

The logo for Soft Trek, featuring the words "SOFT TREK" in a stylized, blue, serif font. The letters are slightly shadowed and appear to be floating above a light blue, wavy background element.

ipTicker v2.00

User Guide

Contact Details

Soft Trek Pty Ltd
PO Box 2271
Carlingford Court
NSW 2118
Australia

Internet: <http://www.soft-trek.com.au>

Support: support@soft-trek.com.au

Sales: sales@soft-trek.com.au

Table of Content

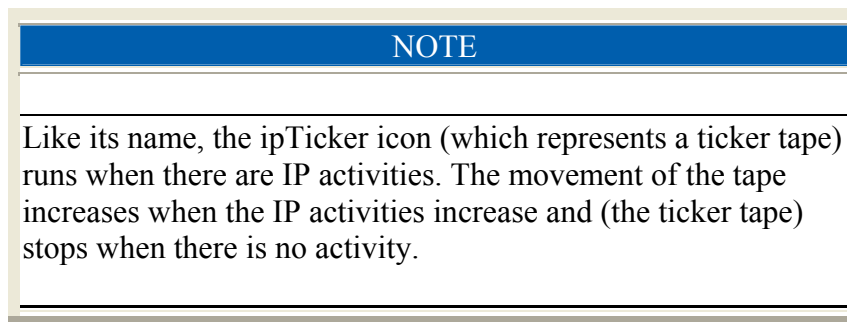
Overview.....	3
What is ipTicker?.....	3
Quick Start.....	5
What do you need to run ipTicker?.....	5
How to install ipTicker?.....	5
How to uninstall ipTicker?.....	6
IpTicker Operation.....	7
Using IpTicker.....	7
To run ipTicker in its iconic mode.....	13
How to exclude an event.....	13
How to manage excludes.....	13
How to determine if an event has changed.....	13
Checking ipTicker Version.....	14
IpTicker Alarms.....	15
The Alarm algorithm.....	15
Configuring the Alarm options.....	16
Configuring your Safe Ports.....	16
Configuring your Safe Countries.....	18
Configuring your Safe IP Addresses.....	19
Managing Alarms.....	19

Overview

What is ipTicker?

IpTicker is a diagnostic tool that detects and measures IP (internet protocol) traffic to and from your PC. It listens to all ports and reports the activities centrally on its screen in real time. It reports IP activities in following ways: -

- A summary screen – where it shows the IP statistics group by the IP address, direction and port
- An active audit trail screen where it shows the current IP activities
- An active alarm screen where it shows the current IP alarms
- A dump screen where it shows the most recent dump of TCP/UDP data

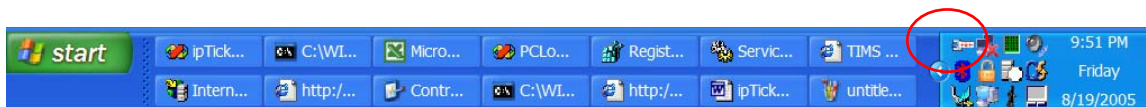


Here are some sample scenarios where ipTicker could be useful: -

Determine if there is any IP traffic.

You surf to a web site. Your browser icon keeps spinning showing that it is doing work. Normally you would associate the spinning of the browser icon as IP activity (as there are data being downloaded to your browser). IpTicker icon shows the same behaviour (it runs when there are IP activities).

Now you download a file. Your Browser shows a download dialog box with a progress bar to indicate the download progress. You noted that the progress bar is showing 26% for a long while but you have no idea if there is any real data being downloaded, if the network is slow, or if the web site is down. You are about to abort the download by pressing the Cancel button when you noted that the ipTicker icon (in the system tray) is running very quickly.



You observed in the ipTicker Audit Trail screen that there are indeed a lot of rows showing activities for the web site of interest and it keeps recording new rows (indicating that downloading of data is really happening).

The end result : you have the confirmation you need to make the decision – not to cancel the download operation because it (the download) is still active.

Determine if there is any suspicious activity.

Keyboard loggers are spywares – they capture your keystroke and then upload or send your keystrokes back to the hacker. Let's assume for the exercise that there is a keyboard logger logging your activities (especially those logon details when you are logging on your favorite Internet Bank (e.g. ANZ Bank) or to your favorite shopping site (e.g. e-Bay).

