.

To start monitoring a single node instead, right-click on the node and select “Start Monitoring”.

Stop Monitoring All

This stops monitoring for all the nodes in the list.

To stop monitoring only for a single node, right-click the node and select “Stop Monitoring”.

Check All Now

This causes all nodes to be immediately checked.

Configure Menu Option

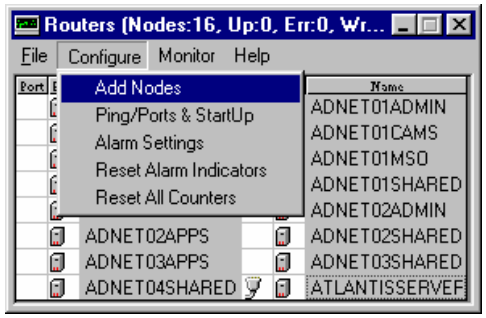


Figure 10.3: Configure menu

The Configure menu contains options to set up NodeMon's behavior.

Add Nodes

Selecting this option brings up a list of nodes/devices that can be added to NodeMon monitored list. Each node/device must have an IP address assigned, otherwise it is not selectable and has the message (No IP Address) next to the node name. The node list is managed by Event Manager. Click “Edit Node List” in Event Manager to edit it.

Ping/Ports & StartUp

Selecting this option brings up a dialog box that allows changes to the setup settings, monitoring rate, ping and port settings. These settings are explained later in this guide.

Alarm Settings

This brings up a dialog box that allows changes to NodeMon’s alarms. This is described later in the section called “Configuring Alarms”.

Reset Alarm Indicators

When an error occurs the color of the affected component changes to red and the node is rotated to the top of the list. If the component regains functionality the color changes to yellow. Selecting “Reset Warning” resets all errors and warning flags, and sets the colors back to normal.

Reset All Counters

Each component maintains on going stats that can be quickly viewed by placing the mouse pointer over a component's icon. Selecting Reset All Counters resets all stats for all components.

Settings – Misc Tab

This option brings up the settings dialog which provides controls for loading, ping and port settings.

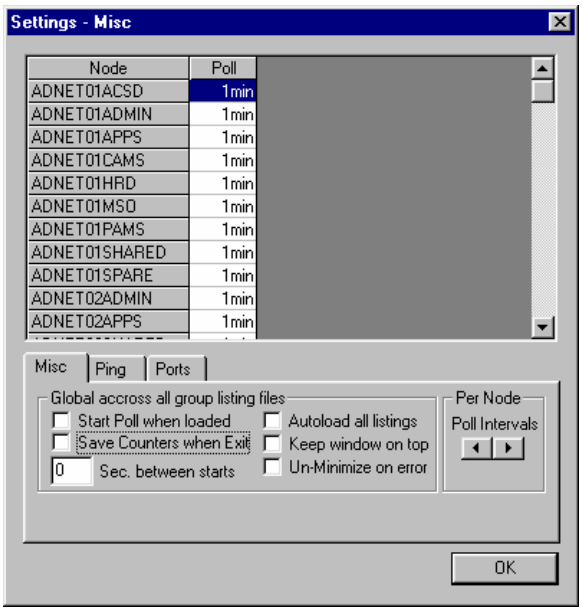


Figure 10.4: Settings – Misc. menu

Start Poll when loaded

If checked it automatically begins polling when Node Monitor loads a group file.

Save Counters when Exit

When checked counters are saved when NodeMon exits.

Autoload all listings

Checking this option causes NodeMon to automatically load a copy of NodeMon for each previously saved group file.

Keep window on top

This causes NodeMon to always be on top.

Sec. between starts

When starting to monitor all nodes, NodeMon will wait for (n) seconds between starting each node. This causes a cascade starting effect.

Un-Minimize on error

If NodeMon is minimized and an error occurs, NodeMon restores the NodeMon window. If unchecked the icon flashes on received errors.

Poll Intervals

To change the time between polls, select the node(s) to change and click the left arrow to decrease time or the right arrow to increase time. Each node can have its own interval setting.

Settings - Ping Tab

The Ping Tab provides control over the ping's behavior.

