

Intelligence User Guide

Table Of Contents

Welcome To Intelligence!	1
About Vicomsoft	1
About Intelligence	1
Getting Started	3
System Requirements	3
Installation	4
Uninstall.....	5
Log Generator	7
About Log Generator	7
Intelligence	9
About Intelligence	9
Starting Intelligence	10
Viewing Reports	13
View Statistics	13
Filters	16
Administration Options.....	19
Contacting Vicomsoft	23
Terms Of Use	25

Welcome To Intelligence!

About Vicomsoft

Vicomsoft is a leading provider of software connectivity products for Macintosh and Windows computers.

Our range of products include:

[Internet Connectivity](#)

[FTP](#)

[Terminal Emulation](#)

For further information about the Vicomsoft range, visit our web site at <http://www.vicomsoft.com>

About Intelligence

Intelligence is an optional module of the InterGate suite. Its purpose is to provide a full reporting capability for the usage of InterGate and the Internet by users on the network.

Standard reports include the following:

Internet usage by User, Group and IP address

Internet access by Host, Web page (where applicable), and Category Of Host

Denied access to Internet by User or IP address

Denied access by Host

Internet usage by Protocol

Allowed or Denied Application usage (such as Instant Messaging and Peer to Peer)

Attempted Firewall attacks

DHCP leases and renewals

Remote and local InterGate configuration management events

System errors

These fundamental reports give an overall picture of how InterGate and your Internet connection is being used. However, Intelligence provides the ability to relate one report to another, enabling a high resolution of reporting: For example, report all the web pages that one user has visited during a specific time.

Getting Started

System Requirements

- Any Mac OS X supported PowerMac
- Mac OS X 10.3 or later
- Safari, Firefox or similar Web Browser (Internet Explorer not supported)

In addition to the above requirement, since the database that Intelligence creates from InterGate's log output can be large (depending upon usage), it is recommended that a suitably large hard drive is dedicated to the storage of this information.

Installation

The Intelligence and Log Generator applications are provided on an image file named Vicomsoft Intelligence.dmg.

To install:

- Double click the Vicomsoft Intelligence.dmg file
- From the window which is subsequently displayed:
 - Drag the Intelligence application icon to your Applications folder
 - Drag the Log Generator application icon to your InterGate folder

Uninstall

Since both Intelligence and Log Generator are simply applications, to uninstall them simply drag them from their installed locations to the Trash and then empty the Trash. Note that both applications should be quit before attempting to uninstall them.

Log Generator

About Log Generator

The Log Generator application converts the raw log data files generated by InterGate into compressed, text-formatted files that [Intelligence](#) can process.

Log Generator is launched automatically by InterGate each time log output is generated at the time and day specified in InterGate's Logging preferences. It will also be launched when the Generate Log option is selected from the File menu in the InterGate's Administrator Console application.

The Log Generator application should never be launched manually, although this capability is provided in case of a catastrophic failure where InterGate has not produced a log output file.

Intelligence

About Intelligence

The Intelligence application parses log output files produced by the [Log Generator](#) application and builds a database of the information contained in these files, which can then be queried.

The Intelligence application is not a general purpose reporting tool, which all too often provide generic and often confusing results. On the contrary, Intelligence has been highly optimised and fully pre-configured for use only with the InterGate logging capabilities, to provide the highest level of detail in an easy to understand and easy to use way.

Intelligence uses a web browser based user interface, so your default web browser will be launched whenever the View Statistics or Admin Options are chosen from the Intelligence dialog.

Starting Intelligence

Starting Intelligence For The First Time

Before starting Intelligence for the first time after installation, ensure that there is log output from the [Log Generator](#) application otherwise an error will be displayed that there is no log data.

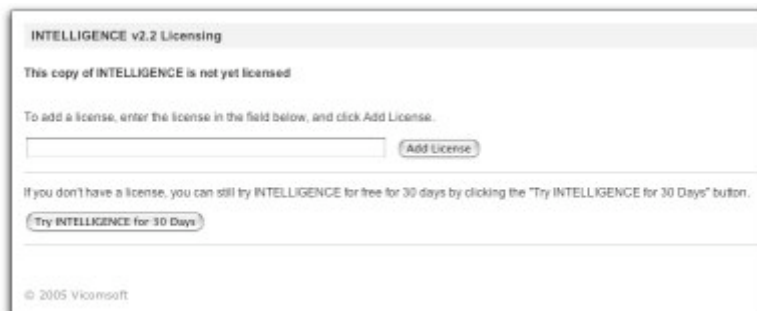
To check if log output is available, see if there are one or more files with the extension "lg.gz" inside the Logs folder, which is located inside the Vicomsoft InterGate folder.

