Rainbow Diamond Limited

Intrusion Detector

User Guide rev.78

http://www.brd.ie/

info@brd.ie

NOTE: The pictures in this manual are optimised for printing, and may not view correctly on-screen.

CONTENTS

Overview 3

Installing Intrusion Detector 4

- How to install 4
- Installing other network programs after Intrusion Detector 4

Licensing 5

- Evaluating without a license 5
- Obtaining Ordering Information 6
- Entering license codes 6

Getting Updates 6

Getting Help 7

- Viewing Online Help 7
- Help on the Web 7
- Before Seeking Assistance 7
- Seeking Assistance 7

The Event List 8

Hiding the Main Window 9

Restoring the Main Window 9

Viewing the Log 9

Clearing the Event List 9

Exiting Intrusion Detector 10

Advanced Options 10

- Adding Ports 10
- Removing Ports 11
- Resetting factory defaults 11

Ignoring local connections 11

Configuring whether or not to play sounds 11

Troubleshooting 12

If other network programs stop working after installation of Intrusion Detector 12

If Intrusion Detector logs a large number of probes from the local machine 12

Chapter

1

Getting Started

Installation, licensing, and support

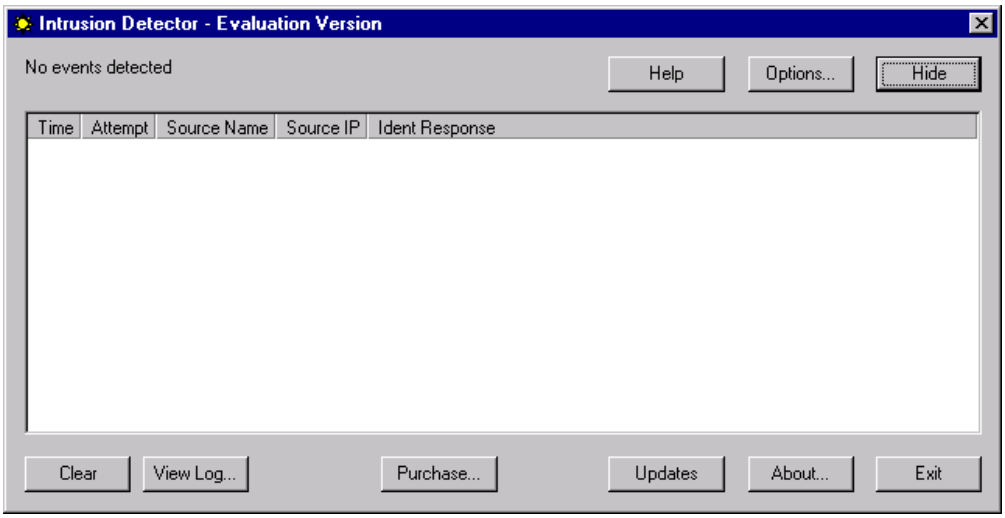
Overview

Intrusion Detector is designed to detect anomalous network connection attempts that may be a prelude to an attempt to break into your computer. If an attacker attempts to connect to your machine, Intrusion Detector will log the connection attempt and try to alert you. It will also attempt to determine the source of the connection attempt.

In most cases, you can simply install Intrusion Detector, and no further configuration will be necessary. Intrusion Detector will launch every time you start your machine, and can be controlled from the tray icon shown below. In the event that a possible intrusion attempt is detected, the tray icon will flash and (if you have a sound card) an alarm will sound. To activate Intrusion Detector, or to change its configuration, click on the tray icon.

• Figure 1: Tray Icon

Clicking on the tray icon will produce Intrusion Detector's main window, shown below. This will also be activated automatically in the event that a possible intrusion is in progress.



• Figure 2: Intrusion Detector Main Window

Note that not all probes correspond to malicious intrusion attempts. In some cases, there may be an innocent explanation for a probe, or probes may be initiated by your local network security team. Therefore, if Intrusion Detector logs a suspicious event, contact your network administrator or your ISP (Internet Service Provider) in the first instance, before accusing someone of trying to break into your computer.

Installing Intrusion Detector

Before installing Intrusion Detector, it is recommended that you:

1) Run any programs you have that use the network (including Frontpage, web servers, etc.), and leave them running until the installation is complete.