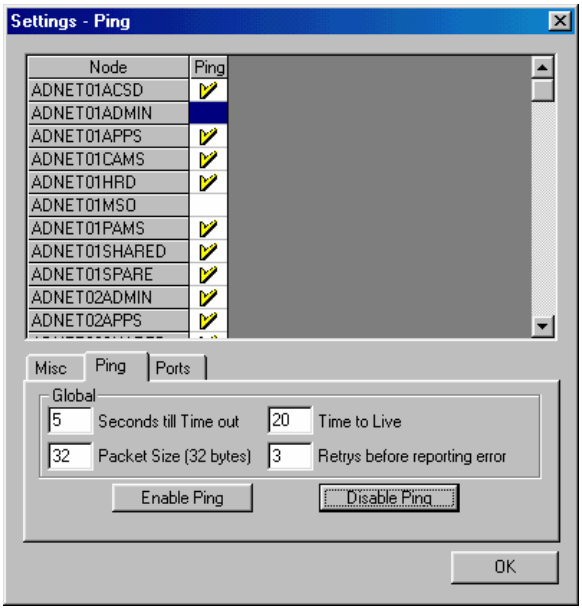


Figure 10.5: Settings – Ping menu

Seconds till Time out

This is the amount of seconds that NodeMon waits for a node to respond to a ping request. It is recommended to set this to 2 to 5 seconds.
This setting is global to all nodes.

Packet Size

This is the size of the UDP diagnostic packet (ping). 32 bytes is the smallest setting.

Time to Live (TTL)

This is the maximum amount of hops (nodes) the ping packet is allowed to pass though before it expires and is dropped.

Retries before reporting error

This is the amount of retries before the node is reported as not responding and an alarm is sent. It is possible that the node is fine and that the packet (ping) was just lost. It is recommended to set this to at least 3.

Enable/Disable Ping Buttons

A node is pinged if it has a check mark next to its name. To enable or disable ping for node(s), select the node(s) then click either "Enable Ping" or "Disable Ping". Double-clicking in the "Ping" column also enables/disables ping for that node.

Settings - Ports Tab

The Ports tab provides the ability to manage ports/sockets, including creating, assigning, editing, and deleting.

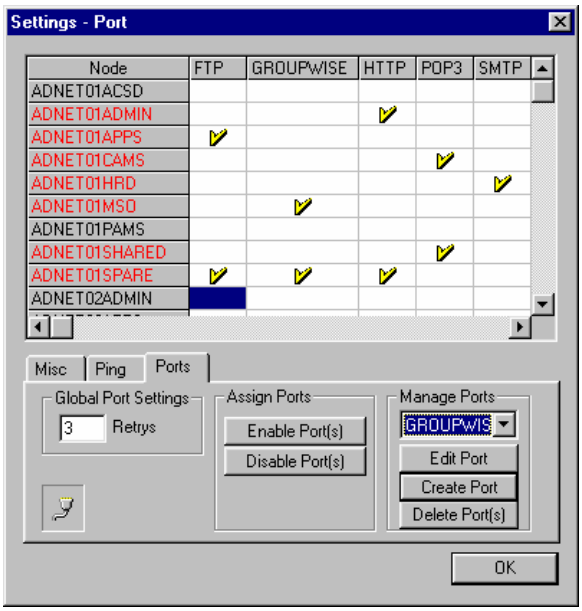


Figure 10.6: Settings – Port menu

Retries

This is how many times the port is tried before it is reported as an error. It is recommended to have this set to 3.

Enable/Disable Port(s)

To enable or disable monitoring of a specific port on a specific nodes/devices, either double-click in the port field or select multiple ports and multiple nodes and then click either “Enable Port” or “Disable Port”. If it is enabled a check mark appears in the Port field for the node.

Edit Port

To edit or test a port select the port to use from the dropdown box then click “Edit Port”. For detailed instructions for the Port Settings screen please refer to the "Managing Ports/Sockets" section.

Create Port

Clicking this button brings up the Port Settings screen to create and test a port configuration. Create a port/socket that can call into a website and download a web page and compare it with a previously saved original copy. If a difference is detected an alarm is issued. Please refer to the "Managing Ports/Sockets" section for further details.

Delete Port

To delete a previously created port select the port from the dropdown port list and click “Delete Port”. When a port is deleted, it is removed from all previously saved group files.

