NETsoft/NETsoft Pro

Alarm over IP (AoIP) Software

Installation & Operating Guide

PIMA

FOR BETTER PROTECTION

NETsoft SOFTWARE LICENSE AGREEMENT

Before you use NETsoft software, please read this agreement. You may use this software only as described in this license.

1. SOFTWARE

The capitalized term "SOFTWARE" used below refers to NETsoft, any updates to the SOFTWARE, any supplemental code provided to you by PIMA Electronic Systems Ltd., the user manual, any associated SOFTWARE components, any related media and printed materials, and any "online" or electronic documentation.

2. COPYRIGHT

3. EVALUATION VERSION

You may use (launch) the SOFTWARE 60 days or 75,000 events (which ever comes first) for evaluation purposes without any charge. The SOFTWARE can be installed on as many computers as you wish. Upon purchasing your license, a USB key will be supplied which will allow you to continue to use the SOFTWARE uninterrupted. Otherwise, you must delete (uninstall) the SOFTWARE from your computer. For information on buying this product, contact your local PIMA distributor or check PIMA's web site: http://www.pima-alarms.com.

4. REGISTERED VERSION

Upon enabling (via the hardware code key) the SOFTWARE, you may use it on any computer as long as the hardware code key is installed. You may also make copies of the SOFTWARE for backup or archival purposes. Otherwise, you may not copy the SOFTWARE in whole or in part. You may permanently transfer all of your rights to the SOFTWARE under this license provided you transfer all copies of the SOFTWARE, the hardware code key and the recipient agrees to the terms of this license. All rights not expressly granted under this license are reserved by PIMA Electronic Systems Ltd.

5. DISCLAIMER

PIMA Electronic Systems Ltd. does not represent that its software may not be compromised and/or circumvented, or that the software will prevent any death, personal and/or bodily injury and/or damage to property resulting from burglary, robbery, fire or otherwise, or that the software will in all cases provide adequate warning or protection.

You understand that a properly installed and maintained computer and software may only reduce the risk of events such as burglary, robbery, and fire without warning, but it is not insurance or a guarantee that such will not occur or that there will be no death, personal damage and/or damage to property as a result.

Pima Electronic Systems Ltd. shall have no liability for any death, personal and/or bodily injury and/or damage to property or other loss whether direct, indirect, incidental, consequential or otherwise, based on a claim that the software failed to function.

You acknowledge that you have read this license, understand it and agree to be bound by its terms.

Please refer to a separate warranty statement found on PIMA website at:
http://www.pima-alarms.com/site/Content/t1.asp?pid=472&sid=57

6. WARNING

You should follow the installation and operation instructions and among other things test the Product and the whole system at least once a week as well as perform scheduled backups. For various reasons, including, but not limited to, changes in environment conditions, electric or electronic disruptions and tampering, the Product may not perform as expected. The user is advised to take all necessary precautions for his/her safety and the protection of his/her property.

7. DISTRIBUTION
The SOFTWARE may be distributed under the limitation and rights from PIMA Electronic Systems Ltd. in its original unmodified form. The distribution has to include all files and code key hardware as in its original distribution.

8. OTHER RESTRICTIONS
You may not modify, reverse engineer, decompile or disassemble the SOFTWARE in any way, including changing or removing any messages or windows. You are not allowed to change any part of the SOFTWARE. You are not allowed to rent, lease, or lend the SOFTWARE. PIMA Electronic Systems Ltd. keeps full rights to change any part of the SOFTWARE.

9. TERMINATION
This license terminates if you fail to comply with its terms and conditions. If your license terminates, you must destroy all copies of the SOFTWARE and return to PIMA Electronic Systems Ltd. the code key you have. The termination of this license does not limit other rights that PIMA Electronic Systems Ltd. may have by law.

If you have any questions about this license agreement, please mail to: support@pima-alarms.com

Table of Contents

INTRODUCTION

NETsoft is PIMA's Alarm over Internet Protocol (AoIP) software, for receiving events sent by the intruder alarm systems via Ethernet. The reports are encrypted (using AES 256bit algorithm) and sent by PIMA's Hunter-Pro Series panels via net4pro or GSM-200 to the Central Monitoring Station. NETsoft decodes the reports and transfers them to the management software (e.g., 'Andromeda') in a standard protocol (e.g. Contact ID).

The Pro version adds line monitoring, anti-substitution and anti-replay protection.

NETsoft can be installed on the Monitoring Station's control PC, but is recommended to be installed on a dedicated PC (see hardware requirements further on).
The connection to the Monitoring Station software can be via a physical COM port or a virtual COM, using a Virtual COM Port (VCP)[1] application.

