PSentry™ Software version 3.x
Users Guide

Plus Communications

Published: March 2006
Updated:

This document is provided to you along with the accompanied PSentry™ software. It is for informational purposes only.

PLUS COMMUNICATIONS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Use the PSentry™ Software in accordance to and complying with all applicable laws and regulations is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced without the express written permission of Plus communications.

Except as expressly provided in any written license agreement from Plus Communications, the furnishing of this document does not give you any license to use the product, trademarks, copyrights, or other intellectual property.

Table of Contents

1 Introduction

This is User Guide document for PSentry™ Software. PSentry™ is a handy tool to capture common Internet data traffic over the network. Please read and refer this document to familiarize the product prior to the installation.

This user guide does not contain terms of software license agreement. Please refer the separate document or file license.txt accompanied to the PSentry™ Software. You must read it first and acknowledge you agree to the terms in order to be able to proceed to complete the installation and use the software.

2 PSentry™ main features

When properly installed and configured, PSentry™ Software listens or sniffs over the Internet traffics coming from and to all computers over your LAN, and captures relevant information and record them to disk. PSentry™ can perform following functions as listed in this section below. It automatically saves any activity it detects to history log files according to your system settings. PSentry™ provides a Web Management console through http interface for real time monitoring. It also provides a tool which you can look for any word or text string from the saved history logs.

2.1 Captures Instant Messenger chat conversations

a) PSentry™ captures and records common instant messenger conversations including MSN, ICQ, AIM, Yahoo and Tecent's QQ over the local network. PSentry™ automatically saves all messenger conversations in daily log files for easy retrieval.

b) Shows real time status of all user names and IDs who is chatting online over your network through instant messenger programs.

c) Easy configuration tools to apply flexible policies governing the use of instant messenger. You may use PSentry™ to selectively block or permit based on user ID (using white list or blacklist user) or based on type of chat tools (example allow MSN, AIM, but block ICQ).

2.2 Customizable web surf control policy

a) PSentry™ can record all web sites domain names (URL addresses) visited by users from your LAN (or computers at home if installed at your residence), and save the surf activity log to files by IP address and dates.

b) PSentry™ provides you the flexibility to customized surf control policy. You may selectively block or permit certain websites address at your discretion, by applying white list, or black list.

2.3 Intercepts and records emails

a) PSentry™ intercepts and records all incoming and out going saved them in history log files. All details of message are contained in log files, including message contents, recipients list, as well as email attachments.

b) PSentry™ captures smtp/pop3/imap emails as well web based email.

c) PSentry™ allows you to customize email policy, to selectively block email based on user ID, or based on computer IP address.

2.4 Captures web postings

a) PSentry™ can capture user postings or content submission to websites from your LAN, such as web based email, bulletin board, file attachment upload, etc

b) You pay set PSentry™ to activate or deactivate your blocking policy to permit or restrict users on your LAN posting onto websites.

2.5 Controls and monitors file transfers

a) PSentry™ may monitor and control file transfers through http and ftp in both download and upload directions.

b) PSentry™ also monitors and controls file transfers through MSN and other p2p file sharing software.

c) You may set your PSentry™ with file transfer policies to allow or prohibit file transfers based on file extension, or based on user ID.

2.6 Monitors Internet bandwidth usage and control

a) PSentry™ provides network administrator a simple tool to monitor Internet bandwidth usage by any user or computer from your local network.
b) Use PSentry™ to set maximum bandwidth permissible for each individual computer IP address or user. This ensures enterprise network resources are adequately shared and prevent abuse.

2.7 Flexible Internet control policy

You may create and apply different levels of internet policies for users in PSentry™. Example, you may select only certain users (example by job ranking) with permissions to use of instant messenger, file transfer, email, online game, stock trading, but blocks all others.

2.8 Keyword match event alert.

a) You may set PSentry™ to listen and look for certain keyword, whenever an event occur and a match is found, an email is automatically generated and sent to the email address you pre-defined in PSentry™.

b) You may also search and look for a keyword or text string in history logs that are already saved on disk.

2.9 Statistic reports

a) PSentry™ can generate periodical (example daily or monthly) Internet usage reports either by instant messenger logs, email, bandwidth usage.

b) PSentry™ can be also configured so that daily activity reports and email automatically generated and sent to the administrator.

3 Installation

3.1 Positioning PSentry™ on the network

For the best performance, it is recommended that install PSentry™ on a standard computer running with operating system window XP, Windows 2003 or higher. Windows2000 is also supported. Position the computer with PSentry™ behind an Internet firewall, as shown in Figure 1.