In this scenario, you left your PC idle. In theory, everything should be quiet but you noted that the ipTicker icon is running very quickly. On checking the ipTicker Audit Trail screen, you noted that there are some new rows. You observed that the recorded rows are pointing to an unknown European web address and using port 25. This is telling you that some application is sending data to an unknown SMTP server. Using netstat (or a similar tool), you discovered the application that is sending the data is an unknown executable. Upon further investigation, you found that the executable is a keyboard trojan.

In v1.10 and higher, you can take advantage of the alarm capability of ipTicker. Depending on your alarm settings, IpTicker may sound an alarm and flashes in its iconic mode for the above condition.

Quick Start

What do you need to run ipTicker?

At a glance, you need

1. Windows 2000 or Windows XP

How to install ipTicker?

This section describes the manual procedure for installing ipTicker.

ipTicker is packaged in a zip file where

- ipTicker.exe is this executable
- ipCountry.txt is the ipAddress to country database
- ipTicker.pdf is the User Guide (this document)

Prerequisite:

1. Your PC Operating System is Windows 2000 or Windows XP (or higher)
2. You know how to use explorer.exe (basic skills)
3. You know how to use winzip.exe (basic skills)
4. You have ipTicker.zip

Assumption:

- You have chosen to install to c:\Program Files\ipTicker
- ipTicker.zip is saved in c:\temp directory

1. Unzip all files from ipTicker.zip into the ipTicker directory.
 - Start winzip.exe
 - Open c:\temp\ipTicker.zip
 - Enter "c:\Program Files\ipTicker" as the "Extract to" directory
 - Select the "All Files" radio button

- Click the Extract button. You should see all the files unzipped into the specified directory.
2. Run the following command
 - Start Explorer
 - Go to the directory "c:\Program Files\ipTicker"
 - Double click on ipTicker.exe to run
 - You may minimize ipTicker to run in its iconic mode.
 - To activate ipTicker (to restore it to its normal mode), right mouse click on the ipTicker icon in the system tray.

How to uninstall ipTicker?

1. Run the following command
 - Start Explorer
 - Delete the "c:\Program Files\ipTicker" directory

IpTicker Operation

Using IpTicker

The summary screen shows the IP statistics

The Audit Trail screen shows the live activities

Selecting the Alarm tap button will show the active alarms.

The dump screen shows the most recent dump of TPC/UDP data

Alarm: Unsafe port (25) is used

When ipTicker starts, it will automatically listen to all IP activities. If there is an IP event, ipTicker will record the event to the Audit Trail screen. The row will record the following details:-

Column	Explanation
Timestamp	<p>The timestamp of the IP event. It is specified in “yyyyMMddhhmmss” where</p> <ul style="list-style-type: none"> • yyyy is the year • MM is the month • dd is the day • hh is the hour • mm is the minute • ss is the second <p>Next to this value, there is a red or green icon. The purpose of</p>

	the icon is a simple color indicator to show when an event has changed (red color) or nothing has changed (green). To reset the colors, press the Acknowledge button. See section “How to determine if an event has changed”.
Direction	The direction of the IP event. The direction is “In” if it is an incoming IP event The direction is “Out” if it is an outgoing IP event
IP Address	The ip address of the IP event For unregistered version, this will be set to “????.????.????.????” once the number of hosts you are monitoring exceed 25.
Host	The hostname of the ip address (if any). If the hostname is not found, then the value in this column will be blank.
Country	The country of the ip address (if any). If the country is not found, then the value in this column will be blank.
Length	The packet size (in bytes)
Protocol	The IP protocol It could be one of these values:- <ul style="list-style-type: none"> • IP • ICMP • IGMP • GGP • IPV4 • TCP • PUP • UDP • IDP • IPV6 • ROUTING • FRAGMENT • ESP • AH • ICMPV6 • NONE • DSTOPTS • ND • ICLFXBM • RAW

Port	The port number of the IP event (if applicable).
------	--



ipTicker provides two view:- Audit Trail view and Alarm view. Selecting the “Audit Trail” tab button shows the Audit Trail view. This is the default view. Selecting the “Alarm” tab button shows the Alarm view.

The Audit Trail screen shows the latest 100 events. The latest event is always on top.

It will also create a row in the Summary screen. The summary screen shows the IP statistics for this web address, which is grouped by the Direction, IP address and port. If there is already an existing row in the Summary Screen, it will update the “Total” column of the row.

