Project SysTraq

System Tracking
For
Windows Based PC

Version: 2.0a

Table Of Contents

Concept

In most organizations, there is a need to accurately track installed hardware and software of installed PC and laptops. This software suite is designed to automate this task and to allow reporting of the installed base at either department, regional or central basis.

The design of the system reports all requested tracking on a daily basis. This allows the servers to determine and log any changes. It also allows the servers to alarm if any of the configured terminals do not respond. This allows faster detection of missing units, their last known configuration, and the last known software installed or company files.

The antitheft unit may also be activated, to allow reporting via the Internet, giving the URL address of the ISP being used, along with other critical information. This allows the parties responsible to be tracked.

Overview

The full system consists of three components. The first two are a Server holding a database of all related PC being tracked, and a client on each of the units reporting back to a nominated in-house server via an Intranet or Internet. The third component is an external WEB based server for the client to notify whenever it is unable to reach its nominated server after a pre defined number of days, and it has detected that it has an open Internet connection.

The server, on a daily basis, requests the file date and size along with any version properties held within executables or files. It is able to also track system settings such as memory installed, video cards, network cards, BIOS versions, Processor serial numbers, RAS Settings, Installed software and many other system related information. INI files and registry settings can also be tracked.

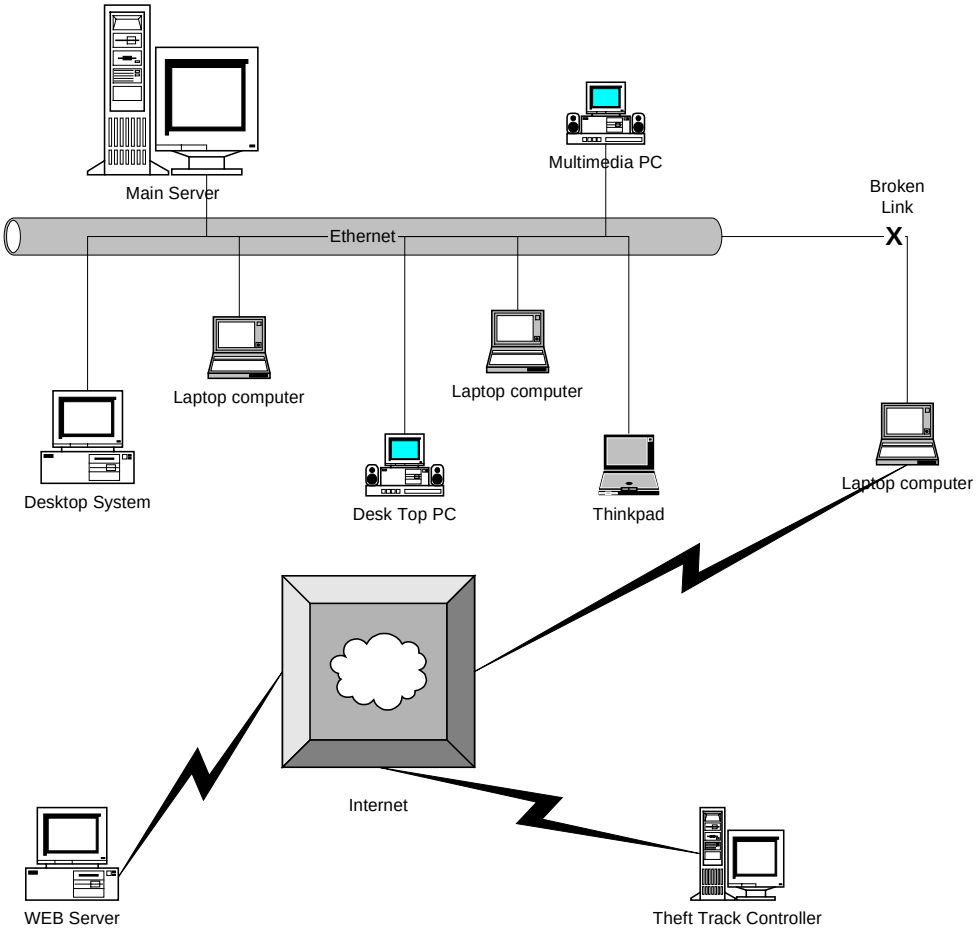
The system is self maintaining, allowing recording of up to the last 99 versions of any specified file, Ini file, registry or system setting along with the date of change.

Tracking options are soft, and controlled by the system administrator. The client is requested by its server to report on specified files and or system information. This reporting can be on a daily basis via internal automatics, or on an add-hoc basis at the request of the administrator.

The system is capable of being configured to allow regional servers, controlling an office or group of offices, along with major regional servers and a central server.

The WEB based server for tracking stolen or missing units is maintained and serviced by an external organization. The same facility is available in-house as well as using a company based WEB server.

Network Architecture



Client Software

The client consists of a single executable. It runs in a mode hidden from the PC or laptop user, and is started each time the user logs on to their system.

The client is normally dormant until a request is received from its server. This request is logged to allow the client to track the last time it was polled by its server. It tracks both manual and automatic requests, and treats both as being polled by its server.

The client is also able to detect access to the Internet via a dial up link. If enabled, and having not been polled for a specified number of days, as soon as this dial up connection is detected it will send a small message to a WEB server giving the serial number of the client, its current ISP connection IP address, its network cards IP address with MAC address and its processor serial number, if its available, and the

RAS dialup parameters used. The anti theft component is optional, and only able to be enabled via the server.

The client software does not use databases or ini files. Its serial number is determined first time it is run. It is able to be installed by download from the WEB, download from the Server, email or diskette.

Functions supported by Client

The server is able to request:

- **File Information**
  - File date
  - File size
  - File version properties
  - Inclusive of any sub directories, if required

- **INI File Information**
  - Complete INI file

- **Registry Information**
  - Full Sections
  - Based on the five major registry keys

- **System information**
  - Processor information
  - Memory
  - Network settings and information
  - Installed software
  - BIOS information
  - Operating system information
  - Disk system information for all configured disks
  - APM system settings and information
  - Common start-up
  - User start-up
  - Display information including Video card
  - Environment information
  - HKCU run information
  - HKLM run information
  - Windows NT extra information (for NT clients)
  - Printers
  - Run Once Information
  - Sound settings
  - Time Zone settings
  - Winsock information
- **Running Processes Information**
  - Name

    - Memory Usage
- Copy Files
- Delete files
- Rename files
- Change clients configuration settings
- Uninstall client
- Log processes used by the user along with the time duration and maximum memory usage (special client unit)
- Change system date and Time

All processing of server requests are done in background, without the user of the system being aware.

Client requirements

Operation systems

- Windows 98 / 95 or
- Windows NT or
- Windows 2000 or
- Windows Me

Hardware

- Intel based system
- Network card
- Serial port (if anti theft enabled)

Database

- None

System Software

- RAS (if anti theft enabled)

Server Software

The server software is able to run both as controller and to act as a client for a server somewhere else in the network.

In client mode, it will do the same functions as a client reporting back to its own server on demand.

Normally the server component runs in background, however it may be made visible by the administrator to allow configuration changes or ad-hoc request. The server normally polls each configured client at least once a day. The start time for the polling is usually after normal business hours have started. The administrator is able to define a block of time where the server will not poll its clients.

The configuration allows for clients to be added / deleted from polling, what information is polled and other base settings. The information consists of three main sections, files, system information and processes run, and theft tracking.

Under files, the administrator defines which files or directories are to be scanned, and the type of file. Types can be normal files, ini files or any of the 5 registry keys. The configuration allows ‘wild cards’ and optional inclusive directory scans for standard file tracking. While it may not be advisable or necessary, this allows for a simple command c:*.* with subdirectories to return all files on Drive C.

The second section is system information. This is expected to remain fairly static. The administrator may reduce what system information is stored.

The final section is theft tracking. This section is only activated when the server has not polled the client for the pre-determined time. The client first polls the server to validate that it is still part of the tracking system, then if not found, will wait for an Internet connection to be made by the user. Once the connection is found, it will then attempt to communicate with a WEB server in background mode leaving details on the WEB server to allow tracking of where the unit is, and who has it.

It the client finds its server during this process, it will either reset its timers or de-configure itself depending on the response received by its server.

Server Utilities

The server is able to track up to 99 changes of the information being tracked. This is configurable by the administrator from 1 to 99. The date of each change is also held. The administrator is able to have a record of changes of any files or system information tracked.

The server is also able to report on clients that have missed being polled.

Using file information tracking, the administrator is able to detect clients whose software is not at the same release as the rest of the network, using criteria such as version information, file date, or file size, or is able to detect when users have files on their system that are restricted.

Server Configuration Information

Each client has an entry defined by the machine name of the client machine. The entry is also assigned an IP Address to allow the server to connect with the client. If this relationship changes between machine name and IP address, then the server can alarm via email if required. The database also allows for the department the unit belongs to, its asset register tag, and the person the unit is assigned to. Cost of unit, date of purchase, date of end of service and client enabled are also within this record.

Both the machine name and IP address are used in all databases, allowing reports to be via machine name, IP address or MAC address (obtained from the client during communication). As the MAC address is unique and locked to a network card, it can be used to track stolen units if the anti theft option is enabled.

The anti theft option relies on both the MAC address of the network card and its processor serial number (if present) to identify a unit. Either of these numbers may be used to reference back to the configuration entry. It also sends other information valuable in locating the stolen unit.

Configuration Information Held per Client Unit

- Machine Name
- IP Address
- MAC Address (after first communication session)
- Processor serial number (after first communication session and if present)
- Enabled
- Company (to allow multiple companies within one database)
- Business Unit
- Department or section
- Region
- Name of User
- Asset Register Tag
- Cost of unit
- Upgrade Costs
- Anti Theft enabled
- Days to wait before reporting theft (if anti theft enabled)
- Site number (if within POS system)
- Location number (if within POS system)
- Terminal number (if within POS system)
- Serial number (after first communication session)

Functions by Server on Client

The functions the server is able to request of each Client:

- **File Information**
  - File date
  - File size
  - File version properties
  - Inclusive of any sub directories, if required

- **INI File Information**
  - Complete INI file

- **Registry Information**
  - Full Sections
  - Based on the five major registry keys

- **System information**
  - Processor information
  - Memory
  - Network settings and information
  - Installed software
  - BIOS information
  - Operating system information
  - Disk system information for all configured disks
  - APM system settings and information
  - Common start-up
  - User start-up
  - Display information including Video card
  - Environment information
  - HKCU run information
  - HKLM run information
  - Windows NT extra information (for NT clients)
  - Printers
  - Run Once Information
  - Sound settings
  - Time Zone settings
  - Winsock information
- **Processes Running**
  - Name
  - Memory Usage
- Copy Files (Ad-Hoc only, by the administrator)
- Delete files (Ad-Hoc only, by the administrator)
- Rename files (Ad-Hoc only, by the administrator)

- Change clients configuration settings (Ad-Hoc only, by the administrator)
- Uninstall client (Ad-Hoc only, by the administrator)
- Log processes used by the user along with the time duration and maximum memory usage (Special Client unit required)
- Change system Date time (Ad-Hoc only, by the administrator)

Server requirements

Operation systems

- Windows NT or
- Windows 2000

Hardware

- Intel based system
- Network card
- Serial port (if anti theft enabled)

Database

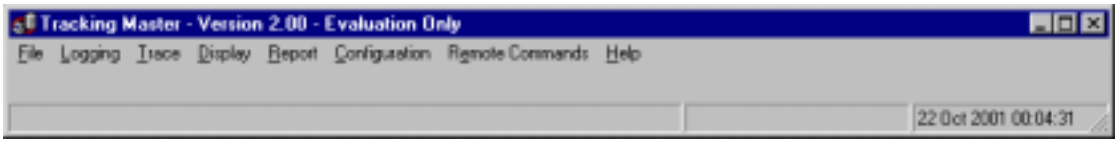
- Paradox or
- Inter Base or
- Oracle

System Software

- RAS (if anti theft enabled)

Server Configuration

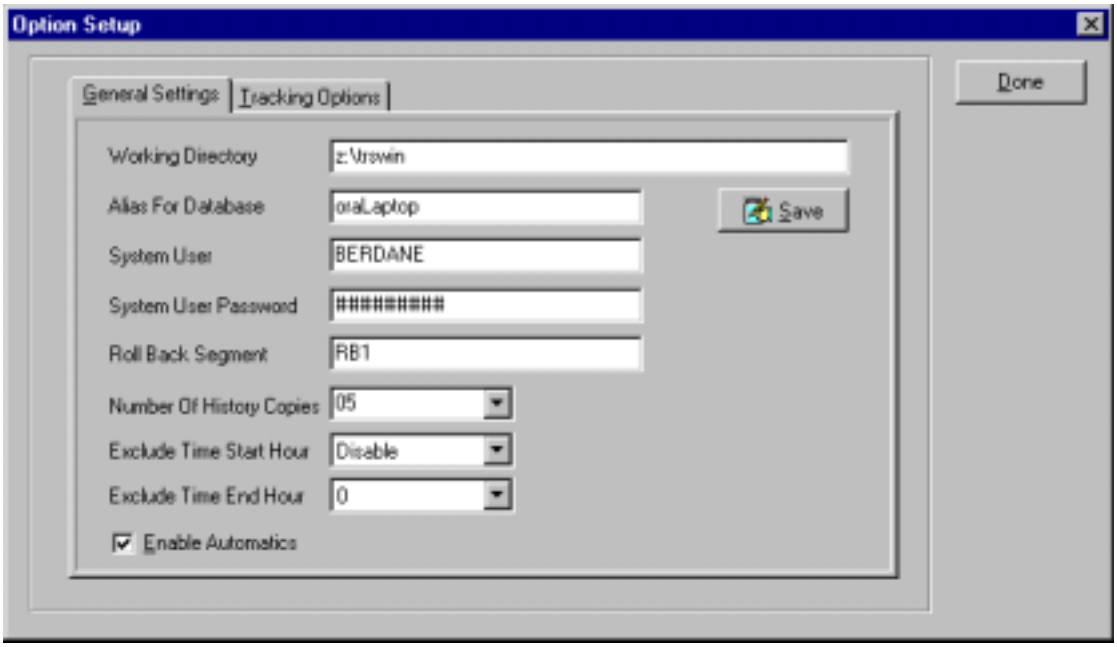
The server normally runs in minimised mode. If the user activates the manual functions, it disables the automatics during the manual session.