Note that although the Logs folder is the default location for log output, this location can be modified in the Logging tab of the Administrator Console Preferences window.

Starting Intelligence

To start the Intelligence application, double click its icon. Since Intelligence uses a web browser based user interface, your preferred web browser will be launched.

If Intelligence has never been run before, the following screen will be displayed:



Enter your license code as supplied to you by Vicomsoft and press the Add License button. If you do not have a license code, contact Vicomsoft regarding your purchase at sales@vicomsoft.com. If required, you may try Intelligence for 30 days by pressing the Try Intelligence for 30 Days button.

When the following screen is displayed, enter admin as the username and admin as the password. These are the username and password settings for the Intelligence administrator account. These can be changed in the Users section which is described later in the User Guide.

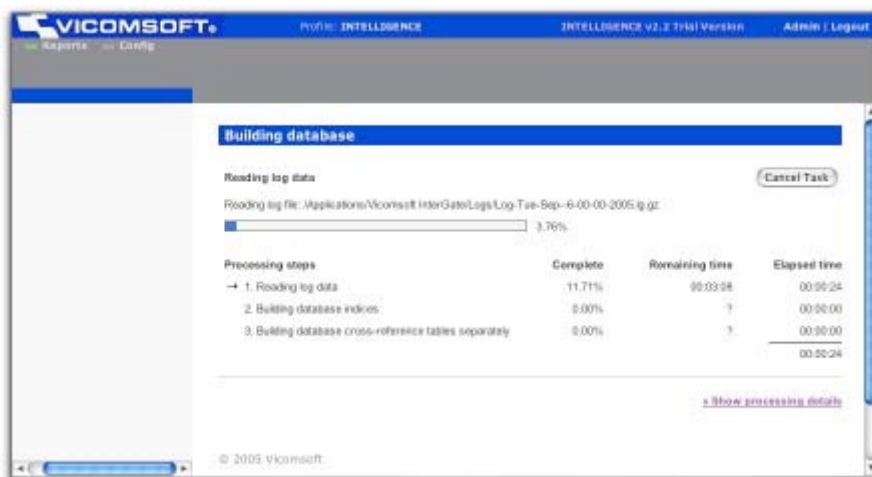


When the username and password have been entered the following screen will be displayed:



Press the Show Reports button.

Since Intelligence has never displayed report data before, the data in the log output file(s) must be parsed in order to display reports and the following screen will appear:



When processing is completed, the [View Statistics](#) screen will be displayed.

Subsequent launches of Intelligence will display the [View Statistics](#) screen immediately. You will not need to enter the administrator username and password each time. This screen is described in the following section.

User / Administrator Mode

When the Intelligence application is double clicked it enters User mode by default. This means that the user cannot make modifications to the Intelligence configuration or the reporting engine. In User mode, reports can be viewed and the database built from InterGate's log output data can be updated with new log output data or completely rebuilt. The User mode is provided for simplicity for non-technical end users and to protect the established configuration.

Administrator mode allows a user who knows the administrator password to make changes to the Intelligence configuration, the reporting engine and the report database structure. The default Administrator username/password is admin/admin

Intelligence User Guide

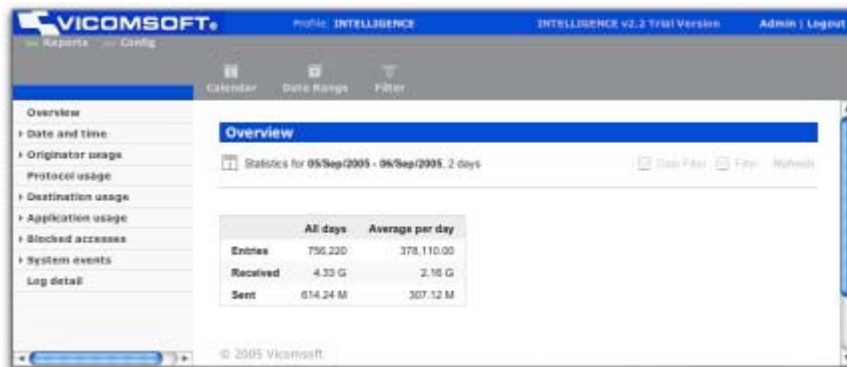
To enter Administrator mode, select Administration Options from the Intelligence dialog.