The Demo version

The Demo version of the NETsoft is a full featured version that is valid for 60 days. It does not require you to use the HASP key (see page 8). If you decide to purchase the product, you will only need to plug in the key before the 60 days are over. When the demo period is over the NETsoft halts and displays an error message: "Feature has expired (H0041)"

As soon as the HASP key is plugged in the NETsoft becomes functional again.

Preliminary Required Information

1. The encryption key (used also by the net4pro and GSM-200). Without the key the NETsoft cannot communicate with the alarm system.
2. The COM port that will be used by the NETsoft.
3. The PC station's fixed IP address.

Recommendations

- Disable any screen saver.
- Disable Windows XP firewall[2].
- Disable any anti-virus application.
- Disable Windows automatic updates feature.
- Install external firewall application[2].

[1] See, for example, http://www.fabulatech.com/virtual-serial-port-kit.html

NETSOFT

Hardware Requirements

- Intel Pentium 4, 2.4 GHz processor and higher, or equivalent
- Network card
- 1024 MB RAM
- 20 MB of available hard-disk space
- Available COM & USB ports
- CD drive (for installing the software only)

Software Requirements

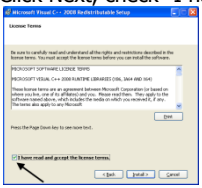
- Operating System: Windows XP SP2 Pro
- IP port #10001[1].
- The default user must have administrator authorizations.
- Visual C++ runtime environment (included in the installation).

Installation

1. Insert the installation CD and wait for the installation wizard to start. If it doesn't start, click the file "netsoft.exe" located in the CD.
2. Click Next, check "I accept the agreement" and click Next again.
3. Click Next as required, then Install.
4. When installation is finished leave the wizard open.
5. The Microsoft 2008 Redistributable Setup starts.

If the Visual C++ is already installed on the PC, click Cancel in the pop-up window.

6. Click Next, check "I have read and accept the license terms" and click Install.



7. Click Finish when installation is done and restart the computer.
8. Press 'Restart now'.

---

[1] NETsoft uses port #10001 to receive events from the network. When using firewall, router, NAT etc., this port must be enabled and/or forwarded. See Appendix A, page 22.

Installing the HASP© Key Runtime Environment

HASP© is a copyright protection USB key. NETsoft cannot run unless the HASP© key is plugged in. The NETsoft checks if the HASP© key is in place every few minutes.

Follow the 2 screen installation wizard. Take notice that it takes about a minute or two for the installation process to end.

If the key is not plugged in, NETsoft stops running and displays error messages: "HASP not found (H0007)"... "HASP session broken (H0039)".

Plug in the HASP key; you can now run the NETsoft.

CONFIGURING THE netsoft

In the Login window, type and retype your password (case sensitive) for the application. Click OK.

Do not lose your password. It cannot be recovered!

The NETsoft configuration window is displayed when logging in.

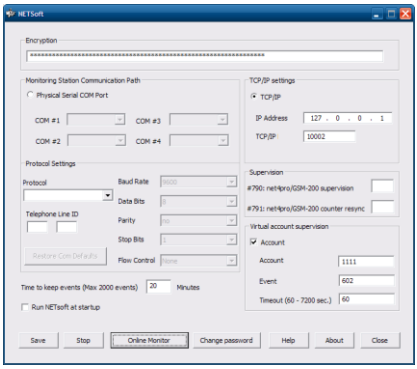


Figure 1. NETsoft's configuration window

The Encryption Key

The encryption key is a 64 characters hexadecimal number. As such, it can include only the digits 1-9 and the letters A-F (not case sensitive). The exact same key is used by the net4pros and GSM-200s.

Next is an example for 64 characters hexadecimal number. It is made of 8 groups of 8 characters in each. When entering a Hex number, do not leave any space between the groups:

A56F85B1 44C7D4EE 91532DF6 E8F53777 AF395F69 CC5375A5 D9EE4658 B29FC62A

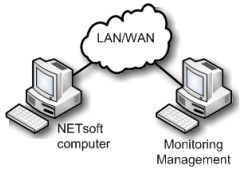
- **Any mismatch between the encryption keys will disable any communication between the panels and the NETsoft.**
- **The software, as well as the transmitters, is configured with a default code, created during QA tests. This code should be changed after installation. Failing to do so will create a security risk!**
- **Write down the code and keep it in a safe place.**
- **If the code is lost and the software needs to be reinstalled, the code cannot be recovered!**
- **It is recommended to make two copies and keep one of them in a safe place outside the premises.**

Delete the default encryption key and enter yours. The key is concealed by asterisks and cannot be revealed otherwise.

COM port settings

Physical Serial COM Port

If the NETsoft is connected to the Monitoring Station via serial communication you can set the priority of the PC COM ports. NETsoft tries to report through the first port you choose once and if it fails, it tries through the second port and so on, until it succeeds. NETsoft will keep using that port from that point on, unless it fails too.