If there is a Windows based proxy server which acts as gateway and serves all incoming and outgoing Internet traffic for your LAN, then you may also install PSentry™ on this proxy server.

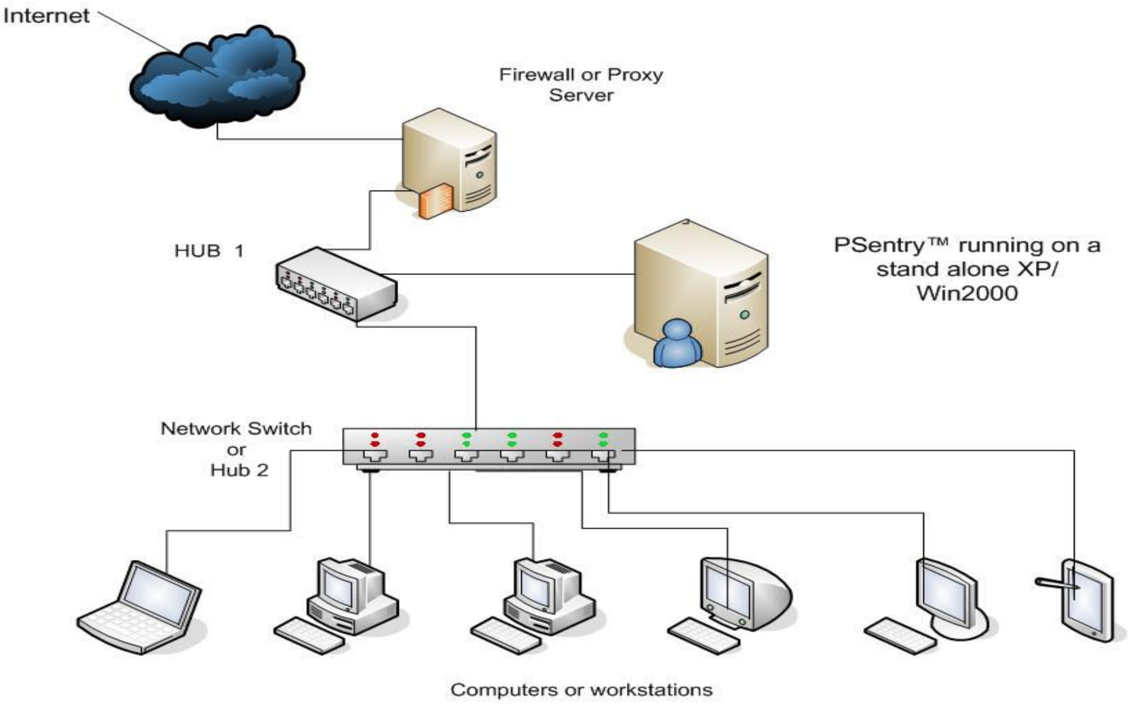
Internet
Firewall or Proxy Server
HUB 1
PSentry™ running on a stand alone XP/ Win2000
Network Switch or Hub 2
Computers or workstations

Figure-1

If the your network connects to a smart switch supports port mirror function, you may enable port mirror and monitoring, then connects the firewall/proxy server and PSentry™ directly to the smart switch in Figure-2. The PSentry™ will be on the listening/monitoring port, and the firewall/proxy server is on mirrored port. In this case, the Hub 1 in Figure-1 is no longer required.

Alternatively, you may avoid using the first hub (Hub 1) in Figure-1 by install two network adaptors on the computer running PSentry™. The external network adaptor connects to firewall or proxy server and the internal network adaptor connect to a switch or hub. You create network bridge or Internet sharing on the computer running PSentry™.