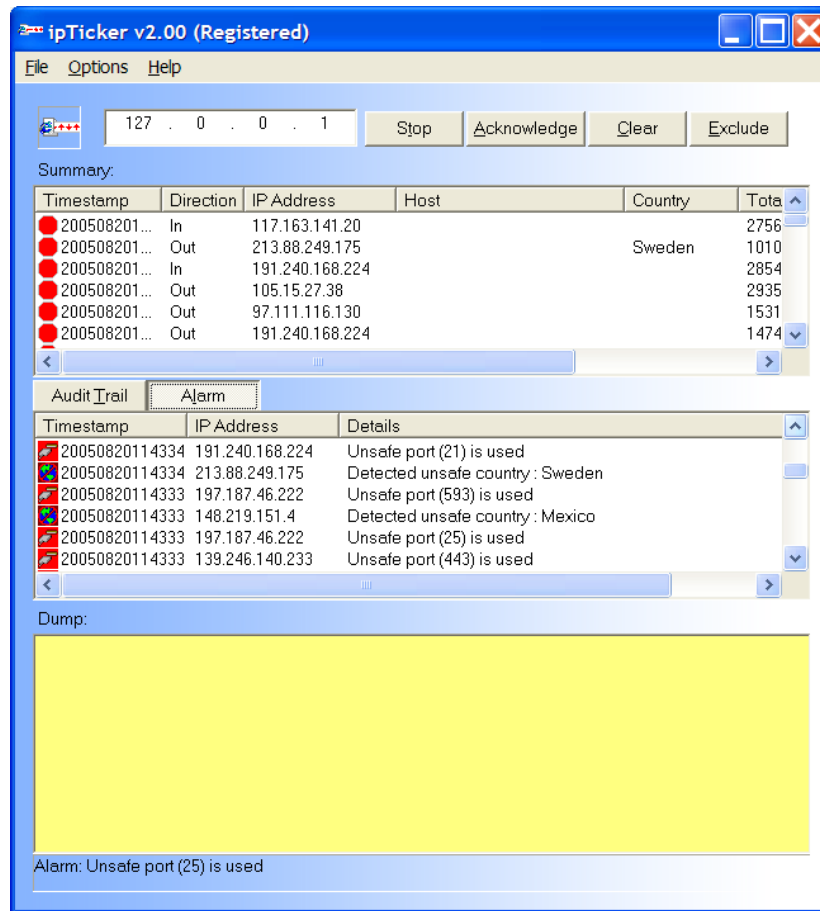
Note 1: For unregistered version, you can only monitor up to 25 hosts. If this number is exceeded, no more rows will be added to the Summary screen.

The details of the Summary row are described below: -





Column	Explanation
(Activity Icon)	 The newest event  The acknowledged (old) event
Timestamp	The latest timestamp of the IP statistics. It is specified in “yyyyMMddhhmmss” where <ul style="list-style-type: none"> • yyyy is the year • MM is the month • dd is the year • hh is the hour • mm is the minute • ss is the second
Direction	The direction of the IP statistics. The direction is “In” if it is an incoming event The direction is “Out” if it is an outgoing event
IP Address	The ip address of the IP statistics. For unregistered version, this will be set to “???.???.???.???” once the number of hosts you are monitoring exceed 25.
Host	The hostname of the ip address (if any). If the hostname is not found, then the value in this column will be blank
Country	The country of the ip address (if any). If the country is not

	found, then the value in this column will be blank.
Total	The accumulated total number of bytes.
Protocol	<p>The IP protocol It could be one of these values:-</p> <ul style="list-style-type: none"> • IP • ICMP • IGMP • GGP • IPV4 • TCP • PUP • UDP • IDP • IPV6 • ROUTING • FRAGMENT • ESP • AH • ICMPV6 • NONE • DSTOPTS • ND • ICLFXBM • RAW
Port	The port number of the IP statistics (if applicable).

The Alarm screen when selected shows the latest 200 alarm events. The alarm view is shown only when the “Alarm” tab button is selected. The latest event is always on top.



If there is an alarm, it will add a row in the alarm view. The details of the Alarm row are described below: -

Column	Explanation
(Icon)	<p>The icon shows the various alarm categories.</p> <p> Unsafe Country Alarm</p> <p> Unsafe Port Alarm</p> <p> Total size Alarm</p> <p> Normal (acknowledged)</p>
Timestamp	<p>The latest timestamp of the IP statistics. It is specified in “yyyyMMddhhmmss” where</p> <ul style="list-style-type: none"> • yyyy is the year • MM is the month • dd is the year • hh is the hour

	<ul style="list-style-type: none">• mm is the minute• ss is the second
IP Address	The ip address of the Alarm event
Details	The alarm message

On the bottom of the screen, there is a Dump screen. The dump screen can record the latest 5000 lines of TCP/UDP data.