2) Have your license information to hand, if you have already purchased a license. (If not, you may evaluate Intrusion Detector free of charge for 21 days.)

How to install

To install the software, run the installation program (IntrusionDetectorV1.exe). Intrusion Detector will install itself and run automatically. After installation, Intrusion Detector will start automatically every time you start your computer (Windows '95 and '98), or every time you log on (Windows NT).

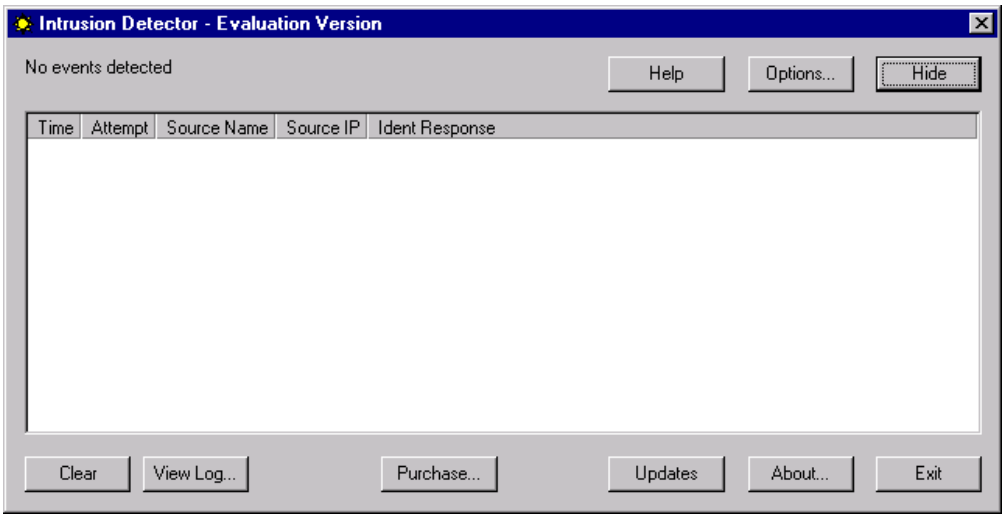
Installing other network programs after Intrusion Detector

While running, Intrusion Detector may interfere with the installation of certain programs that use the network (e.g. Frontpage, web servers, and ftp servers). To successfully install such programs you should:

1) Exit Intrusion Detector.

Do this by clicking on the **tray icon** (see Figure 3 below) to reveal Intrusion Detector's main window (see Figure 4 below). Then click the **Exit** button. Click **OK** to the warning that follows.

• Figure 3: Intrusion Detector Tray Icon



• Figure 4: Intrusion Detector Main Window

2) Install your other software as per the manufacturer's instructions.

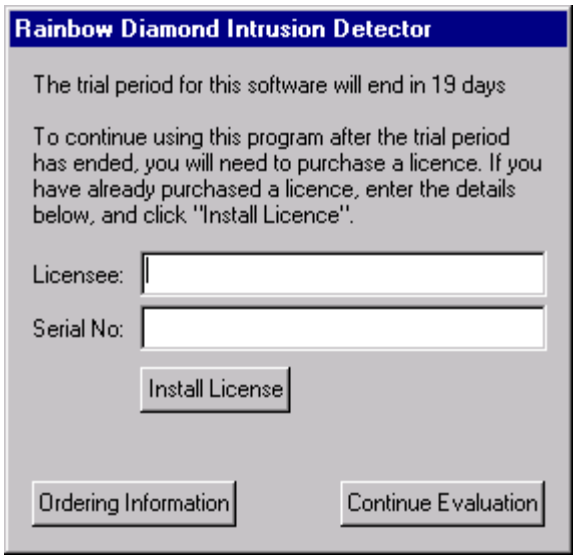
3) Restart Intrusion Detector (Intrusion Detector's icon can be found under *Start/Programs/Rainbow Diamond/Intrusion Detector*).

Licensing

You may evaluate Intrusion Detector free of charge for 21 days. After the evaluation period has ended you must purchase a license and obtain a valid set of license codes.