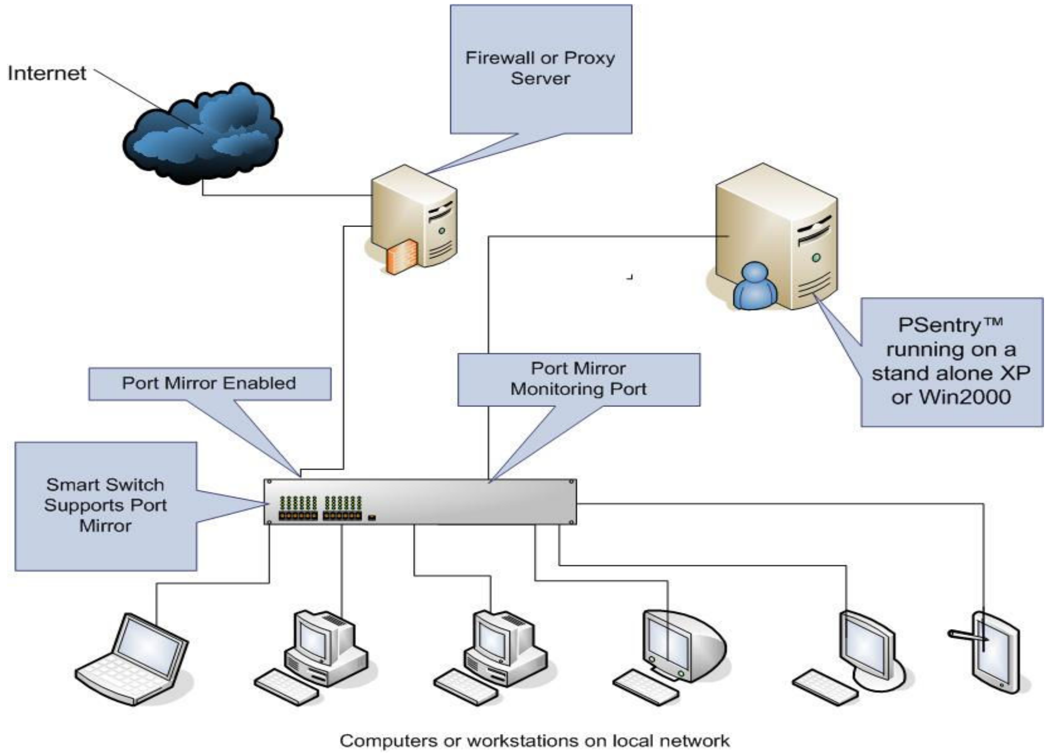
Internet
Firewall or Proxy Server
PSentry™ running on a stand alone XP or Win2000
Port Mirror Enabled
Port Mirror Monitoring Port
Smart Switch Supports Port Mirror
Computers or workstations on local network

Figure-2

3.2 What operating system to run PSentry™

PSentry™ has been tested to run on Windows2000, Windows XP and Windows 2003. Other OS systems have not been tested for compatibility and therefore are not supported.

3.3 Installation Procedures.

a) If your computer contains an earlier version or other types of network sniffer program, please uninstall them prior to install PSentry™.

b) If you have a trial version of PSentry™ installed on your computer, you will need to uninstall the trial version before re-installing the full version.

c) PSentry™ requires operating system loaded with WinPcap driver in order to run. Please verify and see if your computer already contains winpcap driver.

Go to Control Panel ─► Add/Remove Programs and see WinPcap it is listed. If your computer already has WinPcap 3.1 or higher, you may keep the existing version WinPcap driver without having to re-install it. However, if your computer contain version 3.0 or older, it is recommended you shall uninstall the old version and replace it with the latest version or use the one came with PSentry™

The latest version of WinPcap is available on WinpCap.org website. http://www.winpcap.org

d) If your computer do not have WinPcap driver, please install it before install PSentry™. When installation finishes, PSentry™ will automatically start, its sniffer and monitoring service will register to system. Please wait up to few minutes for the service to start up. If you have installed the full version, you'll be required to enter registration information.

4 Operating Instructions

4.1 Start the PSentry™ program

PSentry™ automatically starts when your computer is powered on. Network traffic sniffering and capture and recording process all runs in the background. You do not have to login into local Windows to configure PSentry™.

If you do login into local computer, you will see a quick launch link is on your desktop. It was created during the installation of PSentry™. Click this quick link brings to the entrance to the PSentry™ web management console. If this is first time you enter PSentry™, you shall immediately reset password. The default system administrator name and password are "*admin*, *123456*".

Through this web interface, you can browse and get familiarized with the default settings of PSentry™. You may modify the default configuration according to your Internet use policies. You may create a table to match user name and their corresponding computer IP addresses. PSentry™ will remember and store your custom settings once you click to save.

PSentry™ Software automatically starts to run whenever the computer is turned on, no further user interaction is necessary.

4.2 Remote access to management console

PSentry™ supports local as well as remote administration through a web console. To access data captured and saved on disk, you just need point your browser to port 9090 of the computer running PSentry™.