Port Settings (Managing Ports/Sockets)

The Port Settings dialog provides control over all aspects of how to check a port address. From just a simple check with just opening and closing a port address to opening, sending data, reading data back and having that data compared to expected data.

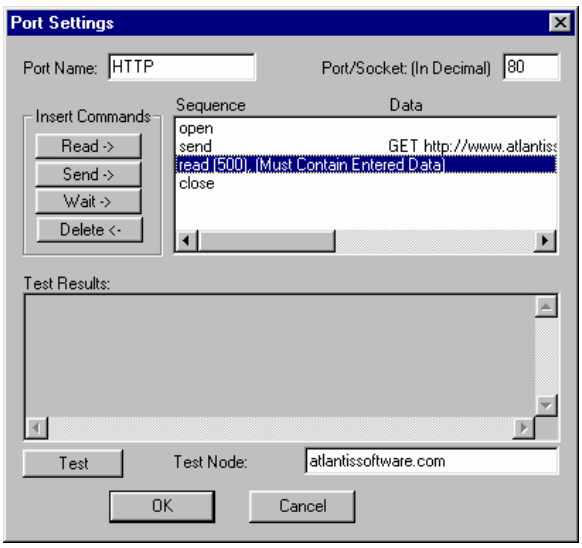


Figure 10.7: Port Settings dialog

Port Name

Enter the desired name for this port configuration.

Port/Socket

Enter the port number for this port/socket. The number must be in decimal frmat. For instance, POP3 uses address 110.

Sequence List

The sequence list box shows the command sequence that is sent to the port. Double-clicking any of the command sequences between “open” and “close” allows editing that command. Editing the “open” and “close” command is not permitted.

Read ->

This brings up the Port Read Settings. Choose to have the “read” command just ignore any received data or compare the received data compared with what is typed here. The type of comparison can be to contain the entered data or match it exactly. The “send” command is inserted above the currently selected command in the command sequence list

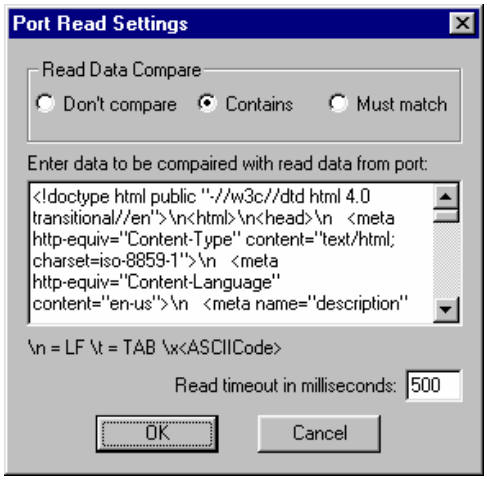


Figure 10.8: Port Read Settings

Note: To enter control characters use the format of \xnn where nn is the two digit ASCII HEX code of the desired control character. It must be exactly two digits, i.e. \x0d

Send ->

Pressing this button brings up the Port Send Settings dialog. Any data to send to the port is entered here. The “send” command is inserted above the currently selected command in the command sequence list.

Wait ->

Inserts a wait command.

Test

To test the port configuration click “Test”. The test results appear in the test results box. This data can be copied and pasted into the “read” command for comparisons.

11
SNMPListener

Introduction

The SNMPListener v2.0 receives and processes SNMP traps, and forwards them to the NotificationWorks system. The built-in MIB compiler supports SNMP v1 and v2 compliant MIBs.

MIB stands for Management Information Base. It is a document written in a specific format that defines the possible alarms (Traps or Notifications) and/or variables that are supported by a specific device or software. A good MIB resource is http://www.mibCentral.com.

SNMP stands for Simple Network Management Protocol and is a specific network packet format for sending and receive network management information.

One of the changes from SNMP v1 to v2 is that “Traps” have been renamed to “Notifications.”

Items to Configure

This section will explain how to start SNMPListener, compile and configure SNMP MIBs and traps

1) Enable Microsoft’s SNMP Trap service
2) Create a MIB collection
3) Compile MIBs
4) Customize Trap (alarm) messages
5) Configure other devices trap targets

Quickstart

The quickstart guide only describes the steps needed to get up and running as quickly as possible. For a more in-depth description of the SNMPListener controls see later in this section.