On first installation, the administrator is required to first setup the server, then register the server using a key provided. This key will provide the base configuration options allowed and the maximum number of clients allowed. The evaluation period starts from the first run of the server and will expire in 30 days unless a key is used to activate the system.

In evaluation mode, the automatics are disabled along with the ability to store data collected manually to a database. The information from the client is however available for viewing.

Using a mouse, or keyboard navigation, the administrator enters the key via the ‘Configuration’ option followed by ‘Options’



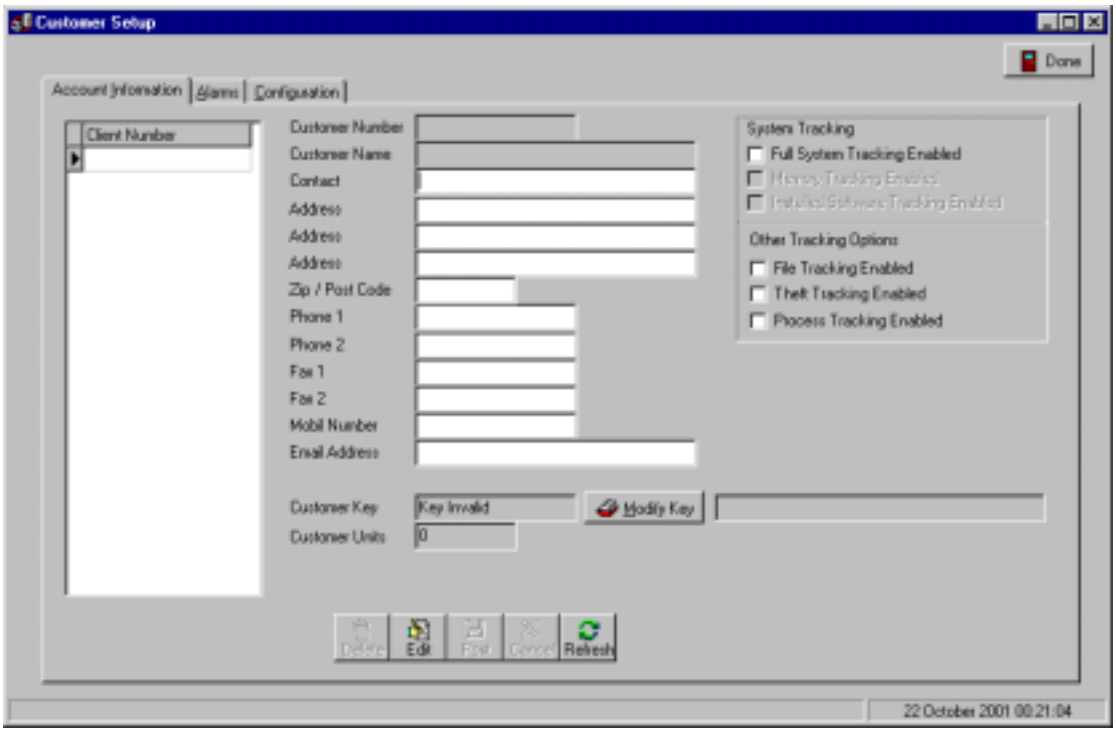
Critical information that must be supplied is the Alias of the database. This defaults to ‘TRACKING’ but may be changed to any valid or new Alias. The system will allocate a paradox connection and create the database if the operating system is not aware of the Alias.

If SQL databases are used, the System User and Password must be entered that will allow the server to access the database. The default Rollback segment of RB1 is the Oracle default. Change this to match the SQL database in use.

Once the Alias, User and Password have been set, the server needs to restart to connect to the new Alias.

The system is now ready for the next phase of configuration, using the databases defined in the previous steps.

Using a mouse, or keyboard navigation, the administrator enters the key via the 'Configuration' option followed by 'Customer setup'

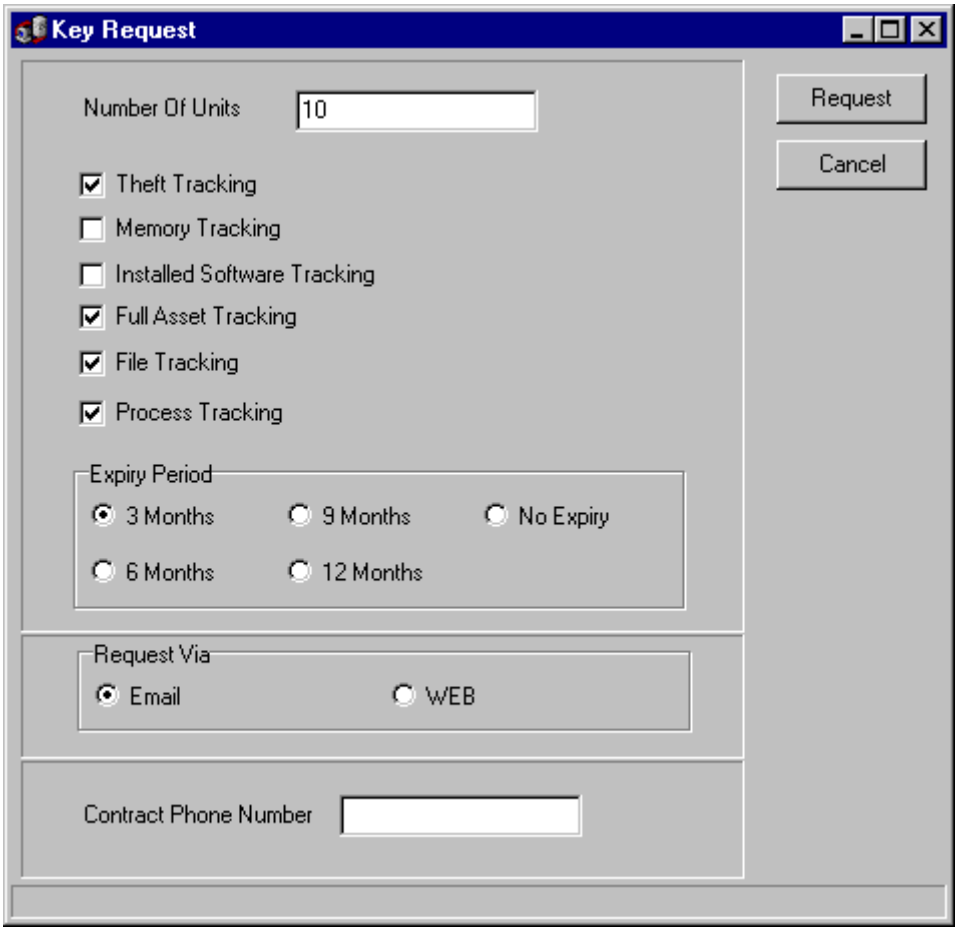


The administrator then adds the base record to the system using the 'Modify Key' button

The Client number is an open field and is usually supplied along with the key. This number becomes important only for theft tracking and support calls.

The registered name must be entered and must match the registered name given with the key request.

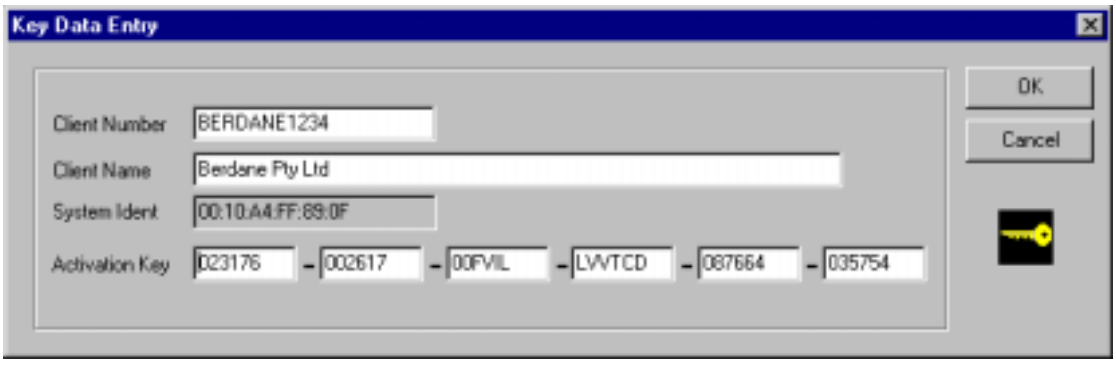
To simplify request of the key, the administrator may click on the 'Key Icon'. This will allow the system to send an Email (see Email Setup) or a request via the WEB direct to a receiving WEB server.



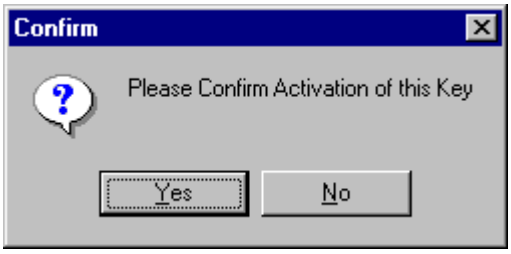
The System ID is a unique number supplied by the system. This number must also have been part of the Key request.

Note, both the key and the registered name are not case sensitive. The key takes the form of 023176-002617-00FVIL-LVVTCD-087664-035754

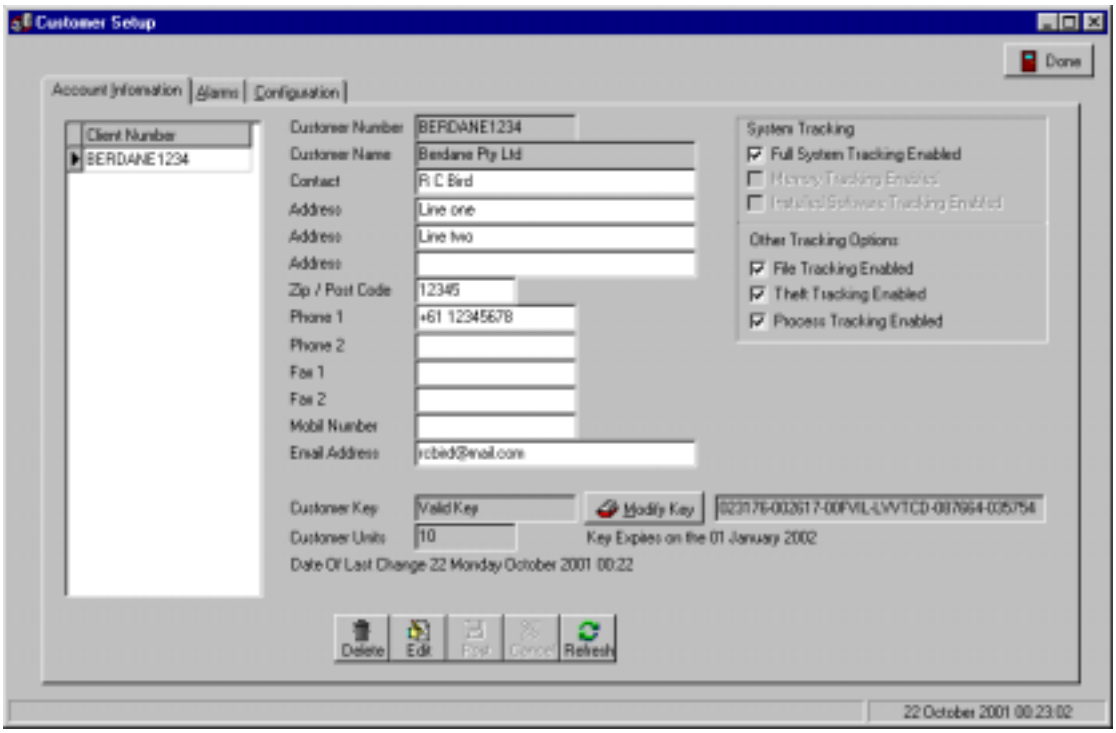
This can be split into its six separate sections, or entered as a complete key into the first edit box.



On clicking the 'OK' button, the system will validate the key and prompt the user to continue.