To enter User mode, select View Statistics from the Intelligence dialog.

Viewing Reports

View Statistics

The View Statistics screen displays the data from the InterGate log output in a report. The first view of the logged data is at the top level - an overview of all the logged data displaying totals and averages for all the logged data.



At the top of the screen are Calendar and Date Range buttons which allow you to choose a particular date or date range to display reports for. Additionally, the Filter button allows you to apply additional user-defined filters which will work in conjunction with the pre-configured report filters on the left of the screen, which are described below.

On the left of the screen are eight buttons which, when selected, filter the view on the logged data to show only certain types of entry, or open up to display additional report options. Each of these filters are described in detail in the [Filters](#) section.

Each time a filter is applied the effect is additional; each selected filter is applied in turn to the logged data before display. In this way, it is possible to drill down from a top-level view of all the logged data, down to a particular parameter in relation to another. For example:-

- Select Destination Usage to show disclose the 3 destination usage reports
- Select All Destination Usage
- Select one accessed host in the displayed report (eg www.vicomsoft.com)
- From the Zoom To Report menu, select All Originator Usage

This combination of filters will show all users on the local network which accessed www.vicomsoft.com

To clear the applied filters and return to the top level, showing all the logged data, select the Overview button.

Also on the screen are several other options which have the following functions:

Date Filter

Clicking on this checkbox will enable/disable date range filtering.

Filter

Clicking on this checkbox will enable/disable user-defined filter

Refresh

Clicking on this button will refresh the displayed report. This is useful after user-defined filters or date range filtering has been applied.

Row Numbers

Clicking on this tab will show Row Number options:

Start Row - Entering a value in here other than 1 (the default) will cause the displayed reports to start at the entered row number.

Number Of Rows - Selecting a value from the popup menu will enable you to choose how many rows of data are shown in the report.

Zoom Options

Clicking on this tab will show a popup menu from which you can choose which report should be shown by default when clicking through the Filters.

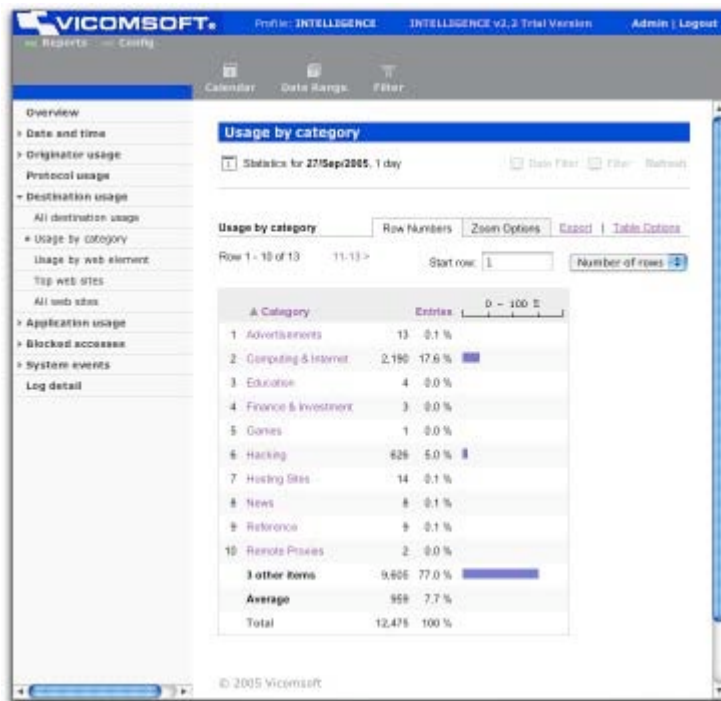
Export

Clicking on this button will output the currently displayed report as a Microsoft Excel CSV file.

Table Options

Clicking on this button will show the options to customize the data which is displayed in the reports.

An example of a filtered report is shown below:



With the exception of the Overview, each report will display a bar graph depicting the report in a graphical form. Entries in the report table displayed in purple-coloured text can be clicked. These also add filters to the current view.