Enter either the ULR address of the IP address or the netbios name of the computer followed by the port number 9090. Example, if the computer running PSentry™ has IP address of 192.168.0.1 and its Netbios name is im01,

Then open your browser to access the web management console from any computer remotely, the ULR address will be:

hptt://192.168.0.1:9090, or http://im01:9090

4.3 Show all current activity online

"*Show all active online*" is the first page information you see when entering web management console. PSentry™ adapts web interface as management console for easy access and viewing all records.

"*Show all active online*" list all computer IP addresses and their corresponding user names (if a user table is defined), chat sessions, file transfers, email and postings and bandwidth usage that are active online. Click refresh for updated status.

The information page shows the number of chat sessions, number of website visited, number of file transfers, number of emails (smtp/pop3), the number of web postings (including web email) during the day, and current bandwidth use associated with each computer IP address. Each line associate with activities recorded from one computer or one user. Click the numbers will bring more details of the recorded activity.

4.4 Show chatting online

Click the second menu bar "*show chatting online*" will display information all users currently chatting online. It list in a table:

- Sequence Number
- messenger type (aim, yahoo, MSN, ICQ, QQ),
- messenger user ID,
- online since time,
- IP address of the user computer, and
- destination TCP port number.

Click the user ID will bring you details of the chat log.

Please note, because PSentry™ must first detect and collect enough data packets from network before it can assemble and record chat messages. So if you just started running PSentry™, you may have to wait for a minute or two before you see any captured chat conversations

It is also normal that sometimes PSentry™ show "???" in a chat session. This is because PSentry™ has detected some data packets, but not sufficient data is available to assemble user ID or chat content.

The "???" usually disappears when PSentry™ detects more Internet data traffic, or when user start to chat with others.

4.5 Show active surfing online

This information page displays in a table format:

- Sequence number
- User name,
- web site last visited,
- web page title,
- time of the last web visit, and
- Requesting computer IP address.

Click page refresh will renew with latest information.

4.6 Show active file transfer online

The link "*Show active file transfer online*"
This page displays the currently active file transfers.

4.7 Display spot view.

Spot view lists 30 most recent Internet activity corresponding to each IP address or user name.

4.8 Search in history records

PSentry™ provides flexible search capabilities to query each history log files. You may define your query criteria by selecting user name (if user table is defined) or IP address, enter the keyword or character string and select the time frame. Query results show the match found.

4.9 Statistic reports

PSentry™ can generates five (5) types of daily or monthly statistical reports and automatically send to administrator by email.

- Top 10 most frequent online chatters.
- Top 10 most frequent web surfers.
- Top 10 highest amount Internet data user
- Top 30 most frequent sites visited
- Over all Internet activity report

5 Configurations

5.1 Configuration sniffer and control settings

Use the web management interface to configure PSentry™ settings, and view status, user online activities, and history records.

a) Sniffing device – This is the network adaptor that PSentry™ set to listens on in promiscuous mode. If no device is available for this selection, it is probably because no WinPcap driver was found or it was not properly installed. Please try to reinstall the latest version WinPcap. If two or more network adaptor exist on the computer running PSentry™, select the adaptor on the internal network as listening device.

b) System status

5.2 User name and computer table

The user name and computer table contains each user name corresponding to IP address of their computers. This table shall be created and verified for accuracy according to each IP address of computer and user names. Update and save this table in the system.

The check mark "*Applicable*" sets the inclusion or exclusion whether the subject computer is being monitored controlled and its activity logged.

The "*Log activity*" column provides a pull down menu, so you can select the level of recording for each user or IP address. There are four (4) selectable options:

- no record,
- high,
- medium, and
- low.

To customize each recording levels, please click the "*customize event recording levels*" link on this page.

"*Apply blocking rules*" column provides you with options to select a policy to apply each individual user or computer. There are four (4) levels of policies to choose from the pull down menu:

- no blocking,
- high,
- medium and
- low.

To customize each blocking levels, please click and go to "*customize blocking levels*" on this page.

"*Maximum bandwidth*" sets the maximum Internet data flow or bandwidth permitted for a user or IP address, in kb/second. If it is set to "0", then it no limit is set. This is the default setting.

Please note, if your licensed points (N) is less than the total number of computers (M) on your LAN, PSentry™ will sniff and monitor the first N numbers on the network it finds. Other computers on the LAN will not subject to PSentry™ monitor or control. You can either purchase more license points, or deselect those computers that you do not need them monitored.