TCP/IP settings

Choose this option if the NETsoft is connected to the Monitoring Station via TCP/IP network. Enter the [IP Address] of the destination Monitoring Station PC.

The Monitoring Management application should be configured to listen to IP 127.0.0.1 port #10003.

Enter the [Port Number] assigned for the Monitoring Management application PC. The default output port is #10003.

- If the NETsoft is installed in the Monitoring Management application PC, the NETsoft should be configured to send reports to the PC's LAN IP, e.g., 192.168.25.4, port #10003.
- The NETsoft's port used for receiving reports from the panel should not be the same as the port for sending the reports to the Central Monitoring Station application.

Time to keep events

Set the time in which incoming events can be kept in the application buffer. The buffer is used whenever the NETsoft cannot immediately send the reports to the Monitoring Station. The information in the buffer cannot be directly accessed.
The default buffer size is 20 minutes and the maximum is 1440 (24h). When the buffer exceeds its limit, the first events are erased. If the buffer is set to zero, the NETsoft will only try once to send the reports.

Protocol

Each Monitoring Management application can be using a different protocol. When a VCP application is used, the output communication parameters (i.e., baud rate, data bits, etc.) must be identical to the Monitoring Station settings.

1. From the drop-down menu, select the **`[Protocol]`** used by the Monitoring Management application.
2. If you need to fine tune the protocol's parameters, set the Baud Rate, Data Bits, Parity, Stop Bits and Flow Control**.**

The protocol data parameters - Baud Rate, Data Bits, Parity, Stop Bits, & Flow Control - are set automatically, according to the protocol defaults. Nevertheless, you should re-check the parameters.

Telephone Line ID

In some protocols the telephone line through which the report is received in the Monitoring Station, can be identified using a two digit hexadecimal number. These fields are enabled when these protocols are selected.

The Restore Defaults button resets all the protocol data parameters to their defaults.

Convert to other ContactID events

Events #790 and #791 are events generated by the intruder panel, for supervision. The two can regularly be converted to any legal ContactID event. Just pick any ContactID event and NETsoft will replace the internal one with the one you've chosen, anytime it reports to the Monitoring Station.

Virtual account supervision

The Central Monitoring Station management application can supervise NETsoft by referring to it as a common subscriber. This is done by giving NETsoft a virtual account ID and setting intervals to receive the supervision reports. A 'no supervision' event can then be generated should the report is not received within the interval time.

The supervision event is sent only if the buffer is empty at the interval time.

Account

Enter the account number to be used by the Monitoring Station software to monitor the NETsoft events.

Event

Set a ContactID event that will be used as a supervision event for the NETsoft. The default event is 602: Periodic test report.

Timeout

Set the timeout for the supervision event. It can be set between 60-7200 seconds.

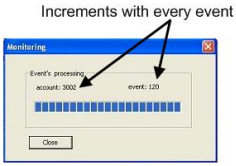
Run NETsoft at startup

This checkbox MUST be checked to make sure continuous operation of the receiver, in case Windows reboots.

Run/Stop

Click this button to run the NETsoft when applying changes (after stopping the NETsoft) or if it is not running from any reason.

Online Monitor



This button launches a monitor that displays incoming events with their account and event ID and a progress bar. It is a useful tool to check that events are coming in and for troubleshooting.

Change password

Click to change the application login password.

Close

Click to stop the NETsoft application and exit the application.

Closing the NETsoft terminates the communication with the Central Monitoring Station. Events will not be received nor sent!

Running NETsoft

Before running NETsoft check the following:

1. Disable any firewall, antivirus and such applications on the PC where NETsoft is installed
2. Check that no user password is set to the default user, i.e., when Windows starts, no password is requested to log-in
3. Disable any settings of a screensaver

4. Disable auto-update of the operating system (such as Windows Update)
5. Network cord is connected.
6. IP address is configured.
7. HASP key is inserted to a USB port.

Click the RUN button. On the tray you'll find the NETsoft icon:

When GREEN: NETsoft is running.

When RED: NETsoft is idle (no event is received or sent).

In case an alert message pops up (e.g. by a firewall software), click 'Unblock'. Otherwise, NETsoft could not run!

NETsoft PRO

What's in the package?

1. A CD containing:
   - NETsoft Pro setup file: "NETsoft Pro.exe"
   - HASP SRM[1] installation file.
   - Windows C++ runtime environment installation.
   - COMAX (for programming net4pro/net4pro-i and GSM-200).
2. HASP SRM USB key.
3. This Installation and Operating guide.

Installation

During the installation process, several applications are installed. There is a separate process for each and the installation wizard invokes them all, one by one.

1. Insert the setup CD and wait for the installation wizard to start.

   If no window pops-up, double click the file "NETsoft Pro.exe", located in the installation CD.

2. In the pop-up window, select the installation language and click 'OK'.
3. Click Next, choose "I accept the agreement" and click 'Next' in the next screens until the "Ready to Install" screen. Click 'Install'.