To run ipTicker in its iconic mode

When you minimize ipTicker, ipTicker will hide itself to the System Tray. To restore ipTicker, right mouse click on the ipTicker icon in the System Tray.

How to exclude an event

This procedure is to exclude an event AFTER you have decided that an event is benign and you do not wish record the event again.

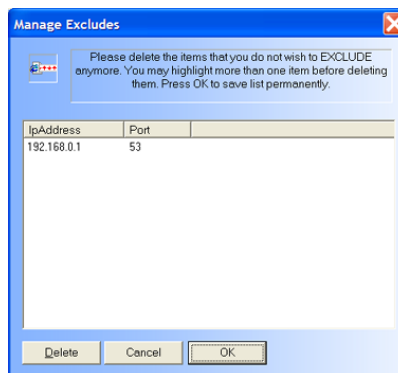
1. In the Summary window, select the event (you may highlight one or more events)
2. Click the **Exclude** button

An excluded IP event is identified by its IP address and its port number. You can exclude up to 2000 events.

How to manage excludes

This procedure is to review or manage excluded events. You can "unexclude" one or more events here.

1. Select the "Options+Manage Excludes" menu item



2. In the "Manage Exclude List" window, select one or more audit trail events
3. Click the **Delete** button
4. Click the **OK** button to save the changes

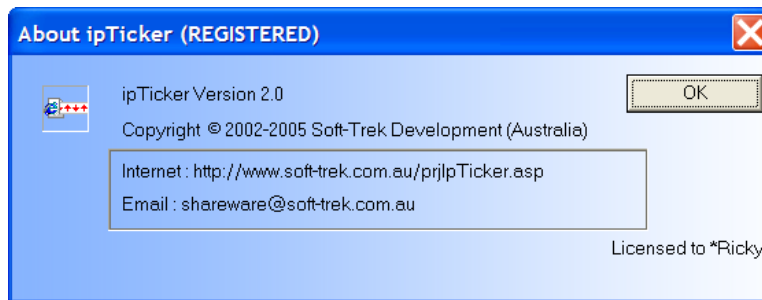
How to determine if an event has changed

In ipTicker, it recorded changed events by the red color indicator on the "Timestamp" column.

1. Press the “Acknowledge” button”
This will reset all the color indicators to “Green”.
2. Wait and let ipTicker detects the changes. New or change events will come in as “red indicators”. If you have a lot of rows, then step 3 may assist you further.
3. Click on the “Timestamp” column.
This should sort on the “Timestamp” column row and display all the “red” color indicators on top.

Checking ipTicker Version

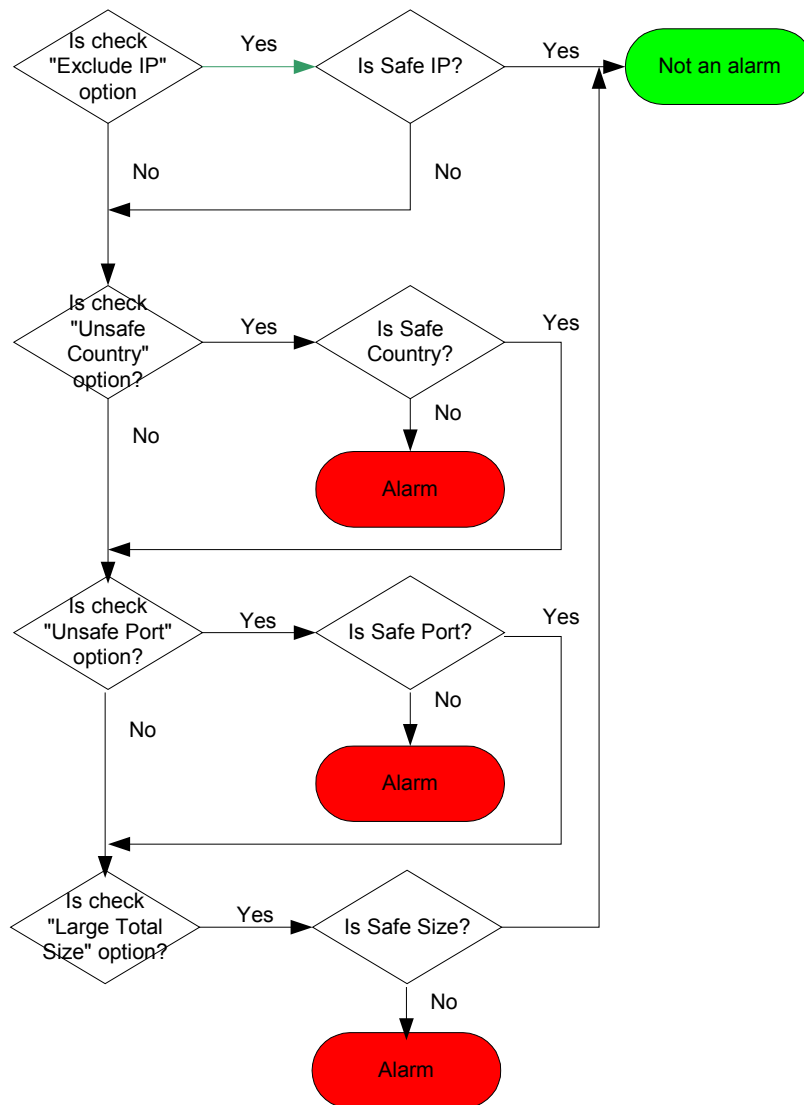
To check the version of ipTicker, select the "About ..." context menu item. An About box will be displayed.