Evaluating without a license

When running Intrusion Detector without license codes, click **Continue Evaluation** when you see the start-up dialog (Figure 5 below). After the evaluation period has ended, this option will no longer be available, and you must purchase and enter valid license codes to continue using Intrusion Detector. See the next section for license code ordering information.



• Figure 5: Purchase Screen

Obtaining Ordering Information

If you have already purchased license codes, proceed to the next section.

To obtain ordering information for license codes, you will require a web browser such as Internet Explorer or Netscape Navigator, and an active Internet connection. Click **Ordering Information** on the start-up dialog (Figure 5 above). You will then be taken to a web page with further instructions.

If the machine you installed Intrusion Detector on does not have a web browser or an active Internet connection, email sales@brd.ie for license code ordering information.

The purchase dialog is also shown if you press the **Purchase…** button on the main window (Figure 4 above).

Entering license codes

When you have purchased license codes, you may enter them in the startup dialog (Figure 5 above), or alternatively press the **Purchase…** button on the main window (Figure 4 above). Enter both the Licensee Name and the Serial Number exactly as they were given to you when you purchased them, then press **Install License**.

Once you have entered valid license codes, the startup dialog will no longer appear and you may continue using Intrusion Detector beyond the evaluation period. Additionally, the **Purchase…** button will no longer appear on the main window.

Getting Updates

To check the web for updates to your software, click on the **Updates** button on the main window. You will require a web browser such as Internet Explorer or Netscape Navigator, and an active Internet connection.

Getting Help

Viewing Online Help

To view the online help, click the Help button in the main window (Figure 4).

Help on the Web

Intrusion Detector resources can be found on the web at http://www.brd.ie/id/

Before Seeking Assistance

Before seeking assistance from Rainbow Diamond Ltd., please:

1) Refer to the 'troubleshooting' section of this manual.

2) Refer to the README file that came with your software.

3) Check the Intrusion Detector FAQ (Frequently Asked Question) list at http://www.brd.ie/id/faq.html

Seeking Assistance

Users who have purchased a license are entitled to support via email for a period of three months from the purchase date.

To obtain support, email support@brd.ie with your question. Please quote your software's serial number.

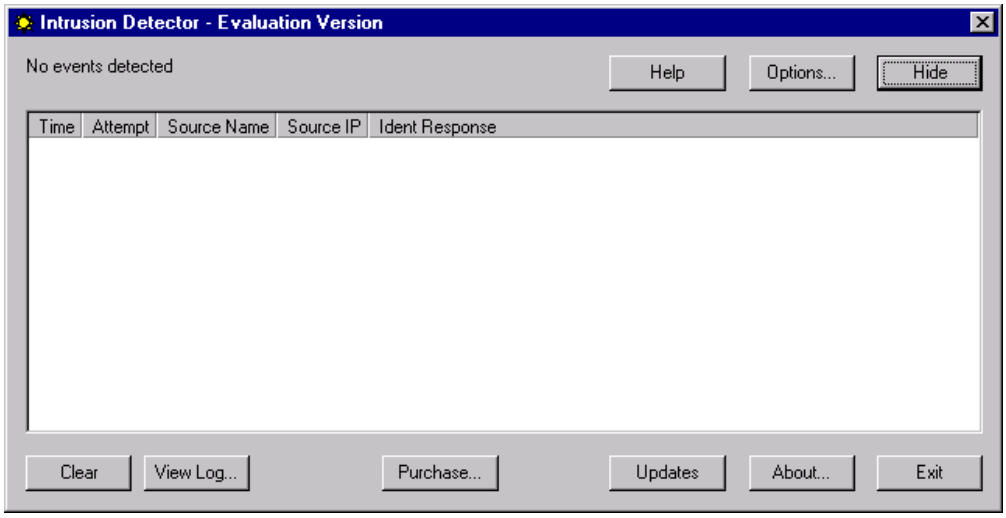
Chapter
2

Using Intrusion Detector

Protecting your computer against intruders

The Event List

Each time you start your computer (Windows '95 and Windows '98) or each time you log on (Windows NT), Intrusion Detector monitors for suspicious network activity ("probes") directed at your computer. Each time a suspicious event is noted, it is logged in the event list (see Figure 6 below).