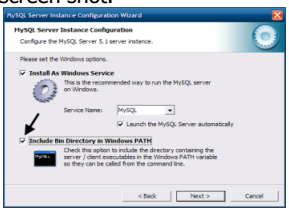
Installing MySQL[2] Server Instance

When the first stage ends, the "MySQL Server 5.1" installation wizard starts. Click 'Next' 3 times (do not change the default settings), then click 'Install'. When this wizard finishes, the "MySQL Sever Instance Configuration" wizard opens up. A command line window is also opens up in the background.

1. Click 'Next' 9 times until the next screen appears. Only in the first time you install MySQL, check "Add firewall exception for this port".

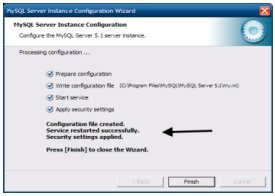
[1] For information and Support: http://www.aladdin.com/support/hasp-srm/enduser.aspx
[2] www.mysql.com

2. Click 'Next' twice and check "Include Bin Directory in Windows PATH". See the next screen shot.



3. Click 'Next'. Enter a new password and enter it in the "New root[1] (Master user) password" and "Retype" fields. The password is alphanumeric and case-sensitive. Write down and keep the password for future use.
4. Check "Enable root access from remote receivers".

5. Click 'Next' and then 'Execute'. Wait for the installation to end.
6. When the wizard finishes successfully, the next confirmation message appears: "Configuration file created. Service restarted successfully. Security settings applied". Click 'Finish'.



[1] The Master username 'root' cannot be changed, both in PIMAnet & HeidiSQL

If in this stage installation fails (you receive an error message), you need to uninstall the MySQL Server Instance, delete its folder under 'C:\Program Files' and re-install it.

Installing Windows Visual C++ Runtime Environment

See NETsoft installation from page 7.

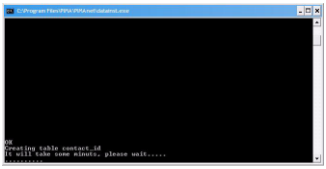
Installing HASP Runtime Environment

See NETsoft installation from page 8.

After the installation insert the HASP key to a USB port.

Creating the My SQL ContactID tables

The next is a command prompt window where you are asked to enter the MySQL 'root' password and click Enter. The wizard now creates the ContactID events table.



Click 'Restart now' when the process is over to restart the PC.

CONFIGURING NETSOFT PRO

The Main Window

NETsoft Pro has 6 services that are accessed through the main window. The services are: NETsoft Pro server, Events, Setup, Accounts, Log & Responses.
The 'Setup' window contains a drop-down menu and 3 buttons: Run & Stop by which the services are run and configured, and Logout, to switch between users.

Some changes made into the server must be applied by stopping and re-running it (see how in the next section).

Figure 2. NETsoft Pro main window

Figure 3. The drop-down menu

The drop-down menu includes the NETsoft Pro services:

1. **NETsoft Pro Server**: by which the NETsoft Pro is run & stopped as well as logged out of the server.
2. **Events**: A table that lists the last 100 incoming events. It refreshes every 5 sec.
3. **Setup**: Configure NETsoft Pro.
4. **Accounts**: Add, manage or delete NETsoft Pro's accounts.
5. **Log**: The application log.
6. **Responses**: Configure the way NETsoft Pro handles each event.

Setup

'Setup' is NETsoft Pro configuration window. To display the Setup window, select it from the main drop-down menu and click 'Run' (see 'Service Manager' on page 27).

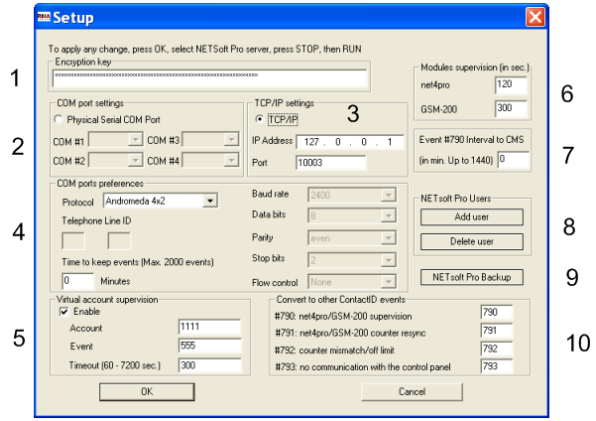
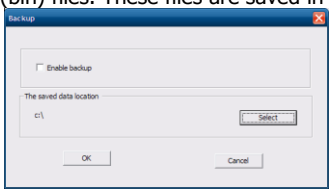


Figure 4. NETsoft Pro Setup window

1. The encryption key: see page 8.
2. COM port settings: see page 9.
3. TCP/IP settings: see page 9.
4. COM port preferences: see page 10.
5. Virtual account supervision: see page 10.
6. Modules supervision: NETsoft Pro supervises the net4pro's and GSM-200s every 20 minutes by default. The minimum should be 1½ times the control panel's supervision time. Note that the NETsoft Pro supervises each module per each customer separately.