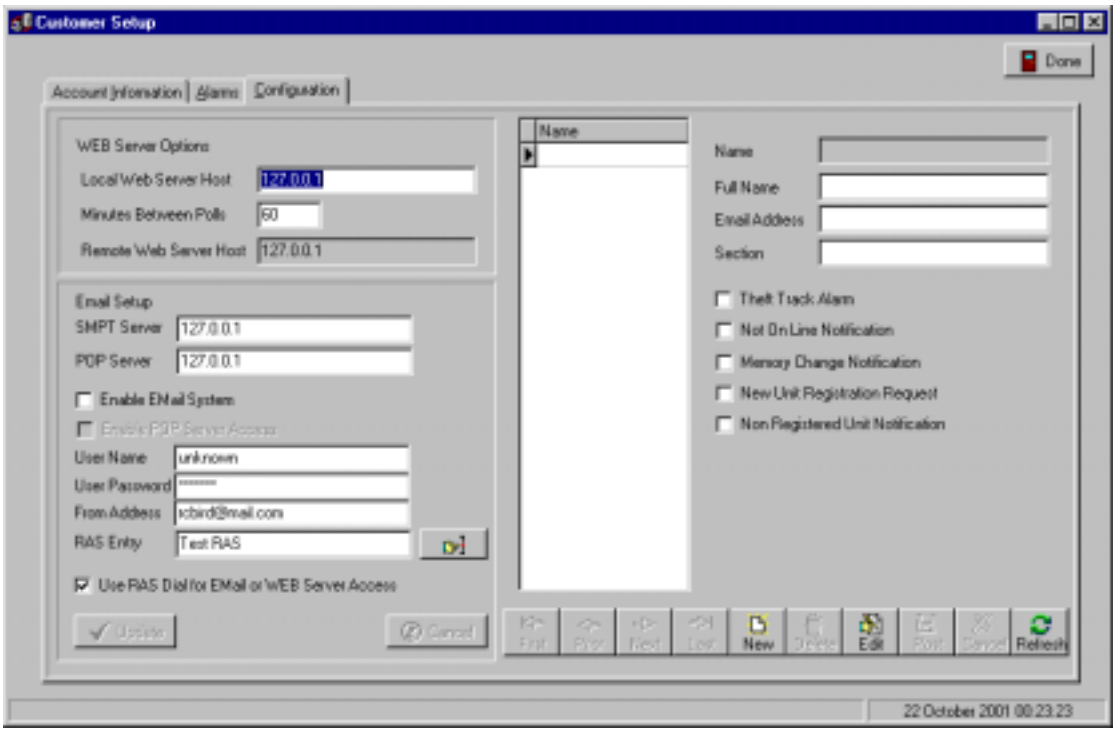
If accepted the system will return the information back to the main edit screen ready to complete the rest of the details.

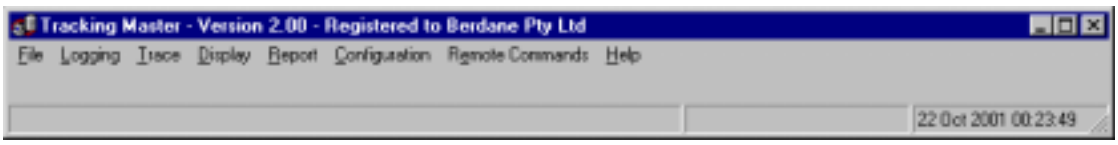


Restarting the system then enables functions as specified by the key; however, other configuration options may be completed before the restart.

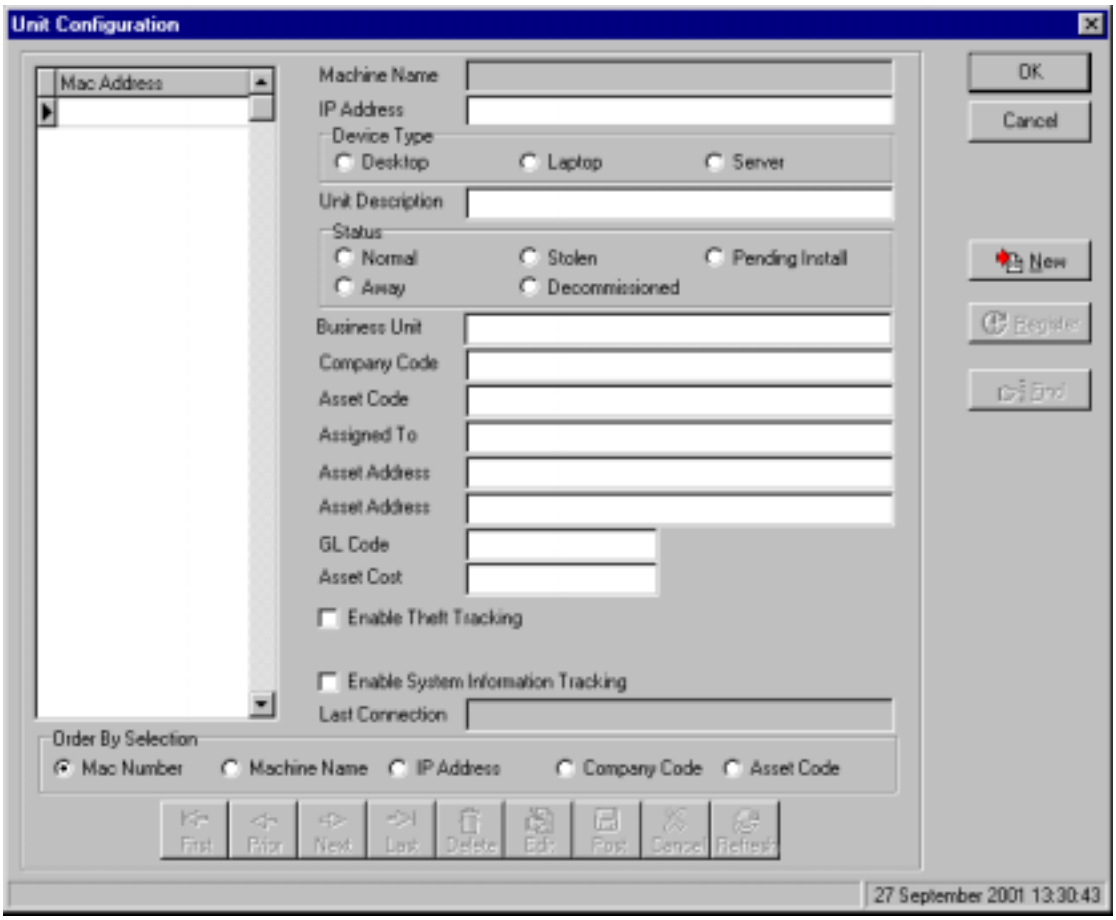
Users that use the Theft tracking will normally be in the ‘pay as you go’ mode and have a renewal key every three months. Others will usually have a non-expiring key.

Within the same section, the email and alarm parameters may be changed to match the customer’s needs.

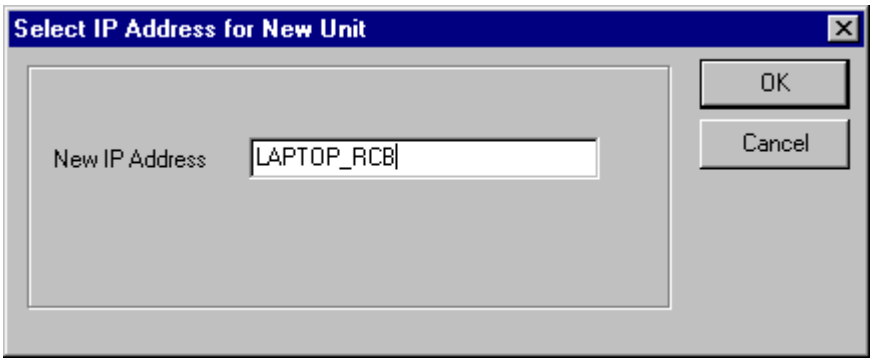




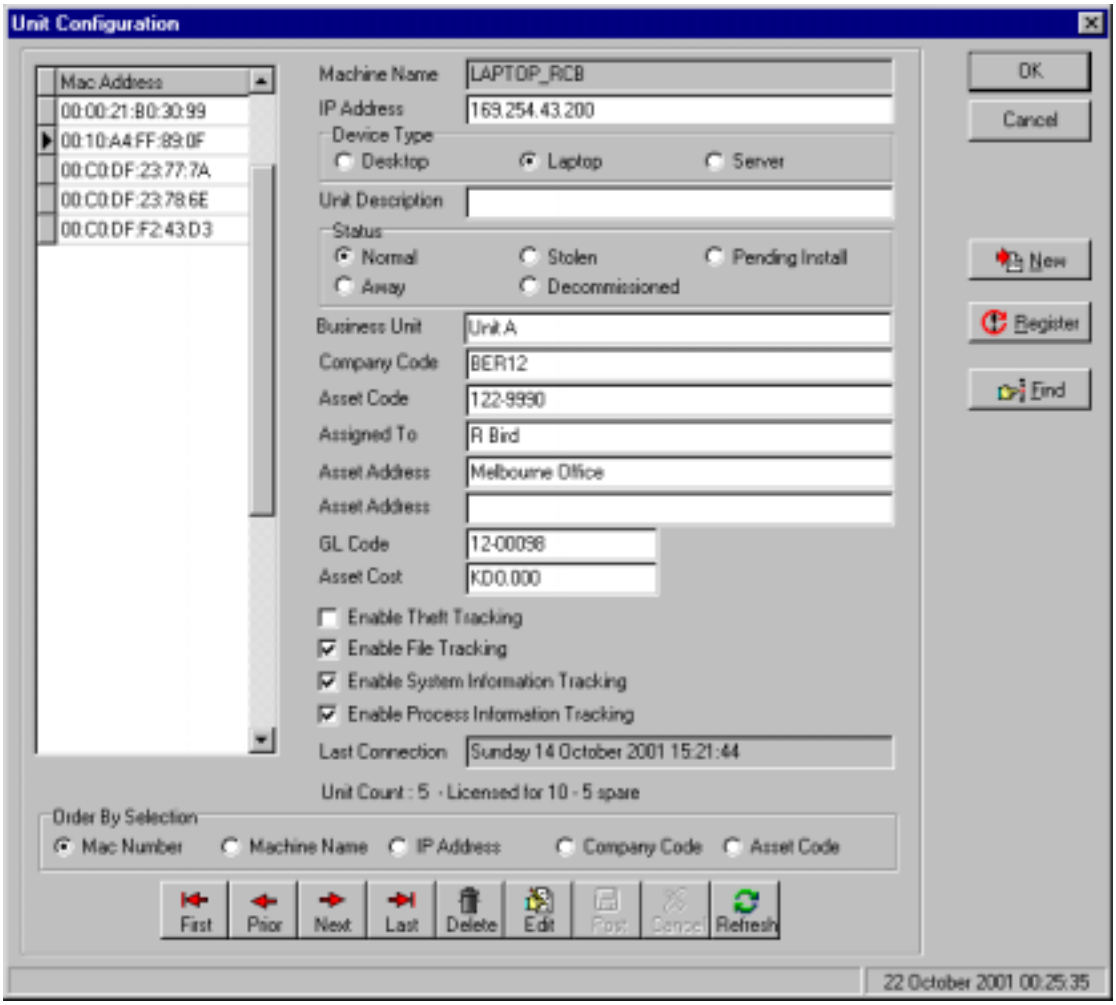
The administrator must then configure the clients to be tracked. Again using the 'Configuration' section, click on 'Unit Setup'



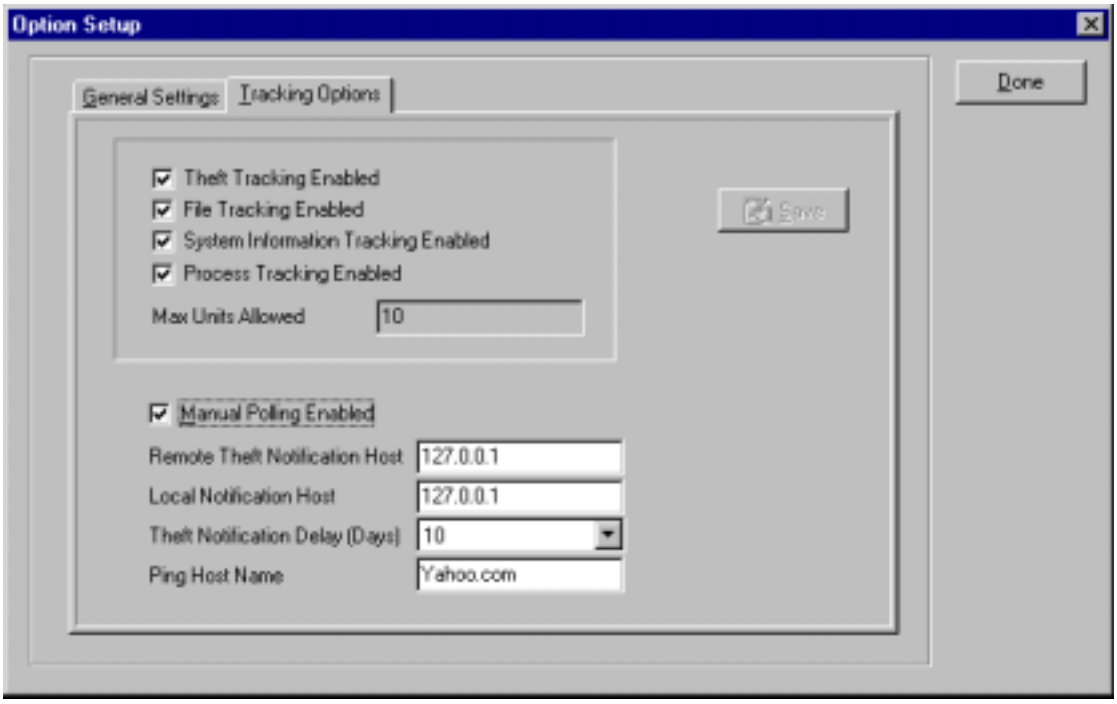
To insert a new unit to track the 'New' button is clicked. The system will then prompt for an IP address.



For systems that use DHCP or DNS methods of controlling IP addresses, then the machine name may be used in place of the IP address. Once the unit has been found, the rest of its details and options can be entered.



Other settings may now also be altered to suit the needs of the company. Again via the 'Configuration' – 'Options' screens, the Theft URL, Theft delays, and manual enable can be configured. The tracking options are set by the key entered during registration and may not be changed without a key change.