Filters

Filters can be applied to the statistics view to limit the displayed log data to certain parameters, thus enabling a high resolution of reporting.

On the [View Statistics](#) screen are several controls which affect the filters applied to the displayed data:

Overview

Selecting this button will display the Overview screen.

Date And Time

Selecting this button will open to display options to report by hour, day, week, month and year.

Originator Usage

Selecting this button will show options to report the source of traffic in the logged data.

There are three reports:

All Originator Usage:

All originators are shown either by IP address or domain name.

Usage By User:

Where a user has logged into InterGate using Remote Control or the Remote Administrator Console, the user name will be displayed here.

Usage By Group:

Where a user has logged into InterGate using Remote Control or the Remote Administrator Console and the user is a member of a group, the group name will be displayed here.

Protocol Usage

Selecting this button will filter the logged data to report the protocols that were recorded in the logged data, such as FTP or HTTP. Where the protocol is unknown, the port number will be displayed and UDP or TCP depending upon which was used.

Destination Usage

Selecting this button will show options to report the recipient of traffic in the logged data.

There are six reports:

All Destination Usage:

All destinations are shown either by IP address or domain name.

Destination Usage By Category:

This report depends on the optional INSPECT content filtering module for InterGate, where each accessed host is categorized by type (for example, News, Pornography, Shopping). The categories of hosts accessed are reported here.

Destination Usage By Web Element:

Where a web page or image has been accessed, the url (without the host name) is listed here.

Top/All Web Sites:

Web sites accessed in order of amount of transferred data/alphabetically.

Web Category

All accessed web sites listed by INSPECT category.

Application Usage

Selecting this button will filter the logged data to report users who have been using Instant Messaging, Peer to Peer and Voice Over IP applications.

There are three reports:

Allowed / Blocked Reports:

These reports show the applications that were allowed or blocked by the INTERCEPT module as separate reports.

All Application Usage:

This report lists the category of applications that were allowed or blocked by the INTERCEPT module in one report.

Blocked Accesses

Selecting this button will filter the logged data to report users and hosts to which access was denied. Denied access is due to one of the Internet Filters applied, such as Time Control, Protocol Blocks, or more commonly inappropriate content. The latter relies on the optional INTERCEPT content filtering module for InterGate.

There are three reports:

Blocked By User/Site:

This report lists users or sites which were denied access and the reason for the denial. Users will appear as usernames if logged into InterGate using Remote Control or Remote Administrator Console. Otherwise, the DHCP user ID or IP address will be shown.

Blocked Access By Filter:

This report lists the InterGate Filters that were invoked to block accesses.

System Events

Selecting this button will show options to report events relating to InterGate itself.

There are four reports:

Firewall:

This report lists host names or IP addresses from which InterGate received packets of data that were not destined for any recipient on the network connected to InterGate. These may be considered malicious attempts to break through the firewall.

DHCP:

This report lists all DHCP events in InterGate - requests, renewals and releases of DHCP assigned IP addresses. The DHCP ID or IP address of each event is shown along with the MAC address of the machine making the transaction.

Management:

This report shows all Remote Management events in InterGate, tracking user logins and logouts (with Remote Control, for example), modifications to the InterGate configuration and other status reports.

Errors:

This report lists critical errors that InterGate encountered during execution, for example, malformed received packets, internal execution errors and other exception states.

Log Detail

This option is not a report as such. It displays the raw data from the log output file as produced by InterGate and LogGenerator.

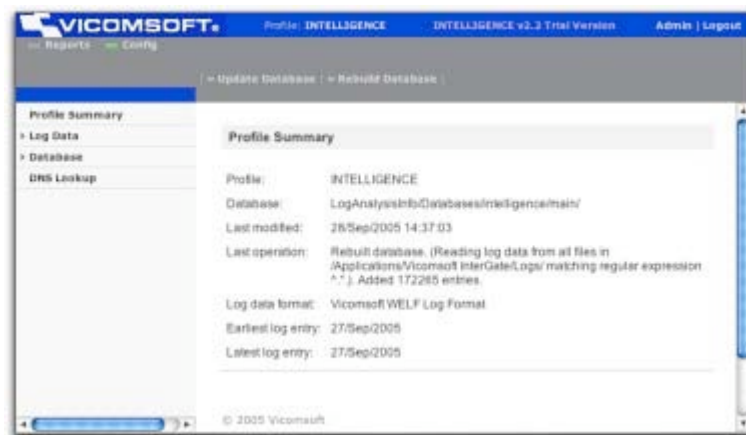
Administration Options

The Administrative screen, as shown below, is the first screen which is shown after the Administration Options button is chosen from the Intelligence dialog and a valid Administrator password has been entered.