5.3 Customize event recording levels

Click the "*customize activity recording levels*" link under the user name and computer table will bring you to the configuration setup page.
You can modify each of the PSentry™ default settings of high, medium and low to your own defined recording levels based on your requirements.

The default levels for high, low and medium recording level are as follows:

- High records messenger conversations, web surf, email, and file transfers.
- Medium – records messenger conversations, web surf, and emails
- Low - records web surf activities.

5.4 Customize blocking levels

Click the link under user name and computer address table to set “customize blocking levels”.

PSentry™ has three default settings for high, medium and low levels. You may modify or customize each recording levels according to your own requirements.

The default levels for high, low and medium recording level are as follows:

- High blocks all messenger conversations, web surf, email, and file transfers, online gaming and stock trade
- Medium permits: web surfing, instant messengers, email and web posting, blocks following: ftp, msn file transfers, QQ, telent, ssh, online games and stock trading
- Low – permits web surfing, blocks selected instant messengers, and blocks online game and stock trading

5.5 Select items to block

To select any item to block, click the check mark of the item, and check “*apply*” button to save the setting.

5.6 Black list and white list of website names.

Under the page “Set online blocking rules”, click link “customize website access rules” to create web surf policy with a black list or white list.

The white list contains all website names permitted to access. Any website names that are not on this list are all blocked.

The black list contains all website names prohibited to access. Any website names that not on black list are all permitted.

Under the “control policy”, select to activate either white list or black list.

5.7 Black list and white list for mail domains.

Under the page “*Set online blocking rules*”, click link “*Customize mail access rules*” to create black a list or a white list to set up mail domain access rules.

The white list contains mail domain names permitted to access. Any mail domains that are not on white list are all blocked.

The black list contains mail domain names blocked for access. Any mail domains that are not on the black list are all permitted.

Under the “control policy”, select to activate either white list or black list.

5.8 Black list and white list for instant messengers.

Under the page “Set online blocking rules lick the “Customize user access list” brings you to the page to create white list or black list settings for Instant Messengers.

a) Black list user and messenger pair
The black list contains user ID and messenger type pair that is blocked sending and receiving instant messengers.
Create one entry per line, messenger type followed by user ID. Example,

```
MSN  john_doe@hotmail.com
ICQ  55667788
AIM john_doe
```

If black list policy is activated, instant message sent from or to not matching the entries on black list are automatically permitted.

b) White list user and messenger pair

The white list contains user ID and instant messenger pair who is permitted to chat online using instant messengers. One entry per line, each line messenger type followed by user ID.
If white list policy is activated, only users on the white list can receive and send instant messages. All other users are blocked using IM.

5.9 File transfers black list and white list.

Under the page “*Set online blocking rules*” click the “*Customize file transfer policies*” brings up the page where you can create white list or black list settings with file transfers.

Select whether to activate black list or white list.

a) Black List
File transfer containing the file extensions on black list are all blocked. File transfers containing all other extensions are all permitted.

b) White list
Only those files names containing the extensions on the white list are permitted for transfers. Otherwise file transfers will be blocked by PSentry™.

5.10 Custom defined blocking rules

Under the page "*Set online blocking rules*" click the "*define other communication ports*" brings you to the page where you can add, or change other ports that you wish to control or monitor.

Enter port number=description communication service type, one entry per line.

5.11 Set time table for policy control and monitor

You may set up a weekly cycle time table that PSentry™ activates control and monitor policy rules and capture Internet activities.

PSentry™ will be idle and no blocking rules will apply and no data will be captured for the time outside this time table.

The default time table is set from 0:00 am to 23:59pm, ie. PSentry™ control and monitor policies is effective 24 hours a day. You may modify this default setting to fit your requirements.

6 System administration and event alert notification.

6.1 Default system administrator

PSentry™ provides a default system administrator name: admin, with default password 123456.

For security reasons, It is recommended you change the default password immediately after the initial installation and safe guard your new password.

6.2 Add an administrator into access PSentry™

PSentry™ provides you the ability to add additional system administrators in the system for access, viewing online or log query. Under the page link "PSentry ™ *Administrator*" click the "*add*" to add an operator under PSentry™. You will prompt a page where you can create and assign the administrators with certain privileges. Pick a user name and enter the persons name, set login password, and select one or more access privileges from the following:

View active status online
Query history logs
Configuration settings
Help

6.3 Set email notification on event alert in PSentry™

You may enable PSentry™ to alert you whenever a new event (example a chat conversation) contains any certain keywords. An alert notification then is emailed to you, or to an email address you define.