7. Event #790 Interval: this is a unique event that is generated by the alarm system for the purpose of supervising by the NETsoft Pro. Since the Central Monitoring Station may have to supervise hundreds and even thousands of modules, the NETsoft Pro can report the Central Monitoring Station on this event only occasionally, in the interval set here.
   The range is zero (no interval. All reports are sent to the management software immediately) to 1440 (a day).
8. Add and Delete Users: Here you can add and delete the application users. There are 2 types of users: Administrator and User. The difference between the two is that a user can only view the information (events, accounts etc.) but cannot access the Setup window, while the administrator has all authorizations.
9. NETsoft Pro Backup: set the path to the NETsoft Pro backup file. NETsoft Pro backs-up all its information daily at midnight. The logs are saved by day, month and year in binary (bin) files. These files are saved in folders that NETsoft Pro automatically creates.



A. To enable the backup, check 'Enable backup'.
B. Click 'Select', choose where the location of the backup file and click 'OK'.

1. **The NETsoft Pro package also contains a full back script that includes the database files too. This script runs separately. If you change the default location of the NETsoft Pro backup, you need to update the full backup script. See how in page 21.**
2. **It is recommended to save the backup file on a different computer and to backup it to an external device.**

10. Convert to other ContactID events: The NETsoft Pro uses 4 events for Alarm system supervision, anti-substitution and reporting on faults. The events are described in Responses, on page 20.
    These events are non-standard ContacID reports. They can be converted to standard ContactID events and be handled by the monitoring station accordingly. For each of the four, set a ContactID event that will be reported to the Central Monitoring Station instead of the NETsoft Pro event.

Accounts

From the main drop-down menu, select 'Accounts' and click 'Start'. 'Accounts' refer to subscribers: these are the net4pro and GSM-200 modules that are connected to the application.

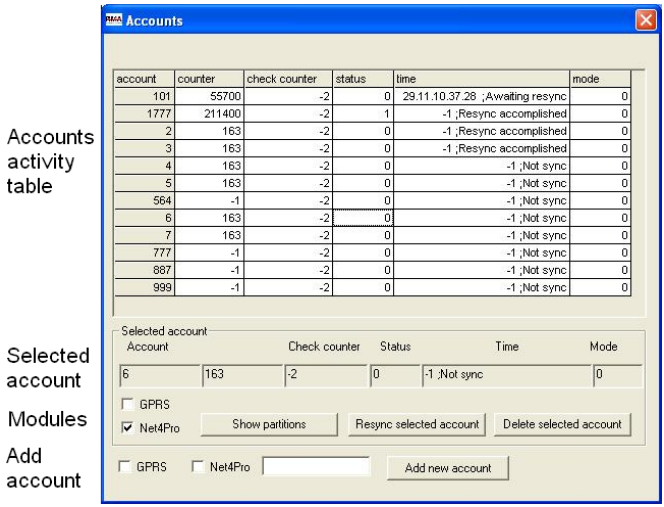


Figure 5. The accounts window

1. To add a new account check the module/s, fill-in the account number and click 'Add new account'. The new account is added to the accounts table.
2. To change and re-sync an account, select it from the table. Its details will be displayed under the table. If you try to add or remove a module you are prompt to approve it.
   To re-sync an account, click the Re-sync button. The NETsoft Pro waits for the Hunter-Pro Series alarm system to send sync event. In the alarm system enter the Master code then -->ENTR-->BACK-->BACK-->ENTR.

   - Re-syncing time is up to 4 hours.
   - Syncing details appear in the Time column.
   - Syncing event is #791.
   - The table is refreshed

3. To display the account partitions, click 'Show partitions'.

   Only partition #1 is synchronized. The log, however, keeps the events with their respective partitions

EVENTS

The Events window displays the last 100 incoming events of the current day, with all the related information. To display this window, select 'Events' from the main drop-down menu and click 'Run'.

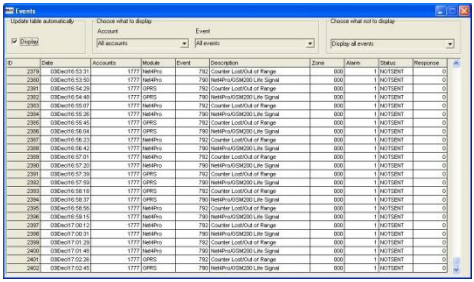


Figure 6. The events window

1. Update table automatically: check this checkbox to display the incoming events and refresh them every 10 seconds. If this checkbox is not checked, the table is empty.
2. Choose what to display:
   Account: choose an account that its events will be displayed.
   Event: Choose an event that will be displayed. Choosing both account and event will result in displaying the selected event type of the selected account.