IpTicker Alarms

The Alarm algorithm

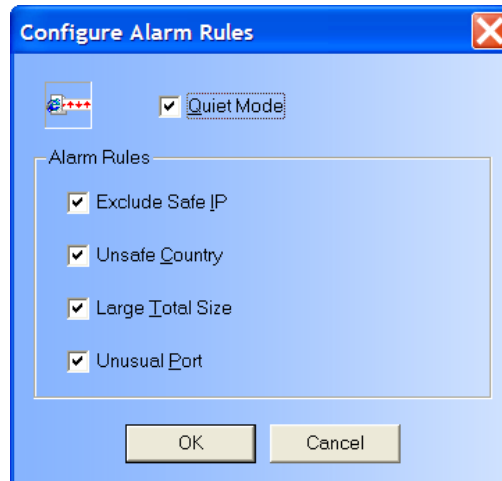
ipTicker implements its alarms by using the algorithm shown below. By understanding how ipTicker works, one can configure the alarm options for one's personalized security needs.



Configuring the Alarm options

This procedure is to configure the ipTicker alarm options. You configure ipTicker's alarm engine by enabling or disabling various alarm rules.

1. Select the "Options+Alarm Options ..." menu item



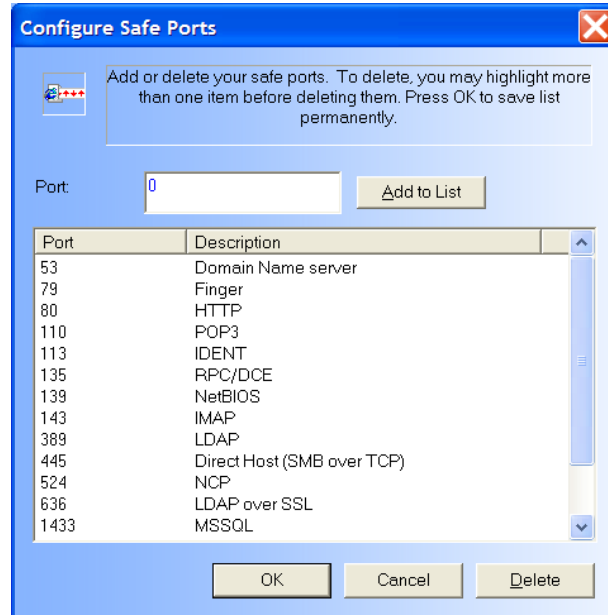
Option	Explanation
Quiet Mode	If enabled, then no alarm will be sounded. By default, this is enabled (i.e. no sound).
Exclude Safe IP	If enabled, then ipTicker will check if there is any safe IP address. By default, this is enabled.
Unsafe Country	If enabled, then ipTicker will check if there is any safe country. By default, this is enabled.
Large Total Size	If enabled, then ipTicker will check if the total size of a row (in the Summary view) exceeds 10Mb. By default, this is enabled.
Unusual Port	If enabled, then ipTicker will check if there is any safe port. By default, this is enabled.