Profiles

The Show Config option in the Profiles screen allows modification of the Intelligence configuration.



There are also buttons at the top of the screen which allow the database to be updated (Update Database), rebuilt (Rebuild Database), or viewed (Reports).

Profile Summary

The default screen shows the Profile Summary, which describes where the database is located, it's last modified date, the last operation that was made and the date range covered by the data.

Log Data

This screen contains data about the source of the logging data - the log files produced by InterGate and Log Generator.

Log Source

Clicking on this option allows you to change where Intelligence will look for log files to process. By default this location is the Logs folder inside the InterGate folder.

Log Filters

This option is pre-configured for Intelligence and should not be changed unless you have advanced knowledge of the reporting engine.

Database

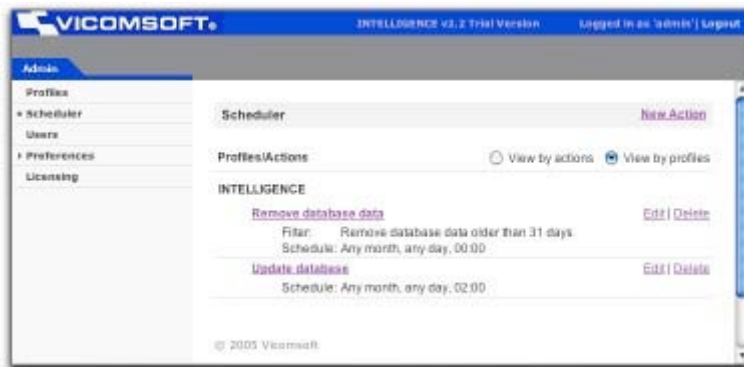
This option allows modification of the internal workings of the Intelligence reporting engine. The settings should be left untouched unless you have advanced knowledge of Intelligence.

DNS Lookup

This option allows modification of the internal workings of the Intelligence reporting engine. The settings should be left untouched unless you have advanced knowledge of Intelligence.

Scheduler

The scheduler allows Intelligence to perform specific, unattended actions at pre-determined times. By default, it is set to expire database entries older than 31 days at 12:00 am and then update the database at 2:00 am.



The most probable use of this feature, other than the defaults, is to send email reports to any number of recipients. This can be done by clicking the New Action button and following the on-screen prompts.

New Action

Clicking this option will add a new scheduled item. A window will appear into which you can configure the action to be taken and when.

Edit/Delete

Clicking this option will edit or delete the action next to it in the list of actions shown. If the edit option is chosen, a window will be displayed with the current settings which can then be modified.

Users

This option allows logins to be created for additional users. By default, there are two users: admin and stats which should not be deleted - Intelligence relies on these two users being present. The username and password can be changed for the admin user, if required. The default setting for the admin user is username:admin and a password: admin



New User

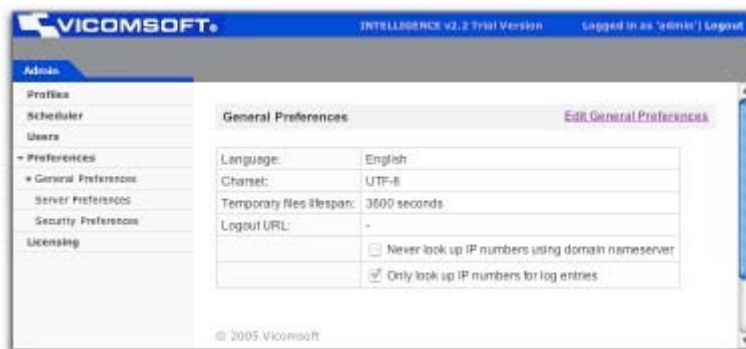
Additional users can be created by pressing the New User button.

Edit/Delete

Existing users can be modified or deleted by pressing the appropriate button next to the user entry in the displayed list.