THE LOG

Select 'Log' from the drop-down menu and click 'Run'.

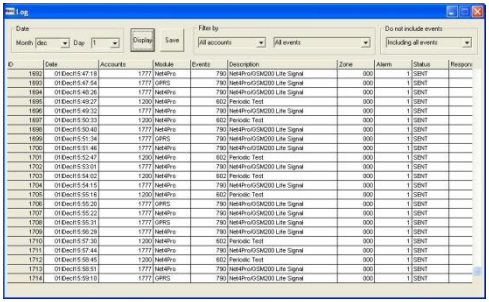


Figure 7. The log wondow

1. Date: the date to display in the log table.
2. Display: to display and refresh the log.
3. Save: to save a text file of the log.

4. Filter by: to choose which events to display.
5. Do not include: to choose which events will not be displayed.
6. The table columns:

   ID: The event ID.

   Date: The date and time the event was received

   Module: The module that was used to report the event

   Events: The event number

   Description: A description of the event

   Zone: The reported zone number, or the subscriber number (only if stated in the report).

   Alarm: NETsoft Pro monitors 3 types of alarms:

   1: Zone violated or system disarmed.

   3: Zone reset or system armed.

   (1-): NETsoft Pro self reports (to the monitoring station), i.e. disconnection, mismatched counter.

   Status: The status of the report.

   Response: The response to the event.

Responses

The responses table lists all NETsoft Pro events and their available responses. The events are standard ContactID events with some NETsoft Pro's:

- 790: net4pro/GSM-200 supervision
- 791: net4pro/GSM-200 counter resync
- 792: Counter mismatch/off limit
- 793: No communication with the control panel
- 796: Unable to output TCP signal (not available in the current version)
- 798: Control/Stu Comms Fail (not available in the current version)

For every event, select one of 4 options (numerated 0-3):

- 0: The event is logged and sent to the monitoring station software.
- 1: The event is only logged. For example, repeating fault.
- 2: The event is sent to the monitoring station but not logged, e.g., technician tests.
- 3: The event is neither logged nor sent to the monitoring station.

To change the response for a certain event, click the event row in the table. Each mouse click changes the option. When done, click the 'Save changes' button.

Any change made to the Response table, such as changing the response to fire alarm, will be applied to all the accounts.

Full Backup

NETsoft Pro has 2 backups: the first is to backup the software logs; this is done by clicking the backup button in the 'Service Manager' window (see page 15).

The second option is to fully backup all the information stored by NETsoft Pro and MySQL, including all event history, NETsoft configuration files and its entire database.

To do so in a single step: on the desktop, locate a shortcut to a file called "NETsoft Pro_instant_backup" (created during the installation) and double-click it. This is a shortcut to a batch file that creates a desktop folder called "Backup" and copies into it the following: Information from NETsoft Pro and MySQL and the backup folder located on drive C (or anywhere else, if you have updated the path. See the next sub-section).

The whole process is short and ends up with a confirmation message. Make sure you backup this file on a different media or network drive regularly.

The backup folder is created when running the backup batch file for the first time. In the next run the folder is written over during the backup procedure.

Changing the backup location

In case the default backup location (in drive C) has been changed, you need to change the desktop shortcut for the "NETsoft Pro_instant_backup" file. To do so:

1. Right-click the shortcut and choose 'Edit'.
2. Change the path in both 'Target' and 'Start in:' to match the new path.
3. Click 'Save & Exit'.

TROUBLESHOOTING

Virtual COM Port

If the Monitoring Station software does not support TCP/IP communication, it is still possible to use TCP/IP communication by using VCP (Virtual COM Port) software. This software creates a virtual COM port that receives events via TCP/IP and sends them to the Monitoring Station software, just as if it were connected via physical COM port.

When a VCP is used, it is important to configure its parameters (i.e., baud rate, data bits, etc.) to match the protocol settings.

Changing NETsoft default listening port

1. In case the default incoming IP port #10001 needs to be changed, open the file "port_pima.txt", located in your root path (c:\) and replace the number in it with the port number you need. Do not enter any other character or spaces, before or after – just the port number.
2. Save the file.
3. Run NETsoft. The application automatically checks the root directory for this file and uses the port number in it.

PIMA NETWORK PRODUCTS

net4pro

Network card for connecting intruder alarms over TCP/IP (Ethernet). Supports both IP and URL.

net4pro-i

Xport™ based network card for connecting the Sentinel repeater and the VKD4net virtual keypad, as well as non-PIMA panels.

GSM-200

GSM cellular transmitter; can be used as primary or backup GPRS communication channel.