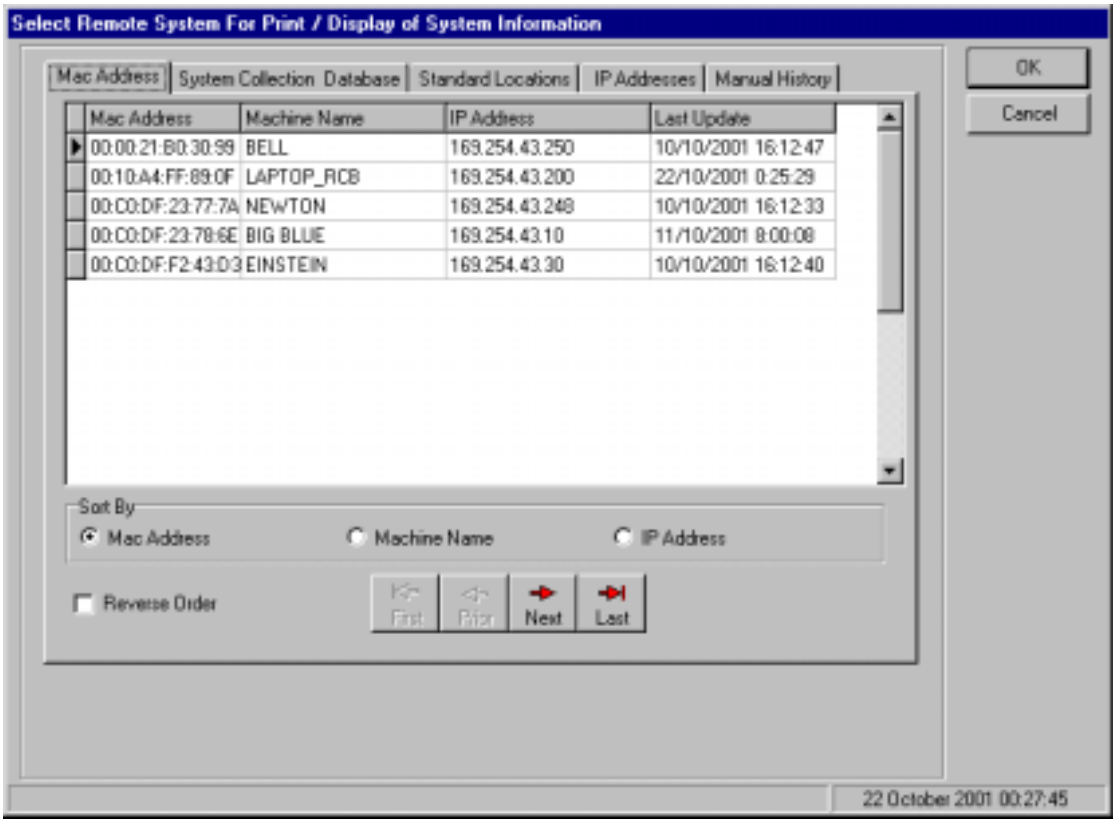


Leaving the IP address at its default, i.e. 127.0.0.1, disables the URL from being used. The Ping Host is normally a WEB URL to allow the client unit to detect WEB connections through non RAS connections.

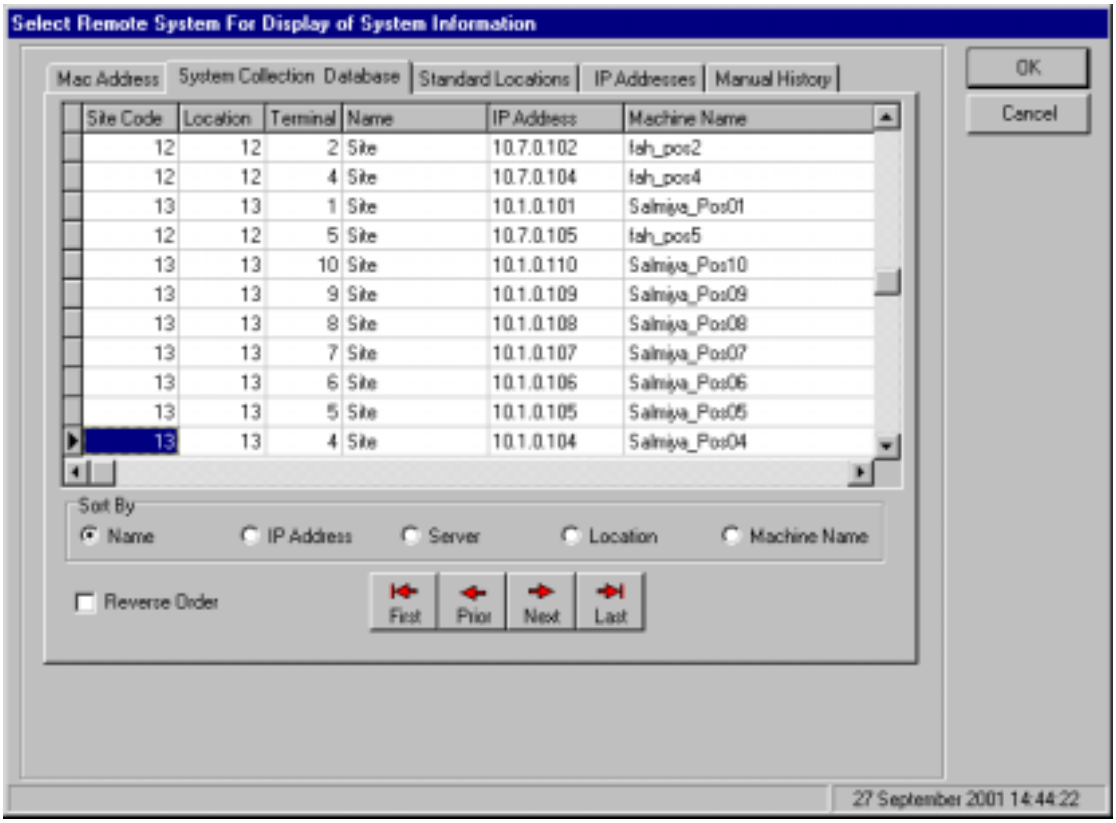
In the case where a key has expired, the server will still allow access to its data, but will not activate its automatics.

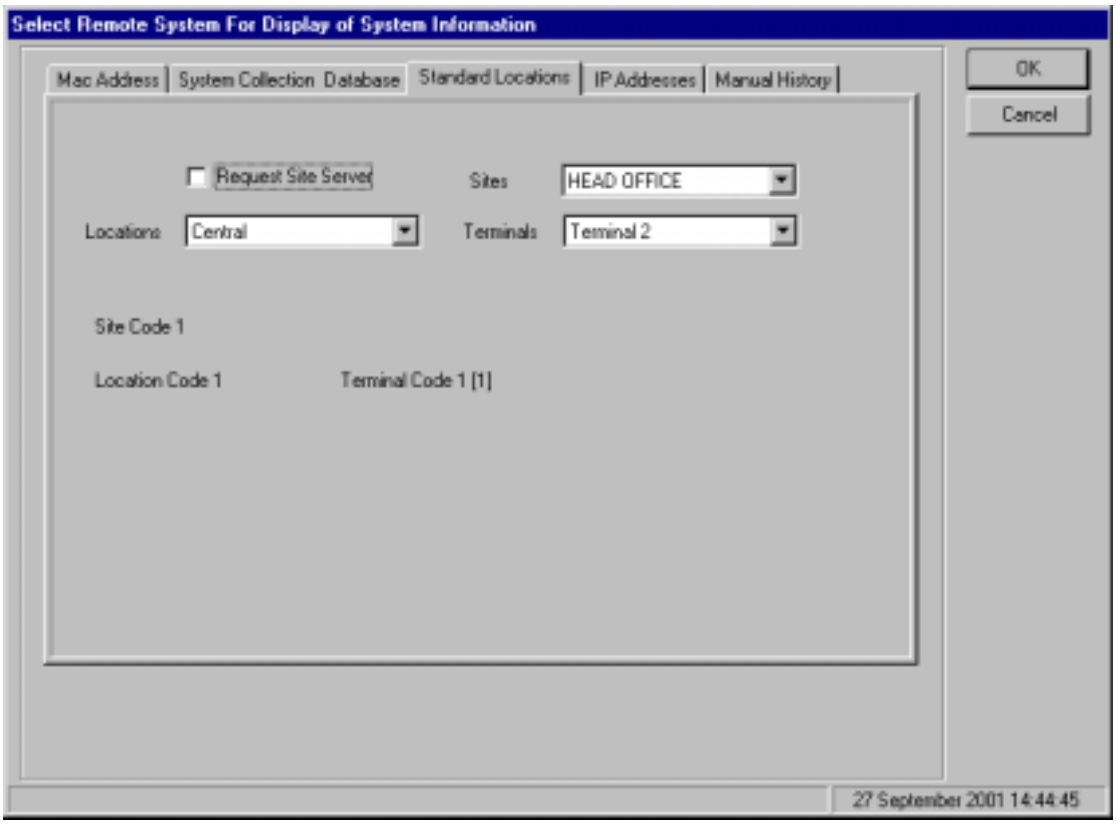
Information On Demand

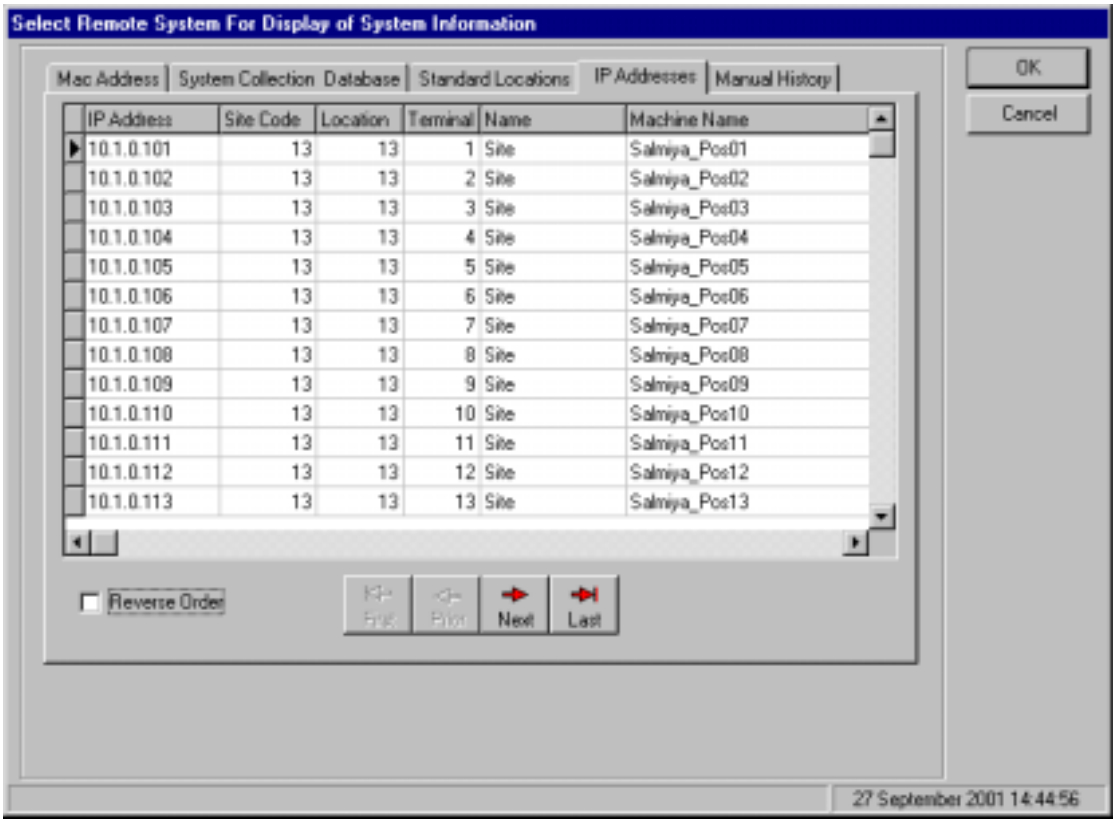
The user may enquire on any of the client units connected to the server. Clicking on 'Display' and then selecting the required selection, the system will prompt with a screen giving a number of ways to select the unit.

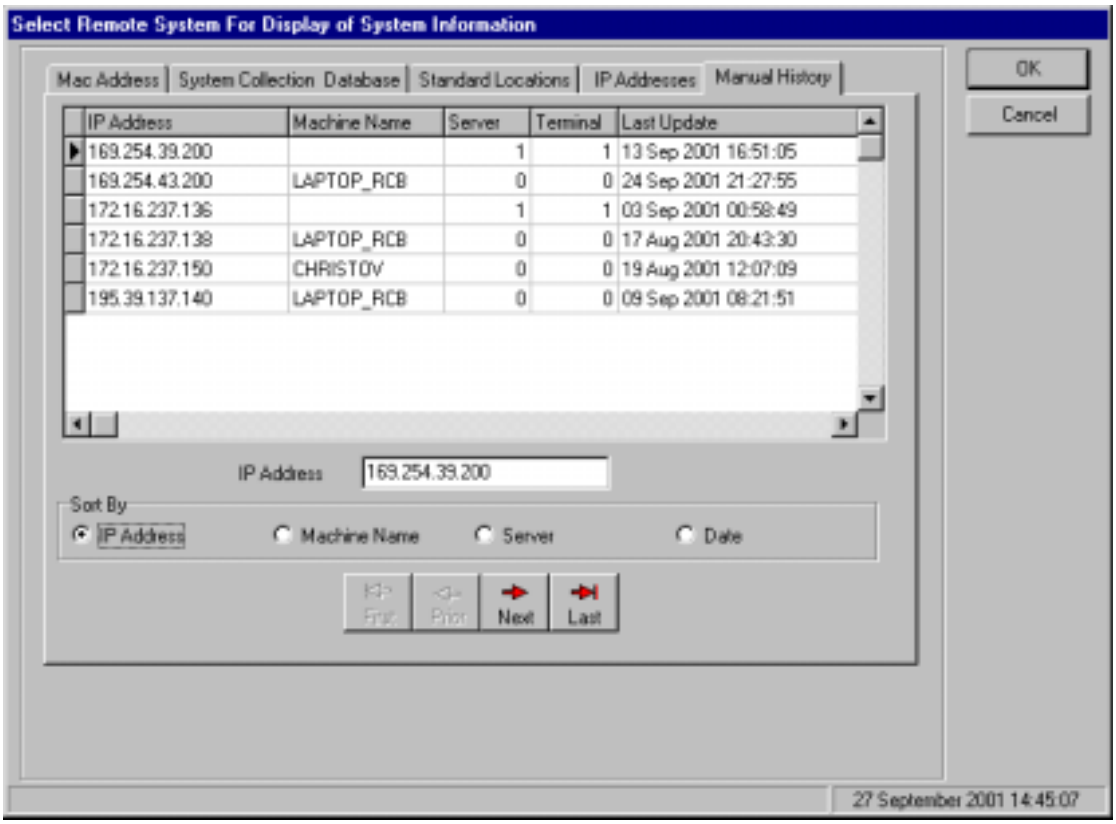


Depending on data available and other existing system such as the related Point Of Sale databases, the select may come from many sources. As a last resort, the 'Manual History' allows the user to specify an IP Address or Machine name not in any of the databases.