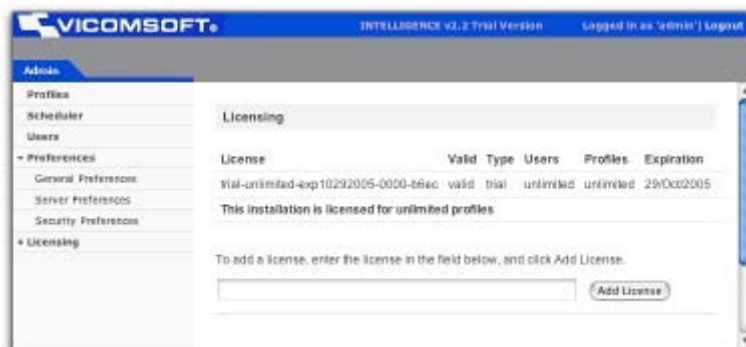
Preferences

This option allows modification of the internal workings of the Intelligence reporting engine. The settings should be left untouched unless you have advance knowledge of Intelligence.



Licensing

This option displays your license information, if any. A purchased license can be added by selecting this option.



Contacting Vicomsoft

Service Contact

In the event of a service or support query, please use the addresses that follow:

World Wide Web: <http://www.vicomsoft.com/>

Email - Information: info@vicomsoft.com

USA & Canada

Email - Sales: sales@vicomsoft.com

Address: 265 E Merrick Road Suite 209, Valley Stream, NY 11580

Sales: (888) 8422608

Fax: (530) 6858896

UK & International

Email - Sales: sales@vicomsoft.com

Address: 70 Norwich Avenue, Bournemouth, BH2 6AW, England

Telephone: +44 (0) 1202 294791

Fax: +44 (0) 1202 310 241

Email Support

Email - Support: support@vicomsoft.com

Terms Of Use

License

The purchase price of the software includes a personal non-exclusive license for the person/company purchasing the license to use or install the program and associated files for their own purposes, on ONE computer at one time.

The license does NOT include the right to make any copies of the program and files for any purpose other than backup or to have the program installed on more than one computer at one time. No copies of all or portions of manuals are to be made. Any copies of software or installation on more than one hard disk or copies of manuals (or portions thereof) shall constitute a breach of copyright and shall be dealt with to the fullest extent of the applicable law.

The word “backup” means a copy for the licensee's own personal security in the event of failure of the disks provided by Vicomsoft Limited. The licensee undertakes not to transmit any copy of his backup to any third party, whether for sale or otherwise. Any such unauthorized transfer shall constitute a breach of license and copyright.

Should the licensee desire to transfer his license to use the software to a third party, he shall firstly obtain the consent in writing of Vicomsoft Limited which consent shall not be unreasonably withheld. Licensees requiring copies of Vicomsoft software to run on multiple CPUs should contact Vicomsoft to obtain details of quantity discounts and site licenses.

Warranty

Should the supplied disks fail, for reasons of defect in material within 12 months of purchase and registration, Vicomsoft will replace such failed disk for the Registered Owner free of charge.

Notwithstanding the above, Vicomsoft shall not replace or be obliged to replace any disk if it has failed as a result of misuse.

Disclaimer Fitness For Particular Purpose

Vicomsoft makes no representations or warranties of any kind whatsoever with respect to the software or the contents thereof, other than that herein set out and specifically disclaims warranty for fitness for any particular purpose. Vicomsoft shall not be liable for errors contained in the software or herein or for incidental or consequential damages in connection with the furnishing, performance or use of the software or the manuals.

Changes to Software or Documentation

Vicomsoft reserves the right to revise the software and/or the User Guide and to make changes in the content thereof, without the obligation to notify any person of such changes.

Trademarks Acknowledged

Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Apple, the Apple logo, Mac, Mac logo, Macintosh, Power Macintosh and Quick Time are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

All trademarks, Service Marks and the like owned or used by third parties and mentioned in this guide are hereby acknowledged.

Technical Support

Vicomsoft shall provide technical support via Email or by telephone, only to bona fide licensees of Vicomsoft software who have completed, signed and returned their Warranty Registration forms.

Upgrades

From time to time Vicomsoft issues upgrades to the Vicomsoft software. These upgrades shall only be available at special discount prices to bona fide licensees of Vicomsoft who have completed, signed and returned their Warranty Registration forms.

Feedback

Vicomsoft have been creating communications products since 1985. Many people have provided input which has contributed to the many improvements and enhancements.

Input from users, corporate support departments, VAR's and dealers regarding future improvements and enhancements, is actively encouraged and gratefully accepted.