• Figure 6: Event List

The fields in the event list are as follows:

Field	Description
Time	The time at which the probe attempt occurred
Attempt	The type of probe attempt (the attempted protocol) noted by Intrusion Detector
Source Name	The name of the host which probed your computer
Source IP	The IP address of the host which probed your computer
Ident Response	The identity of the user that initiated the probe, as reported by the host which probed your computer. Note that this field may be untrustworthy, since the source host is typically under the control of the person that probed your computer. In addition, many computers do not report anything when asked for the identity of a user.

Hiding the Main Window

To hide the main window (see Figure 6 above), click the **Hide** button or close the window. Intrusion Detector will continue to monitor for intrusion attempts, but the main window will not be visible.

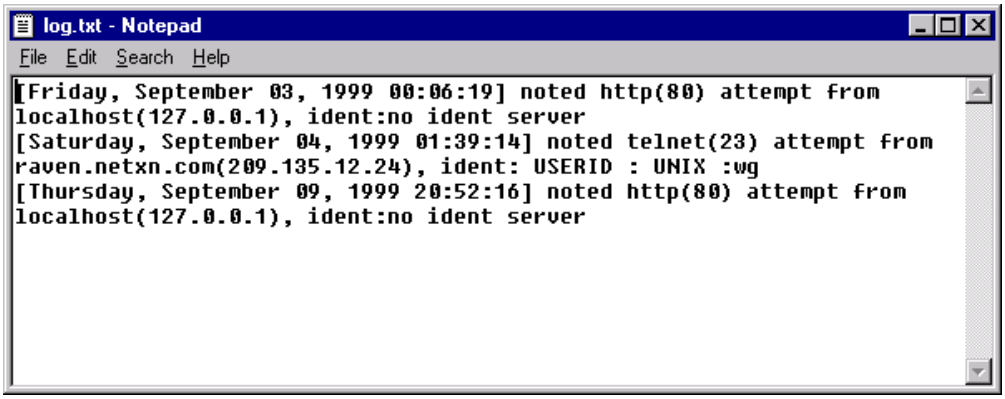
Restoring the Main Window

To restore the main window, click on the tray icon.

• Figure 7: Tray Icon

Viewing the Log

Suspicious events are logged both to the main window's event list (see Figure 6 above), and to a log file on the hard disk. The main window's event list includes only since Intrusion Detector was last started, however the log file contains all events logged since Intrusion Detector was installed. To view the log file, press **View Log…**, and the log file will open in Window's default program for viewing text (.txt) files. Ordinarily, this will be notepad or wordpad (see Figure 8 below).



• Figure 8: Log File

Clearing the Event List

To manually clear the event list, click **Clear**. This will clear the main window's event list, but the events will still remain in the log file.

Exiting Intrusion Detector

To exit Intrusion Detector, click the **Exit** button on the main window. If the main window is not showing, click on the tray icon to activate it.

Note that if Intrusion Detector is exited then it will stop monitoring for intrusion attempts. If you only wish to hide the main window, and still want Intrusion Detector to monitor for intrusion attempts, then click the **Hide** button on the main window, or close the window.

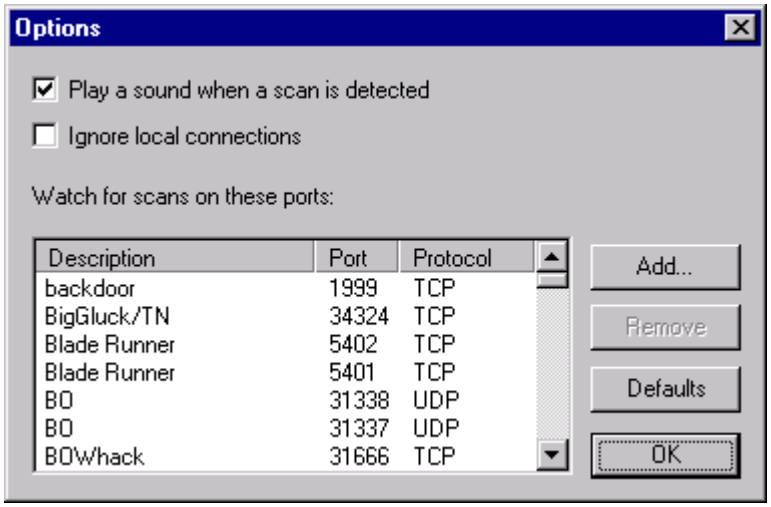
Advanced Options

Intrusion Detector ships preconfigured to monitor a variety of "ports" known to be used by malicious programs. In some cases, advanced users may wish to have Intrusion Detector monitor additional ports, or to remove some ports. **This should only be done by users with an understanding of TCP/IP networking.**