Check mark the "*activate keyword alert notification*" to enable this feature.

Enter the keywords you select one entry per line.
Enter the smtp server that PSentry™ shall use to send email alert.
If you want alert notification sent to multiple email addresses, separate each email address with a comma "," between them.

You may limit the alert message size sent to email. PSentry™ defaults to file size limit 128 mb.

If the smtp server you use requires authentication, you must enter user name and password for the smtp server.

If you want daily report sent by email, check mark the "*automatically send daily reports*"

6.4 Managing PSentry™ system report logs

PSentry™ provides a handy tool to manage logs or system reports at ease.
You will choose one of the following backup options

- No backup, no delete
- Backup and delete all records N days older.
- Delete all records N days older without backup

Backup Directory: this is the location of disk where backup files will be saved to.

Backup Type: select one of the following:

- Web surf
- Posting to web
- Instant messenger conversations
- Incoming/outgoing email
- File transfers
- Computer turn on and off time

End date: All records of this date and older are set for deletion

6.5 Change administrator password

For security reasons, it is recommended that you change default password immediately after installation of PSentry™

Click the '*change password*" link, you'll be prompted to enter current password and new password. Click "*Apply*". Your new password will be saved into the PSentry™.

7 Troubleshooting common problems

7.1 Common problems with Tecent QQ messenger

My PSentry™ does not detect QQ conversations, why?
QQ messages are encrypted. To capture and record conversations in QQ, you must know and enter the password of the QQ user. After you enter correct QQ ID and password, PSentry™ will capture, display and save QQ conversations.

7.2 Issues with blocking Tencent QQ messenger

My PSentry™ can't block QQ conversations, why?
The current version of QQ instant messenger conversations are commonly sent via port UDP 8000 and UDP 8001. When those two UDP ports are unavailable or blocked, then QQ will attempt to transmit using TCP port 80, and TPC port 443.

PSentry™ provides blocking to TCP port 80 and port 443. PSentry™ cannot block UDP ports. You must use other tools to block UDP port 8000 and 8001 in order to block QQ completely. Example, you may try block those UDP port from your router, or from your firewall.

7.3 I don't see PSentry™ login page

PSentry™ runs only on operating system Windows2000, Windows XP, Windows2003 or higher. To access to PSentry™ login page, your browser must be able to access TCP port 9090. If PSentry™ is running and you can't access to the login page, it is possible your firewall have blocked TCP 9090. Check your firewall settings and try again. If problem persists, you may try with reinstalling PSentry™ again.

7.4 Why PSentry™ doesn't detect anything

First check the connection to local area network. In order to sniff network traffic, your computer running PSentry™ must be positioned and connected properly. Refer the installation section for properly installation procedures.

Next, make sure you have WinpCap driver is installed and working.

From "*Settings*" ─► click to go to "*System Configurations*", if the monitoring device showing correct IP address, it indicates that WinPcap driver is properly installed and running. If the monitoring device is shown as blank, it may indicate that WinPcap driver is not found. You may have to reinstall WinPcap.

If you find WinPcap driver is working fine, and PSentry™ still can't detect anything from the LAN, it could be the wrong monitoring device is selected.

If you have checked both WinPcap and network device both working properly, but problem persists. We recommend you uninstall clean and re-install the WinPcap PSentry™ and try again.

You may contact our technical support for assistance at if you continue experience technical difficulties.

7.5 Why PSentry™ detects only my own Internet activities?

If PSentry™ already detects and records your own Internet activity, it indicates the PSentry™ software is already running correctly. You shall check the network hub or switch. Your computer and network hub must be positioned at right place in order to be able to detect all Internet traffic on the local network.

Please refer the section 3.1 titled "Positioning PSentry™ on the network"

7.6 Why PSentry™ only detects "???"

PSentry™ may only have detected limited amount Internet traffic but not sufficient to show user ID or other content. PSentry™ needs to capture more data flow to fully assemble message content. The "???" usually disappears when PSentry™ captures more Internet activity, or when user start to messenger chats with others.

8 Contact us

You may find help full information from our website

http://www.pluscom.us
http://www.psentry.com

By Postal Mail

Plus Communications
705 Wheaton Court
Allen, TX 75013 USA
Tel: 972-396-0300
Fax: 469-675-8500

Contact us by email:

Info@pluscom.us
support@pluscom.us

Contact us via instant messengers
AIM: PSentryPluscom
ICQ: 280707133
MSN: support@pluscom.us
Skeype ID: PSentry