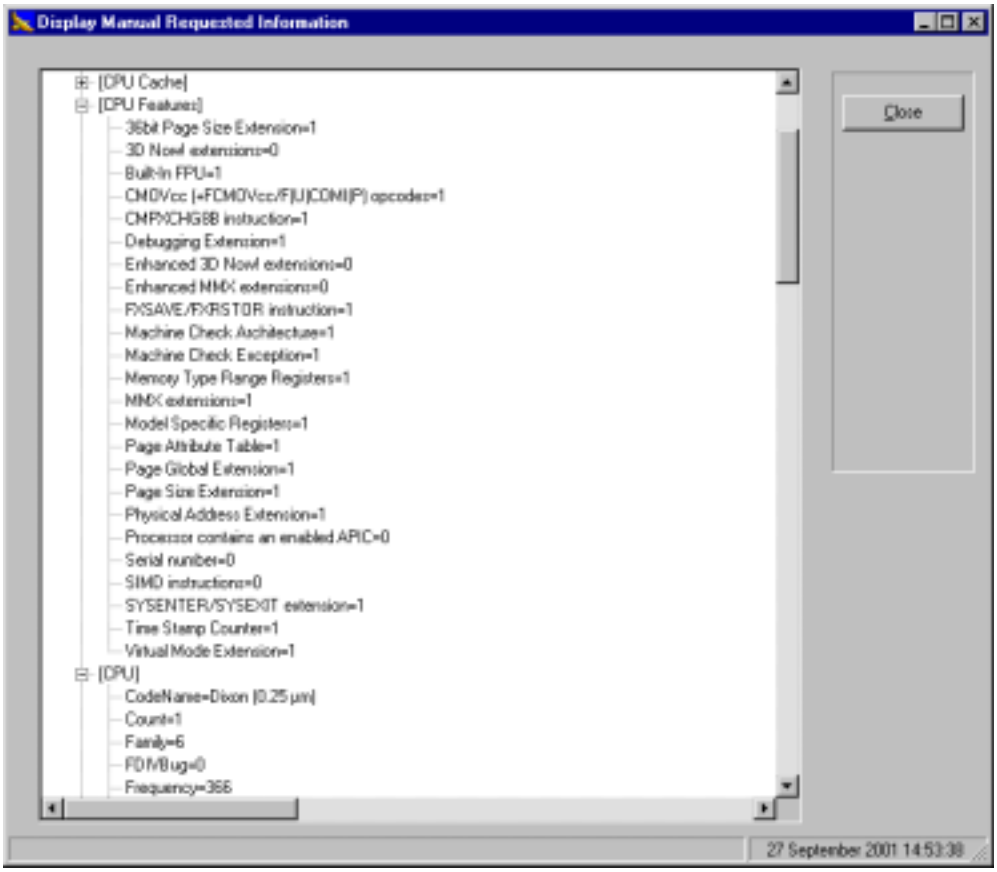


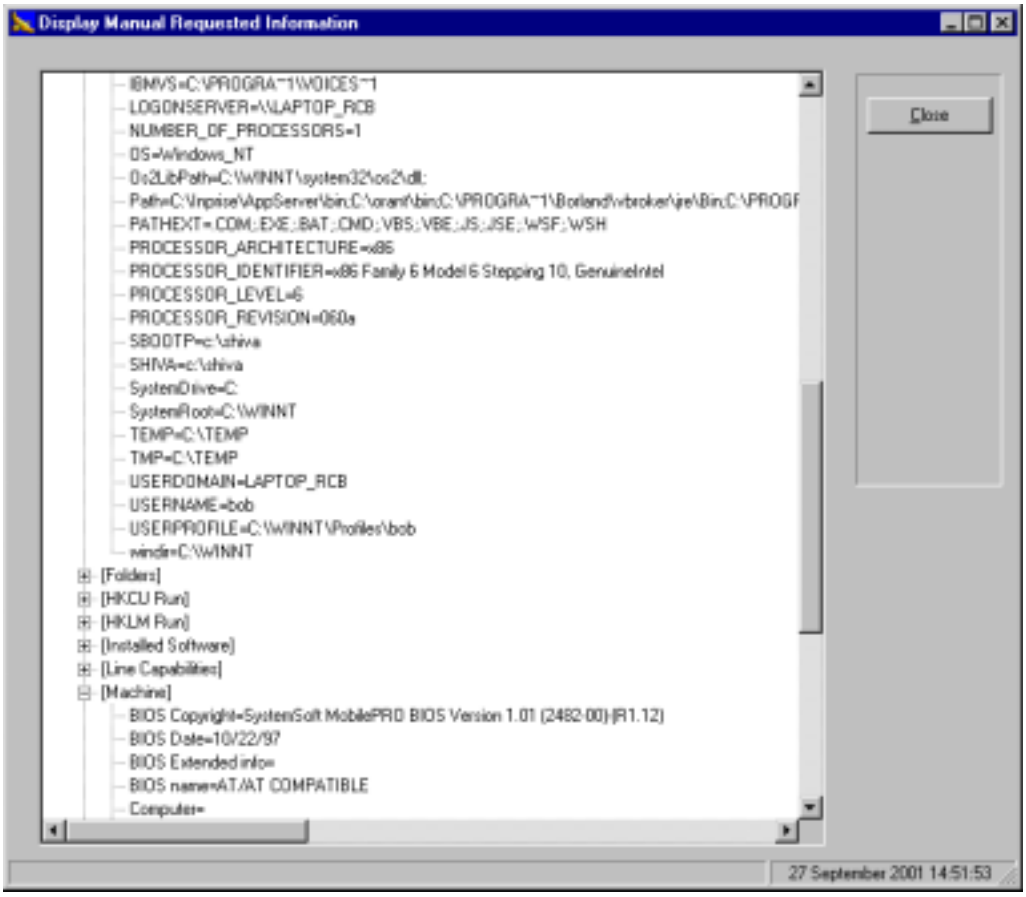




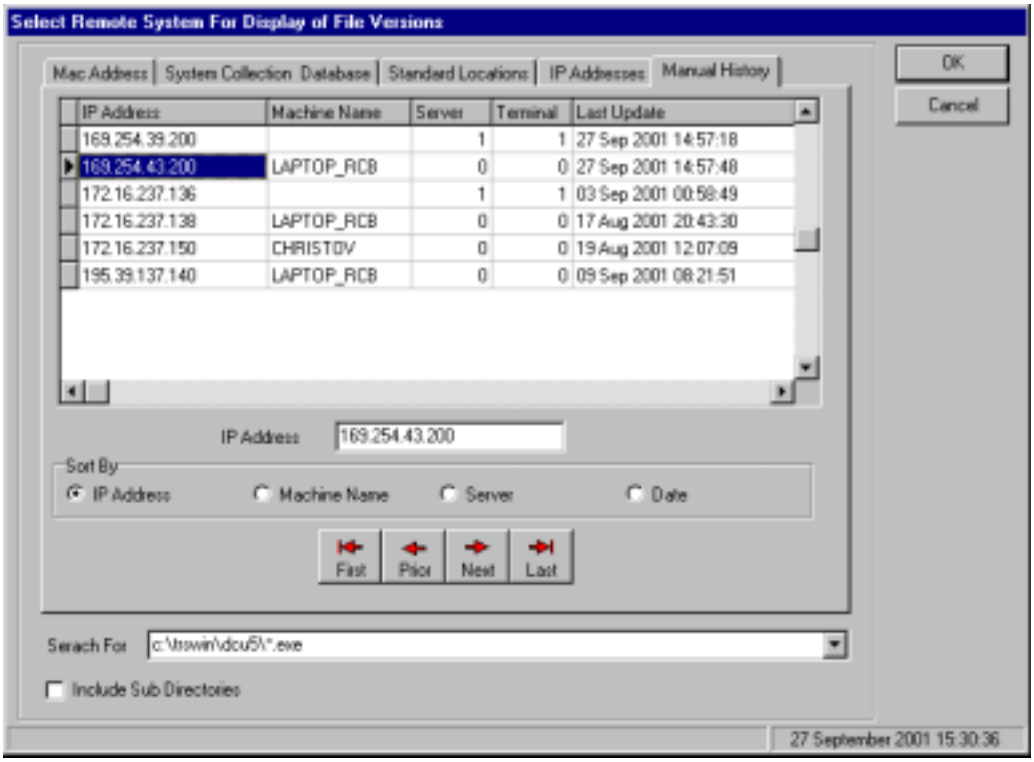


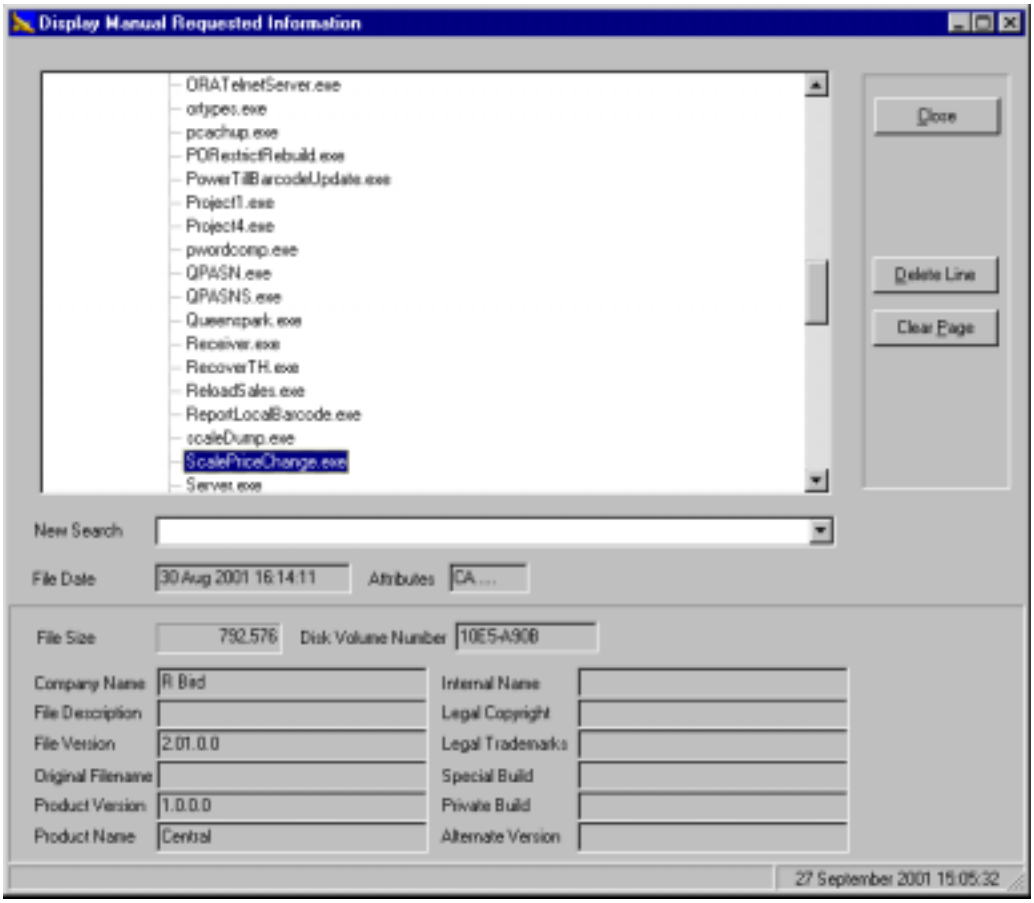
Selecting System information, the user will be presented with:

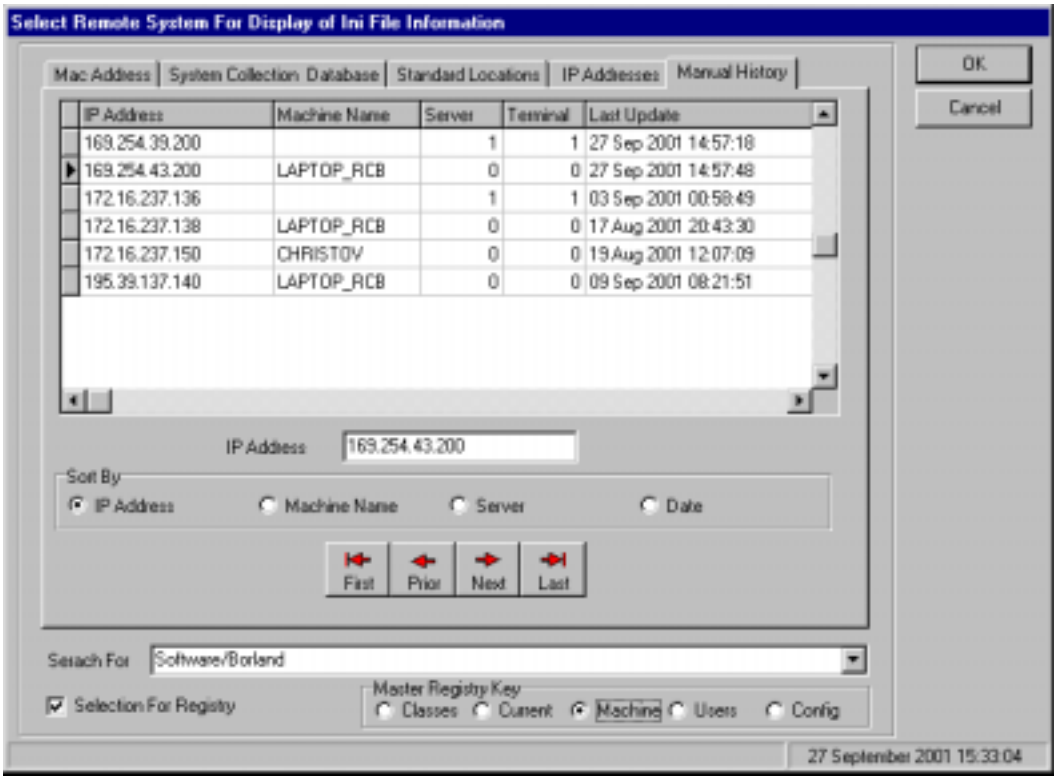


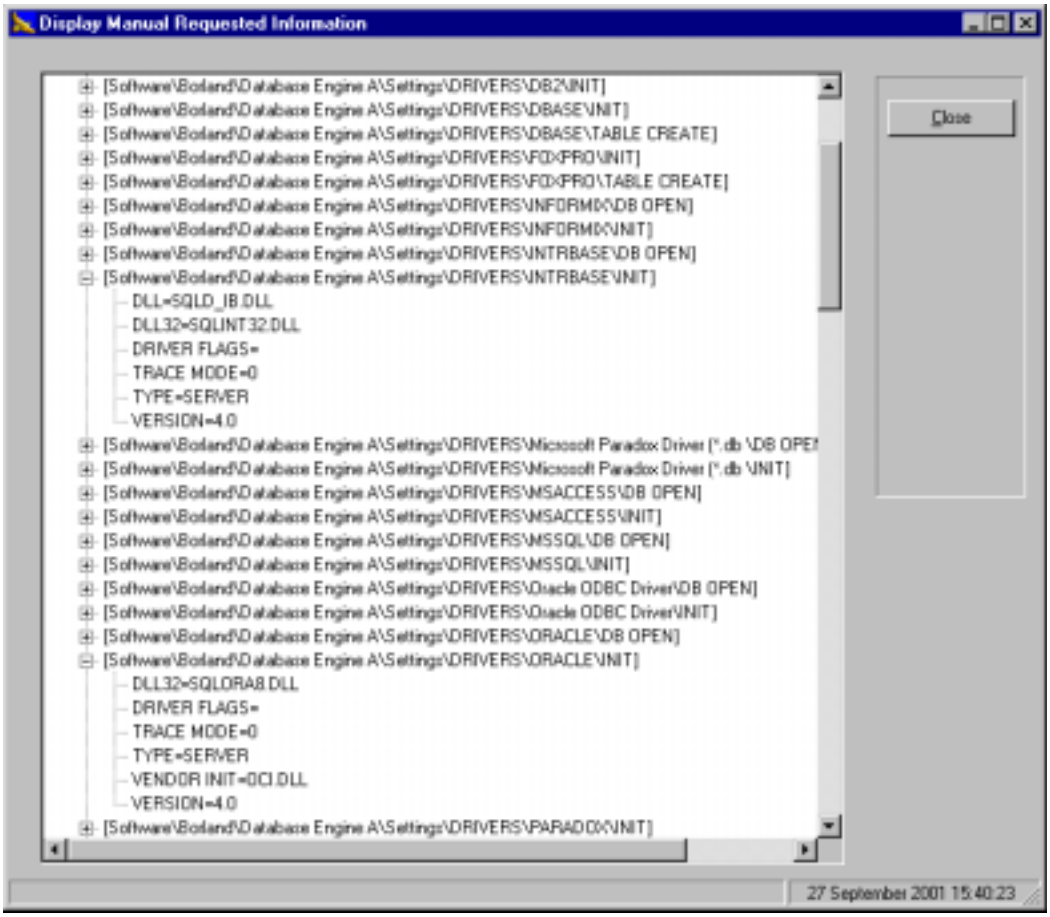


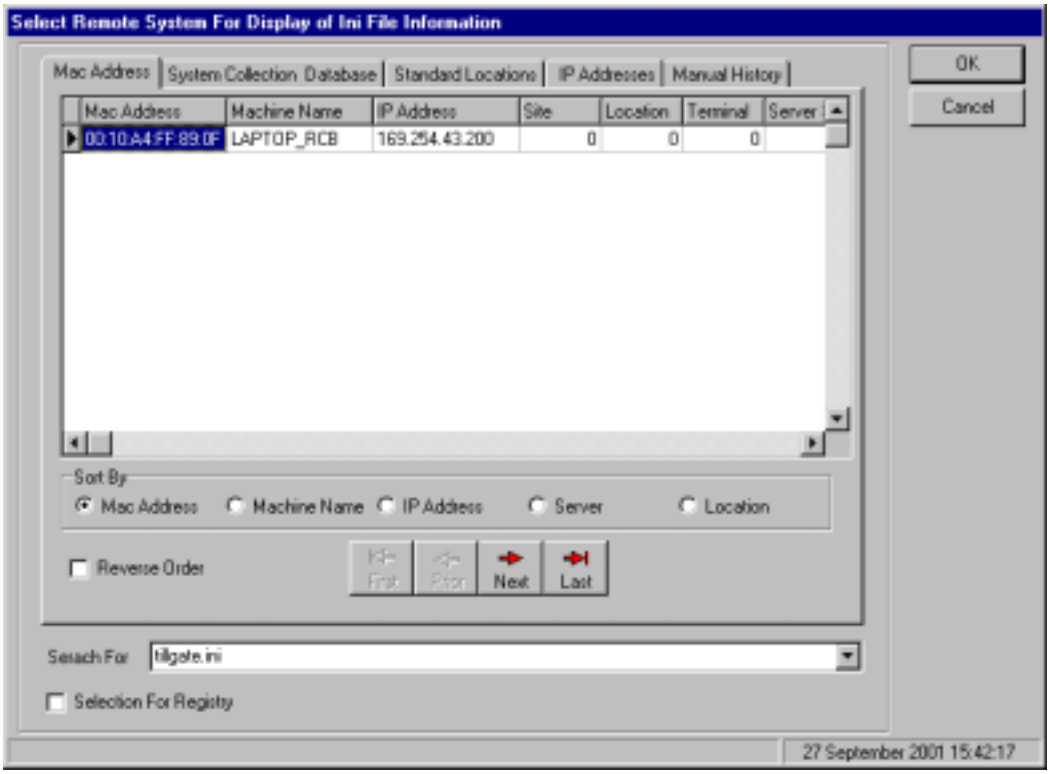
Displaying a remote files attribute, Ini Files or registry sections are done in a similar way.