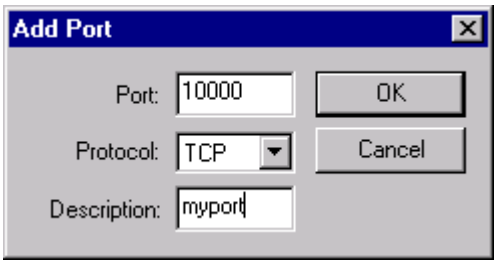
Adding Ports

To add a port, first click on the **Options…** button from the main window. (If the main window is not showing, activate it by clicking on the tray icon.) You will then see the options dialog, which contains a list of the ports monitored by Intrusion Detector (see Figure 9).

When you see the options dialog, click on the **Add…** button. You will then see the Add Port dialog (Figure 10). Enter the port number you wish to monitor, together with a short description of the port, and select whether the port should be monitored for the UDP or TCP protocol, then click **OK**.



• Figure 9: Monitored Ports



• Figure 10: Add Port Dialog

Removing Ports

To remove a port, first click on the **Options…** button from the main window. (If the main window is not showing, activate it by clicking on the tray icon.) You will then see the options dialog, which contains a list of the ports monitored by Intrusion Detector (see Figure 9).

When you see the options dialog, click on the port you wish to remove, then click on the **Remove** button.

NOTE: To avoid disruption to your system, Intrusion Detector will automatically remove ports that it detects are in use by other programs on your computer.

Resetting factory defaults

To have Intrusion Detector monitor the factory-installed ports, first click on the **Options…** button from the main window. (If the main window is not showing, activate it by clicking on the tray icon.) You will then see the options dialog, which contains a list of the ports monitored by Intrusion Detector (see Figure 9).

When you see the options dialog, click on the **Defaults** button.

Ignoring local connections

If probes to some of the ports you wish to monitor may legitimately originate from the local machine, you can select **Ignore local connections** on the options dialog. With this setting, any probes with a source IP address belonging to the local machine will be ignored. (Only enable this setting if absolutely necessary, as otherwise the machine may be vulnerable to probes with spoofed source addresses.)

Configuring whether or not to play sounds

When a suspicious event is logged, Intrusion Detector plays a sound to alert you (if you have a sound card). If you want to disable sounds, first click on the **Options…** button from the main window. (If the main window is not showing, activate it by clicking on the tray icon.) You will then see the options dialog. Disable sounds by clearing the checkbox beside **Play a sound when a scan is detected**.

NOTE: If you want to change the sound that is played, place a WAV file in the Intrusion Detector installation directory, and name it *alarm.wav*.

Troubleshooting

If other network programs stop working after installation of Intrusion Detector

Intrusion Detector should easily coexist with your other network programs, since Intrusion Detector automatically recognises ports that are in use by other programs on your computer, and does not monitor them. However, a conflict may result if:

- You add too many ports (Windows '95 and Windows '98 only). This is a limitation of the networking software supplied with Windows '95 and Windows '98. Try removing some ports.

- You run a network server (e.g. an FTP or web server), and it starts up *after* Intrusion Detector. In this case, Intrusion Detector may monitor the port that your server wishes to use. To fix this, exit Intrusion Detector, and restart your server. Then run Intrusion Detector once more. Intrusion Detector will then detect that the server's port is in use, and will stop monitoring it in future.

If Intrusion Detector logs a large number of probes from the local machine

If this occurs, and you are certain that the logged attempts are legitimate (note that source IP addresses can be spoofed or forged), then select **Ignore local connections** on the Options Dialog.