PIMAnet Pro

A Monitoring Station Alarm over IP receiver and decoder. The PIMAnet Pro supervises line tampering with anti-substitution and anti-recording mechanisms. It Pro also supervises the connection status of the intruder alarms.

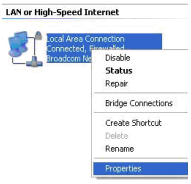
APPENDIX A: CONFIGURING THE IP ADDRESS

Since the DHCP server automatically assigned the NETsoft Pro an IP no. which is probably different from the one your system administrator had assigned, you should now configure it with the static IP no.

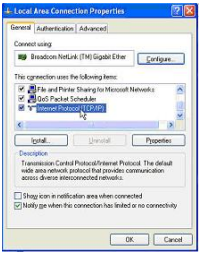
It is recommended that a certified technician would perform the next steps.

1. In Windows taskbar click 'Start' -> 'Control Panel' and double-click on 'Network Connections'.

2. In the opened window, right-click 'Local Area Connection and select 'Properties'.



3. Scroll down and double-click on 'Internet Protocol (TCP/IP)'.



4. Click 'Use the following IP address' radio button and fill-in the 3 parameters: 'IP address', 'Subnet mask' and 'Default gateway' (ask your system administrator for the details).
When using the PIMAnet over WAN, fill the DNS addresses.
The numbers in the image are for example only.

5. Click OK here and the next 'Local Area Connection' window.

APPENDIX B: PORT FORWARDING

Port forwarding is a rule in which firewalls enable a computer from one network to connect to a computer located in another network (LAN). The internet computer must have a destination IP address with a specific port number. The router, through which the LAN computer is connected to the Internet, forwards the connection to the LAN computer (see next drawing).

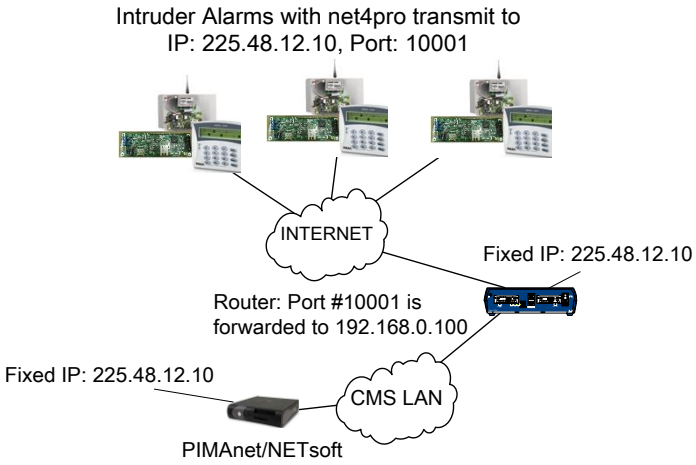
Port forwarding must be used for the net4pros and GSM-200s to connect to the Monitoring Station.

As mentioned in this guide, by default, NETsoft is configured to use port #10001 to receive communication from the net4pros and GSM-200s. Since the Monitoring Station must have a fixed IP address, the net4pros and GSM-200s must be configured with that IP no. and port #10001, which must be forwarded.

For a list of routers and their port forwarding information, see https://portforward.com/store/pfconfig.cgi

Once port forwarding is configured, any net4pro and/or GSM-200 over the internet, trying to communicate with the Monitoring Station IP address and port #10001, will be forwarded to the PIMAnet within the Monitoring Station LAN.

Illustration of Port Forwarding



APPENDIX C: CHANGING USERNAMES & PASSWORDS IN PIMANET PRO

In PIMAnet Pro© receiver only, NETsoft Pro has 2 identical sets of usernames & passwords for Windows logon and for the application logon. These are (default):

Username 1: 'root' Password: server

Username 2: 'Admin' Password: 1234

The 'root' user (both in Windows and in NETsoft Pro) should not be changed. However, the default password for both users should be changed after installation.

The next steps should be taken only by an expert, since it involves changing the Windows registry. Be sure to backup the registry before making any change into it.

Enabling Windows auto logon

In case of system reboot, the NETsoft should run immediately and for that purpose, Windows logon should be automatic. If the PC is not part of a Windows workgroup, see Microsoft's tip at http://support.microsoft.com/kb/315231

If it is part of a workgroup, follow the next steps:

Edit the file "Auto Login.reg", located by default in C:\Program Files\PIMA\PIMAnet:

a. Right click on the file and choose Edit.

b. Replace the text 'DefaultUserName' with your Windows username.

c. Replace the text 'DefaultPassword' with your Windows user password.

d. Save the file and then double-click it. Windows will now update the registry with the new username and password.

To change passwords, in Windows XP, go to 'Start' -> 'Control Panel' -> 'User Accounts'. Click the desired account and then Properties, where you can change its password.