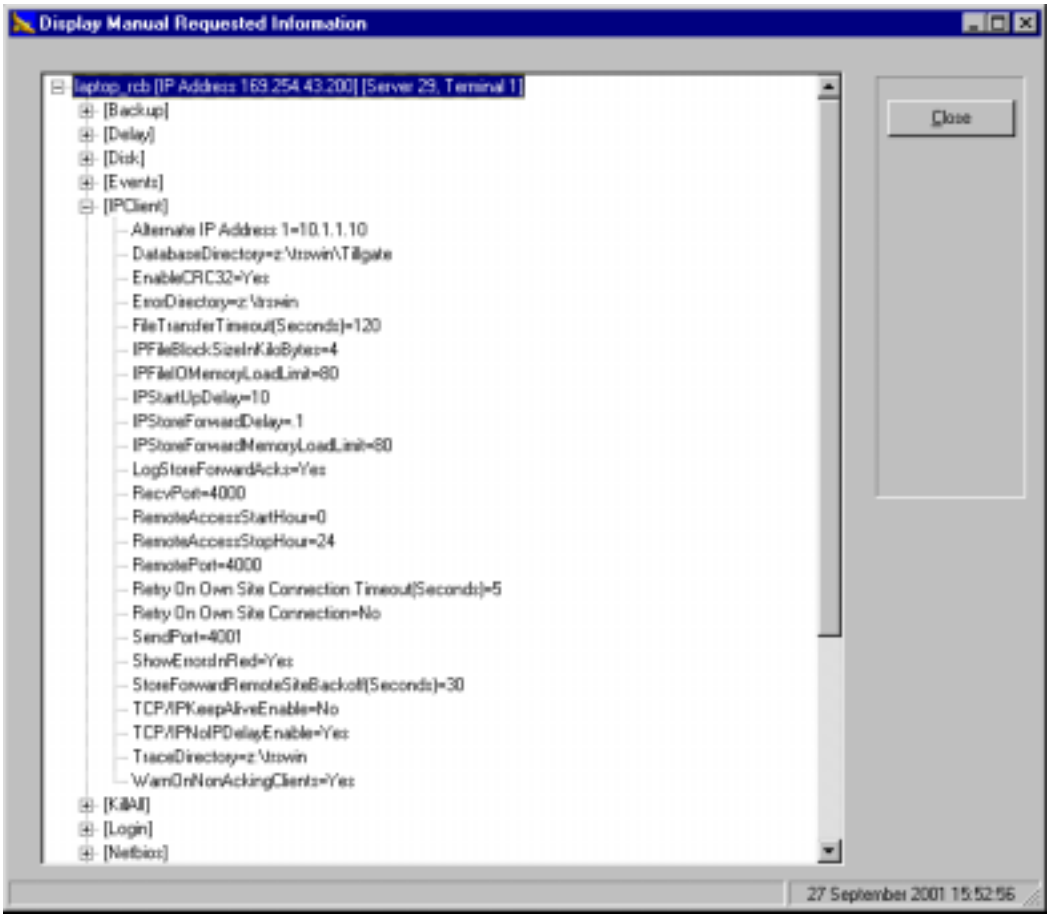






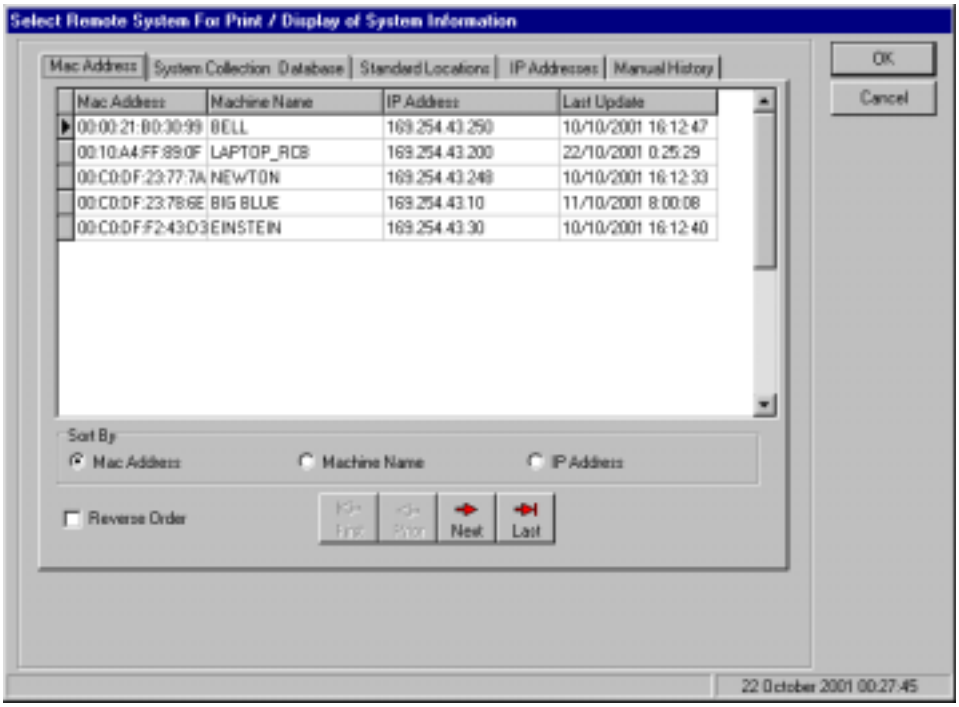


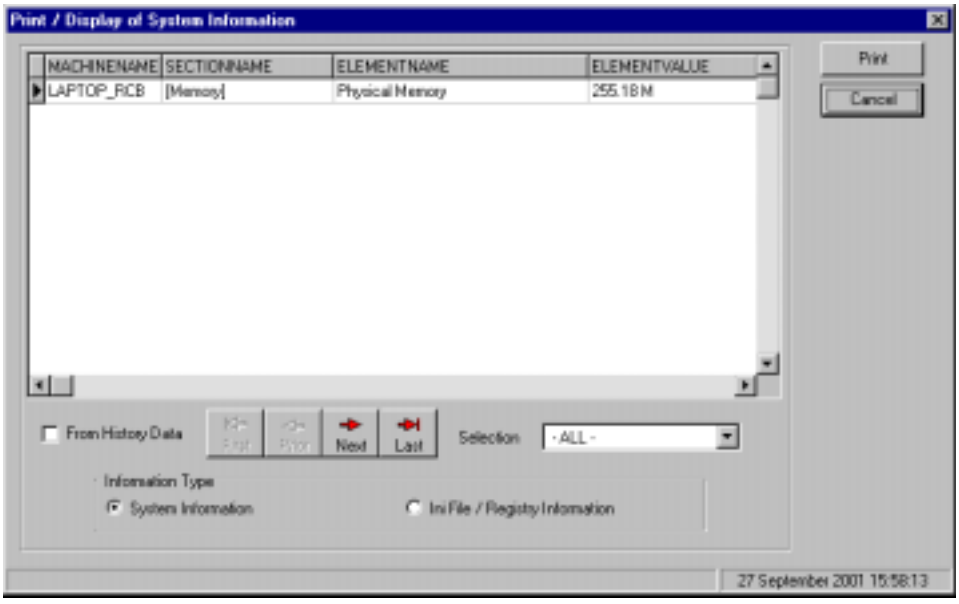




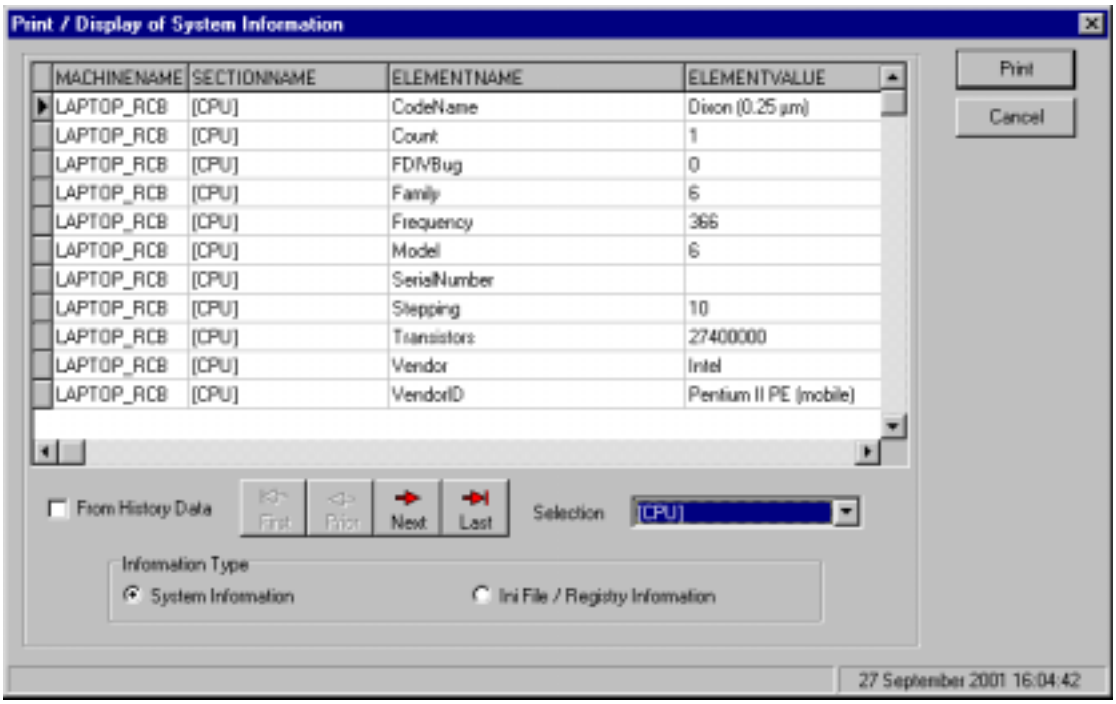
Information In Databases

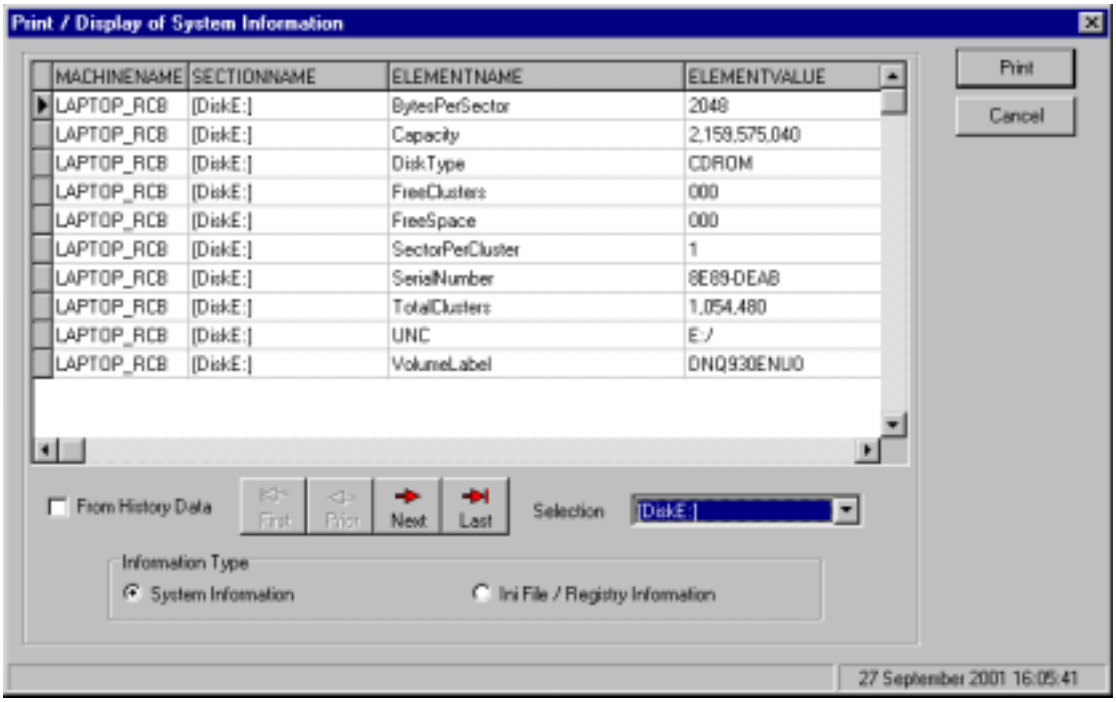
Using the same selection criteria as the manual view of information from the remote unit, data captured via the automatics may also be viewed. In this case there is no communications. Via the ‘Report’ option:

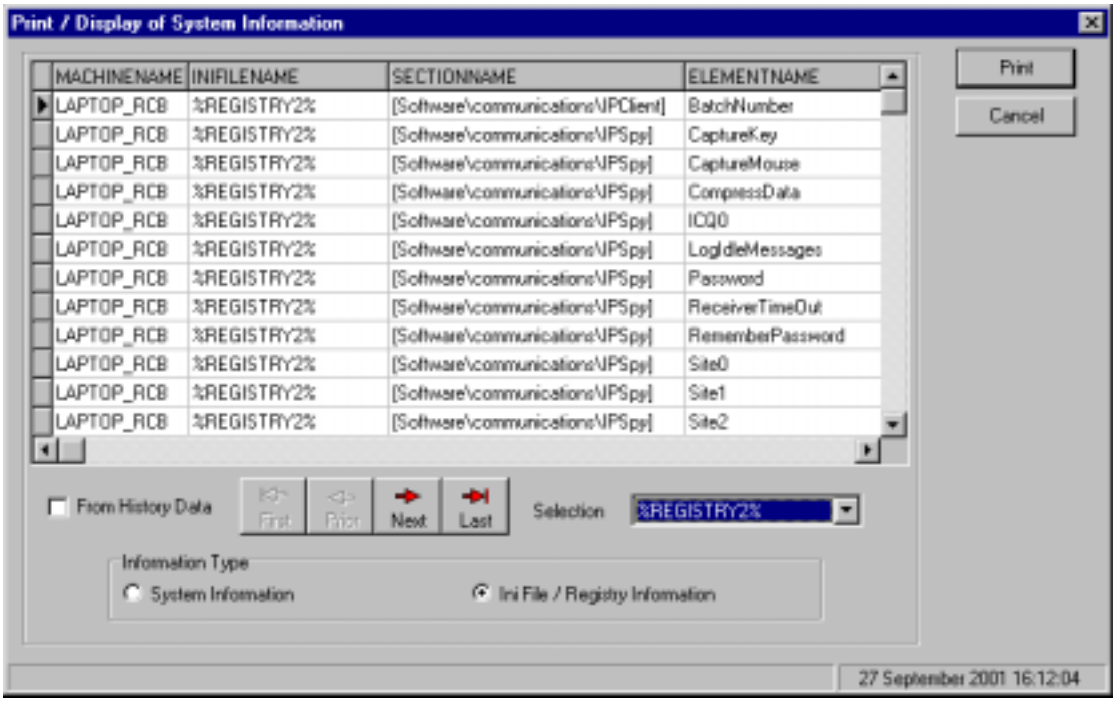


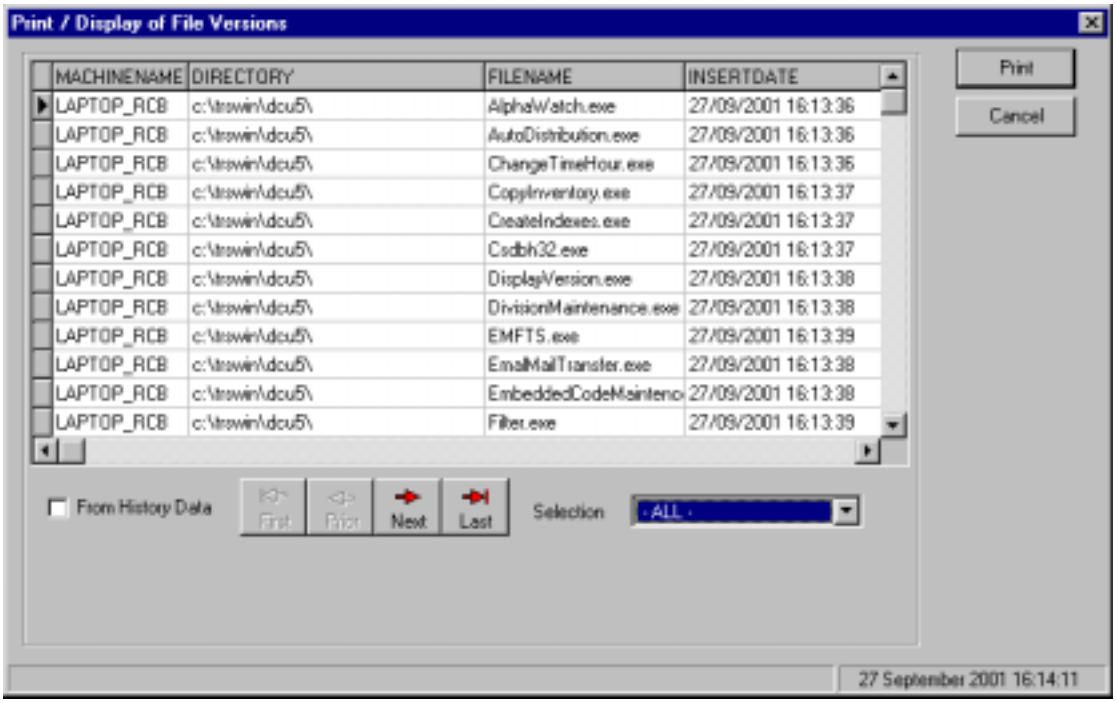


Had the system been enabled for other forms of tracking :