1) **Starting SNMPListener v2.0:**
   a) By default SNMPListener is started when Event Manager (NotificationWorks) is launched. If this is disabled, select SNMPListener from the service module list in Event Manager and press the startup button.
2) **Compile MIBs:**
   a) Create a subdirectory under the SNMPListener called MIBs. Gather all the MIBs that support the devices to receive traps from and copy them into this new directory.

   b) From SNMPListener’s menu click Configure > Compile MIBs

      NOTE: Any MIBs that are highlighted in red have failed to load. If they contain traps they should be fixed and recompiled.

Compiler Dialog Screen

The “MIB Compiler” screen provides the ability to compile and see the results of each compiled MIB.

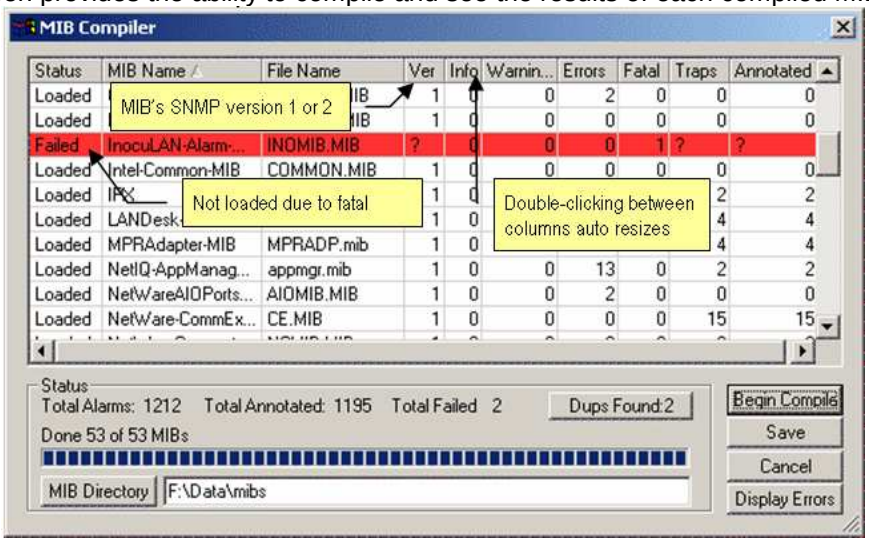


Figure 11.1: MIB Compiler

This screen shows the results of a compile session after clicking “Begin Compile”. The results are divided into 10 columns. Also shown are grand totals displayed below this grid in the Status section.

Rows displayed in red indicate a MIB with at least one fatal error that could not be loaded. If that MIB does not contain the symbol TYPE-TYPE or NOTIFICATION-TYPE and is not trying to be imported by another MIB file, just remove it from the MIB directory. SNMPListener is only concerned about traps/notifications. If that MIB does not contain any then SNMPListener doesn’t need it as long as it is not also trying to be imported by another MIB file.

Sorting

All Atlantis Software products that show a grid can have its contents sorted just by left-clicking on the column name. Clicking on the same column name again reverses the sort order. The sort order is indicated via an up or down arrow shown next to the column name.

Resizing

Each column in the grid can be resized by placing the mouse pointer between two columns. When the mouse pointer changes to a double arrow hold down the left mouse button and drag the column left or right to adjust the column width. Double-clicking the left mouse button will auto size the column to fit the longest text in that column.

The dialog box can also be resized by holding down the left mouse button on the bottom right side of the dialog and dragging it to the new size.

Column Names

The column names and their meanings are:

- **Status**: Current status of that row’s MIB. During compiling this changes based on what is happening at that moment.
- **MIB Name**: Shows the name of the MIB, which is not necessarily the name of its file. Some MIBs files define more than just one MIB
- **MIB File**: Shows the name of the file that defines the MIB. This file name can appear more than once if that file defines more than one MIB
- **Ver**: The version of the MIB, which currently can be 1 or 2
- **Info:** The number of problems found of severity “Informational”
- **Warning:** The number of problems found of severity “Warning”
- **Errors:** The number of problems found of severity “Errors”
- **Fatal:** The number of problems found of severity “Fatal”. A problem of fatal severity prevents the MIB from loading.
- **Traps:** The number of alarms (traps/notifications) found in this MIB.
- **Annotated:** The number of alarms that have custom messages

Editing MIBs

Edit the MIB in Notepad by double-clicking on any MIB row. The corresponding file is loaded into Microsoft Notepad.