2. Press OK to save your options

Configuring your Safe Ports

This procedure sets those ports that you have determined are safe in your environment. Any ports that do not match your list will be regarded as unsafe ports. An unsafe port will generate an alarm event. You can save up to 100 ports.

1. Select the "Options+Safe Ports ..." menu item



2. Specify a port number in the Port field. Press the “Add to List” button to add to the list.
3. To delete a port from your list, select one or more rows and press the “Delete” button.
4. Press the OK button to commit your changes.

Note: ipTicker pre-configures the following ports for your convenience. Please review these ports to determine its safeness in your environment.

Port	Description
53	Domain Name Server
79	Finger
80	HTTP
110	POP3
113	IDENT
135	RPC/DCE
139	Netbios
143	IMAP
389	LDAP
443	HTTPS
524	NCP
636	LDAP over SSL
1433	MSSQL
3268	AD Global Catalog
3389	Window Terminal Server

5000

Upnp

Configuring your Safe Countries

This procedure sets those countries that you have determined are safe in your environment. Any countries that do not match your list will be regarded as unsafe countries. An unsafe country will generate an alarm event. You can save up to 200 countries.

1. Select the "Options+Safe Countries ..." menu item



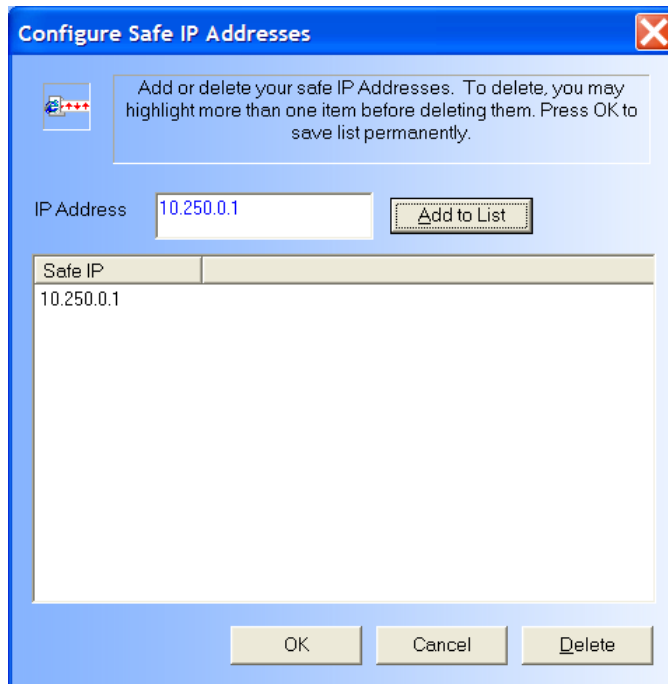
2. Enter a country in the Country field. Press the "Add to List" button to add to the list.
3. To delete a country from your list, select one or more rows and press the "Delete" button.
4. Press the OK button to commit your changes.

Note: ipTicker pre-configures the following countries (Australia, Canada, UK and USA) for your convenience. Please review these countries to determine its safeness in your environment.

Configuring your Safe IP Addresses



This procedure sets those IP addresses that you have determined are safe in your environment. Any IP addresses that do match your list will be regarded as safe. See “The Alarm algorithm” for more details. You can save up to 2000 IP addresses.


1. Select the "Options+Safe IP Addresses..." menu item



2. Enter an IP address in the IP field. Press the “Add to List” button to add to the list.
3. To delete an IP address from your list, select one or more rows and press the “Delete” button.
4. Press the OK button to commit your changes.

Managing Alarms

When an alarm occurs, the system tray icon will flash  and . A new row will be inserted in the alarm view. If the Quiet mode is disabled, ipTicker will beep (up to a maximum of five beeps) to alert you. You can do one of the following actions:-

Press the Acknowledge button	This will clear the alarms. The system tray icon will be reset back to  .
------------------------------	--

Press the Clear button	<p>Only new rows in the Alarm view will trigger an alarm. If a row is already exist, new events of the same alarm will NOT trigger a new alarm. To reset this condition, you must clear the Alarm View.</p> <p>Note: you must be in the Alarm View before you can press the Clear button. Otherwise, pressing the Clear button will only remove entries in the Audit Trail View.</p>
Press the Exclude button	<p>You must be in the Alarm View for this operation.</p> <p>The Exclude button gives you a finer control of your alarms. You may exclude one or more alarm events. This will be saved to an excluded list. Future events that match one of these excluded entries will not generate an alarm.</p>