The user 'Admin'

In PIMAnet Pro receiver only, NETsoft Pro must start automatically in case Windows reboots. To enable it, the Admin username and password must be registered in the Windows registry (as they are by default). If the defaults are changed, the registry must be updated with the new data.

To do so, locate a file called 'Auto Login.reg' in 'c:\program files\PIMA\Setup'. This is a special text file, that when executed, it automatically changes Windows username and password in the Windows registry.

Right-click the file and choose 'Edit'. Locate the 2 text lines: "DefaultUserName"="Admin"; "DefaultPassword"="1234".

Replace the 'Admin' and '1234' with new username and password. Save the file, exit the text editor and double-click the file. Click 'Yes' when asked.

The user 'root'

The Windows 'root' user was created for PIMA support purpose. Therefor, unless you plan not to use the support offered by PIMA, it is advised not to change this user. You can, however, change this user's password.

Configuring Network devices and software

Any network device or software that controls the data traffic must be configured to allow the communication to pass through it, before working with NETsoft Pro. That includes Firewall, Router, NAT, etc. Failing to do so will prevent the PIMAnet Pro to communicate and function in any way.

By now, your system admin knows that you connect the NETsoft Pro receiver to the local network. He also knows the information needed to configure the network traffic control devices: the NETsoft Pro static IP no. and incoming and outgoing ports. Make sure all the devices are configured, before you try to communicate with the net4pro's or GSM-200s.

Installing the HeidiSQL Application

HeidiSQL (http://www.heidisql.com/) is an easy-to-use interface and a "working-horse" for web-developers using the popular MySQL-Database. It allows you to manage and browse your databases and tables from an intuitive Windows® interface.

When the installation wizard starts, Click 'Next', check 'I accept the agreement' and click 'Next' 4 times, and then 'Install'.

Follow the installation wizard and at the last screen, where you need to click Finish, uncheck "Run Heidi now", than click Finish.

Changing the password for NETsoft Pro 'root' user

NETsoft Pro has 2 predefined users: 'root' and 'Admin'. The username 'root' cannot be renamed, only its password can be changed. The 'Admin' user can be changed, but to do so one needs to login as 'root' user.

To change the 'root' password:

1. Go to 'Start\All Programs\MySQL\MySQL Server 5.1' and click "MySQL Server Instant Config Wizard"
2. Click Next until the checkbox "Include Bin Directory in Windows PATH". Check it.
3. Click Next to the screen "Modify Security Settings".

4. Enter the current and new root password. The default password is "server"
5. Click Next and then Execute.

After changing that, the instant backup file must be updated with the new details. The shortcut "NETsoft Pro_ instant_backup" is located on the desktop. Right-click the file and click "Edit".

Look for "user=root --password=server", replace the password (in PIMAnet Pro receiver, the default is 'server') with the new one and save the file.

APPENDIX D: ERROR MESSAGES

Service Manager

When starting the 'Service Manager', if the error: "Reboot application. Username or password problems" appears press Stop and Logout; then press OK and Start, to restart the application.

NETsoft Pro

Message	**Explanation/Solution**	**Respond**
"Service Started already"	Pressing "run" while the server is already running	Click **[OK]**
HASP not found (H0007) or (H0039)	The HASP key is not plugged in.	Click **[OK]**
"TCP port 10001 is busy by another application. Close this program and restart NETsoft"	Change the port no. or first close the application that uses that port.	Click **[OK]**
Timeout is empty! Action canceled.	Supervision timeout is not set.	-
Impossible use that location, or you have old backup there. Action canceled.	Trying to save the backup over an existing backup. Use a different location.	-
Wrong info or file (3.dat) not exist or failed to reach current user. Process stopped.	Installation errors. Re-install the PIMAnet Pro.	-
Wrong info or file (1.dat) not exist. Process stopped.		
Feature has expired (H0041)	The demo period is over.	-
NETsoft		
Restart Server!	To implement new settings, NETsoft must be stopped and restarted	Click **[OK]**
Supervision signal is enabled, but no account or timeout is defined!	Some or all parameters in the Supervision section in the NETsoft Configuration window are missing.	Click **[OK]**
TCP port 10001 is busy by another application. Close this program and	Change the port no. or first close the application that uses that port.	Click **[OK]**

Message	**Explanation/Solution**	**Respond**
restart NETsoft		
HASP not found (H0007) or (H0039)	The HASP key is not plugged in.	Click **[OK]**
Feature has expired (H0041)	The demo period is over.	-

PIMA Electronic Systems Ltd.
5 Hatzoref Street, Holon 58856, Israel
Tel: +972.3.6506414 Fax: +972.3.5500442
Email: support@pima-alarms.com
Internet: http://www.pima-alarms.com
Partners' website: http://www.pima-alarms.com/site/modules/login.asp

4410256

Version: B1, XX en (Dec 2011)