Dup Found Button

The total duplicate MIBs found in the choosing MIB directory is listed on this button. Duplicate MIBs are those files that define the same MIB name even through their file names may be different. Clicking this button cycles through their names and locations. Duplicate MIBs are not compiled, meaning that the first occurrence is but not the duplicate.

MIB Directory Button

Clicking this button brings up a file dialog to choose where to place MIB files. It is recommended to create a subdirectory under the SNMPListener directory called “MIBs” and copy all MIB files into it.

Begin Compile Button

Clicking this button starts the compiler. Each row’s status field is updated with process information during the compile.

Save Button

Do not forget to click “Save” when the compiling session is completed. This saves the compiled information into the alarms database to be used to process received SNMP alarms.

Also note that clicking this button brings up a replace dialog. This provides the ability to select what to replace. This is a good option when a previous compile was done and custom messages were added to the database that should not be overwritten.

Display Errors Button

Display any found MIB problems by selecting that MIB’s row (highlighting it) then clicking “Display errors”.

MIB Manager Dialog Screen

Modify the alarm that is sent by annotating the alarm message and its severity. The alarm description is used instead for any non-annotated alarms.

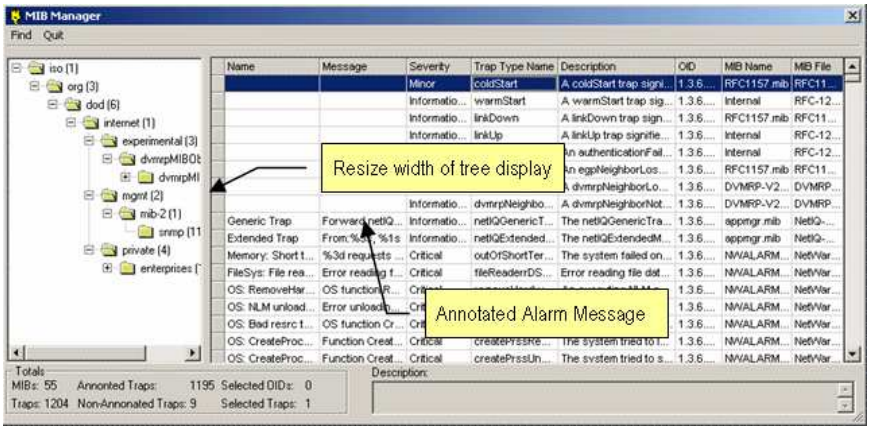


Figure 11.2: MIB Manager

The left side of the screen shows the MIB tree with the OID (Global naming object identifier). The right side shows the alarms belonging to the selected branch on the left.

Click any branch of the MIB tree and the alarm list shows all alarms for the branch and below. This is a good way to see what alarms are available to what company’s MIB that are currently compiled

Resizing

Resize the left and right screens by placing the mouse between both screens. When the mouse pointer changes hold down the left mouse button and drag it to the left or right to resize.

To resize the dialog box just do the same but on the outside edge of the dialog.

The alarm list columns can also be resized by clicking between the column names. To resize the row to fit more than one line of text per row, click between the rows and move the mouse up or down.

NOTE: If the column width becomes too wide it can be resized back to default by double-clicking between its name and the one next to it.

Searching for Alarms

Locate alarms quickly by using the Find command from the menu.

Customizing Alarms

Change what the SNMPListener forwards to NotificationWorks. Change the name of the alarm, which is what is used to schedule alarms for instance in PageManager Pro. Change the message it sends and the severity, even the description (not recommended).

To Change/Customize (Annotate) the Alarm:
Double-click in the message field and enter the text to send. To imbed a variable into the message, right-click and a list of variables appears. Select the variable to insert and it inputs the appropriate flags.

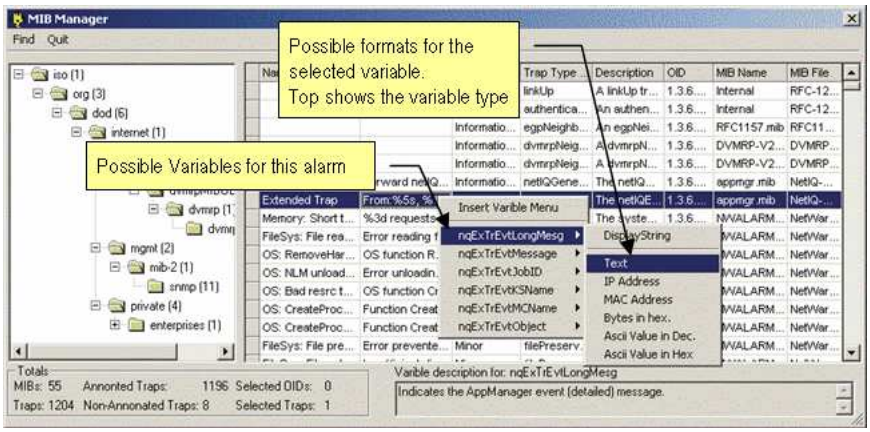


Figure 11.3: MIB Manager Alarm Customization

For example, enter “The server is down”

If the selected alarm has a variable called serverName it could be imbedded into the message by putting the mouse between “server” and “is” then right-click to see the variable list like the one shown in figure 11.3. If serverName is one of the variables select it and then select the format, in this case “Text”. The message now looks like this:

The server %1s is down

When this alarm occurs the “%1s” is replaced by the first variable (1), which is the variable value for serverName.

NOTE: Don’t change the number manually. If the “1” in the above example is changed to a number higher than the available variables, unexpected results could occur.

Try to match the format to the variable’s purpose. For example, in the above example using the format “IP Address” instead of “Text” would cause the server name to be displayed in decimal with dots, i.e. 232.53.53.23 which is not its IP address but its name in decimal form.

If no list appears when right-clicking on the message field, the selected alarm does not contain any variables.

To Change the Severity
Select one or more alarms then right-click in the Severity column and select the new severity from the popup list.

To Change the Alarm Name
Double-click in the Name field and enter the desired name.

Main Dialog

Changing Trap Source

SNMPListener has two options to use as the location where the alarm came from.

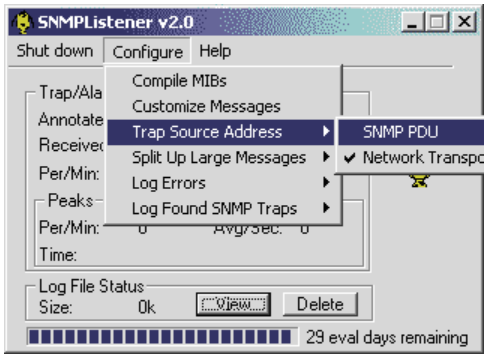


Figure 11.4: SNMPListener Trap Source Address

Option 1 is the SNMP PDU which means it uses the source address field that is part of the SNMP packet This is the default.

Option 2 is the Network Transport source address field.

Split Up Large Messages

Enabled by default. It splits up alarms messages that are longer than 255 characters into multiple alarms. If disabled messages are truncated to 255 characters in length.

12
Network Observer Adapter

Introduction

The Network Observer Adapter (NOA) v1.0 (Service Module) receives and converts the two SNMP traps from Network Observer and translates them into over 120 specific alarms. Each alarm can then be handled using any of the Application Modules like PageManager Pro and Alarm Vocalizer Pro.

Operation

When the NOA receives the SNMP event it uses the translation file called events.ini to translate the event into a more meaningful and useful event message (the Network Observer must send it's SNMP traps to the NotificationWorks PC), then forwards the message to PMPro or AVPro through EventManager.

Items to Configure

1. Install and enable Microsoft SNMP Trap Services
2. Configure the Network Observer to send its alarms using SNMP to the PC running NotificationWorks.
3. From the NOA dialog screen enter the name of the PC along with the Administrator name and password for the PC that is running the Network Observer. This is needed to fetch the list of possible alerts from Network Observer.

That is all there is to it. When Network Observer start sending alerts then you should see the "Total Alarms" counter increasing. If you received any unknown alarms then a log file will be created in the NOA's folder. Just email us this file and we will add support for the new alert.