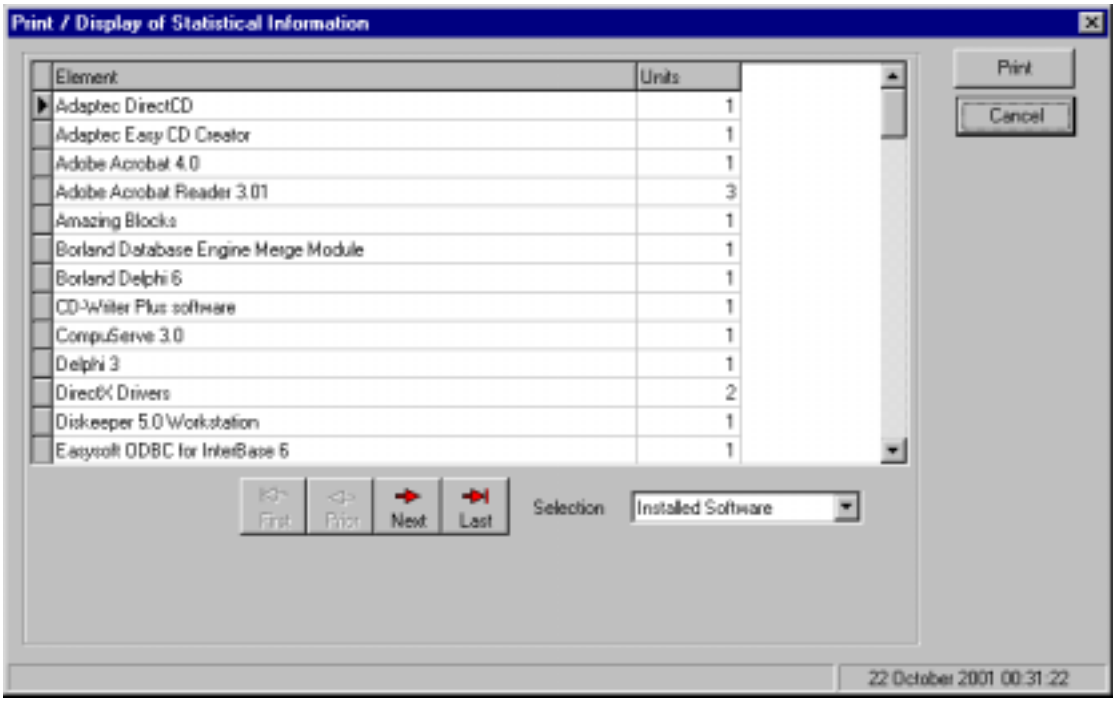




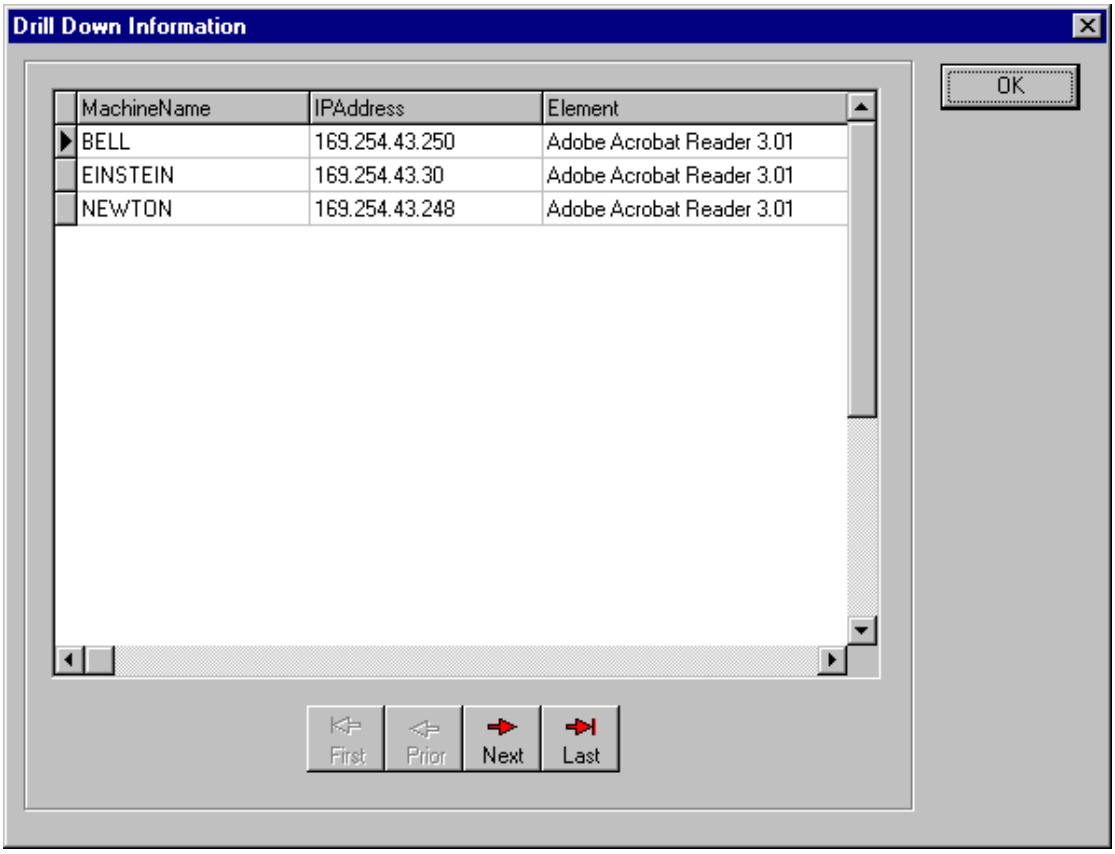


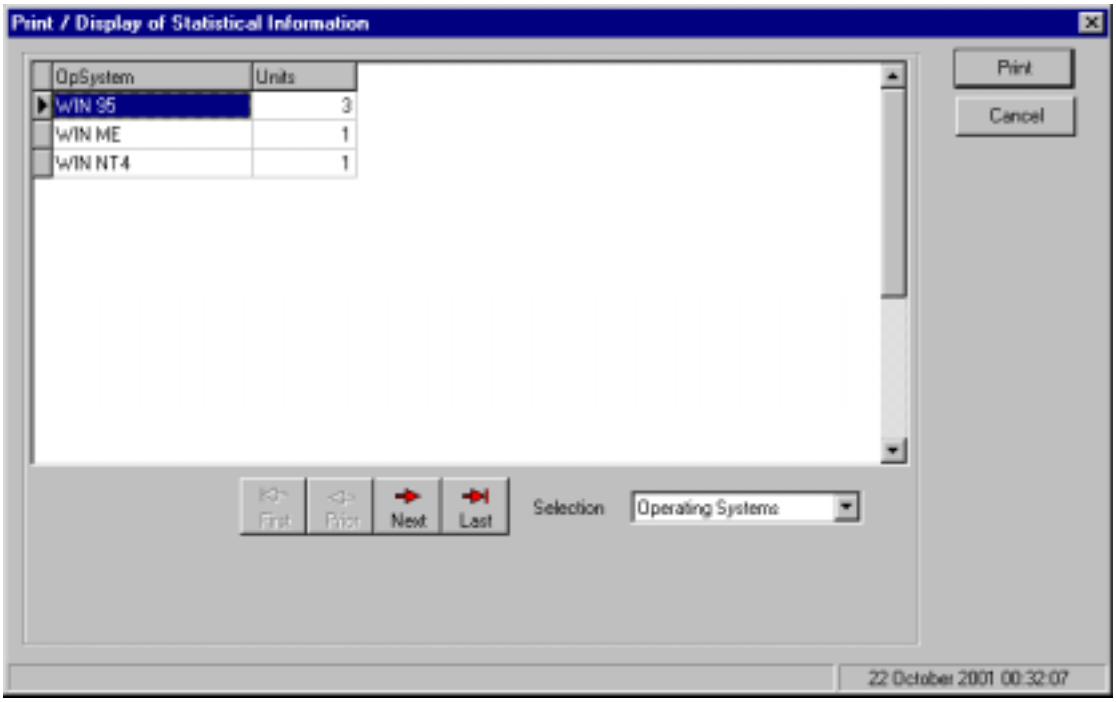


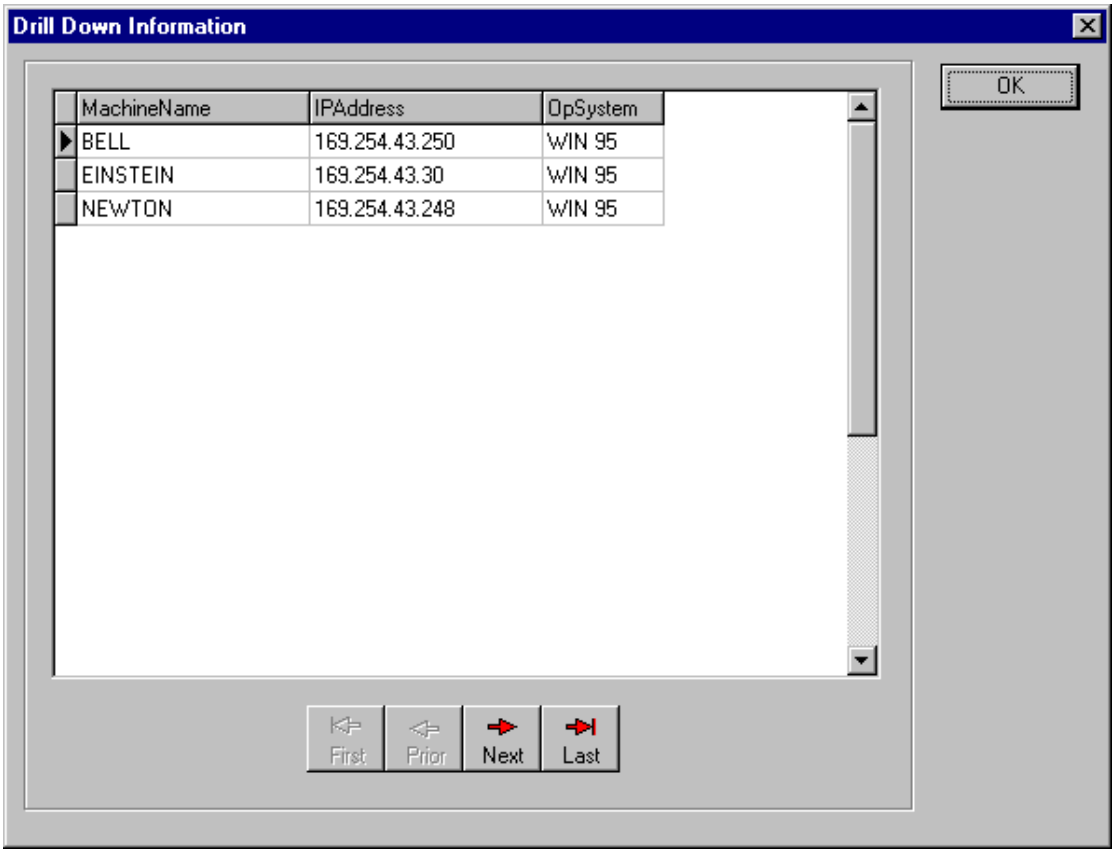
As well as statistics

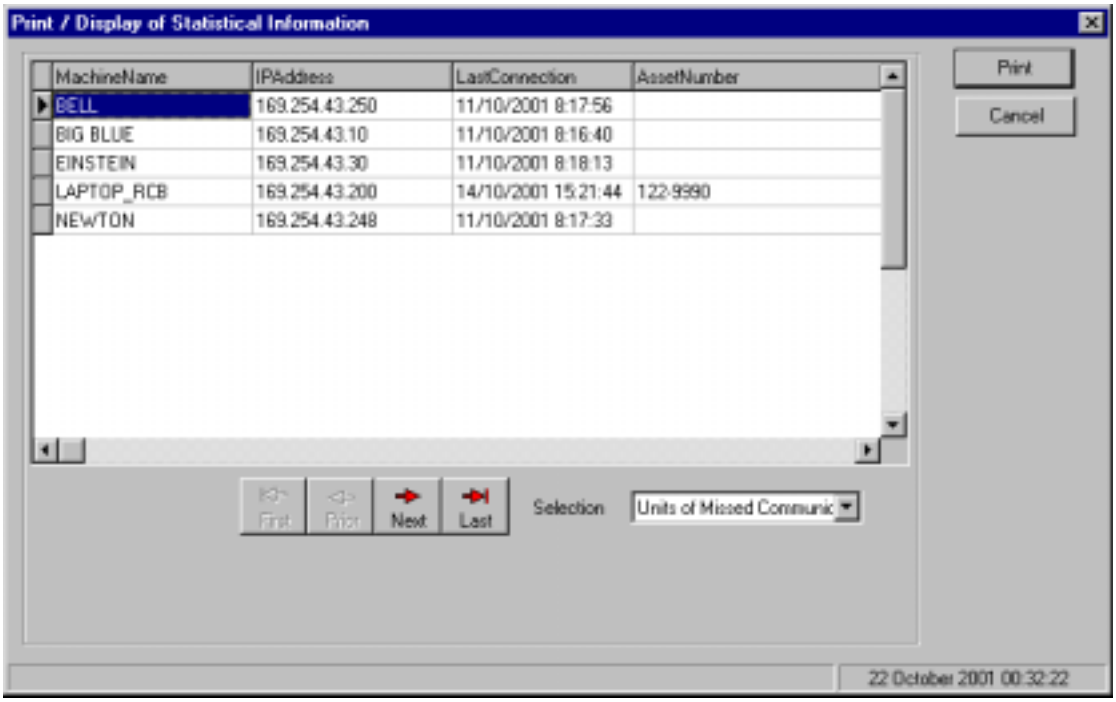


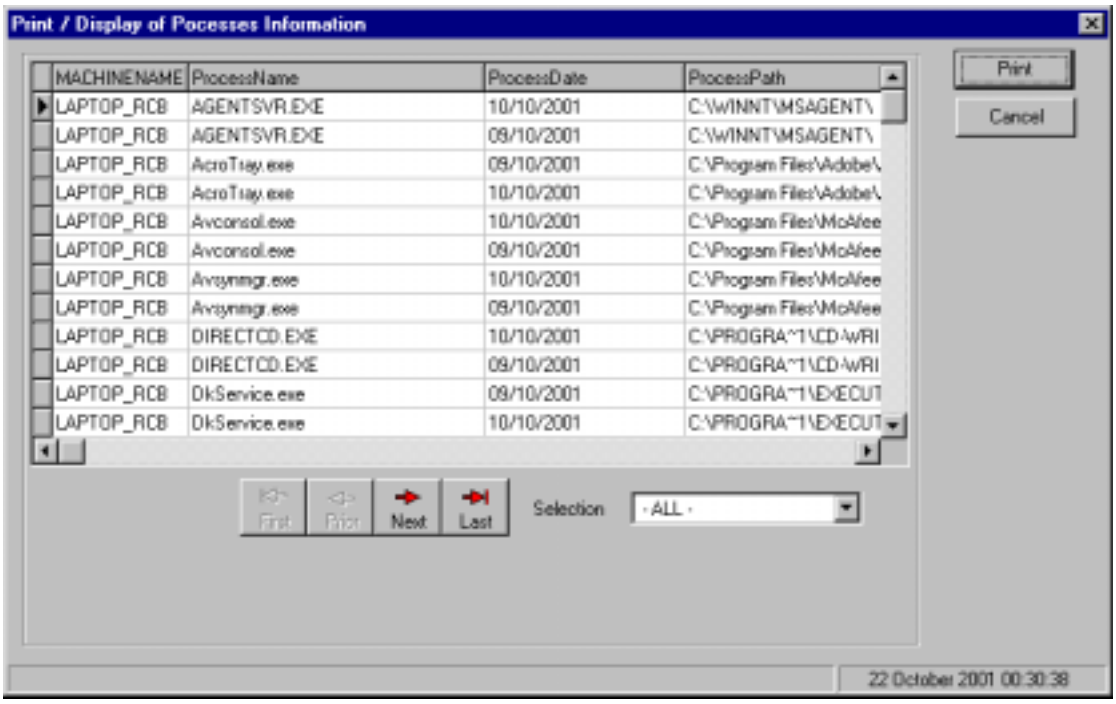
With Drill down

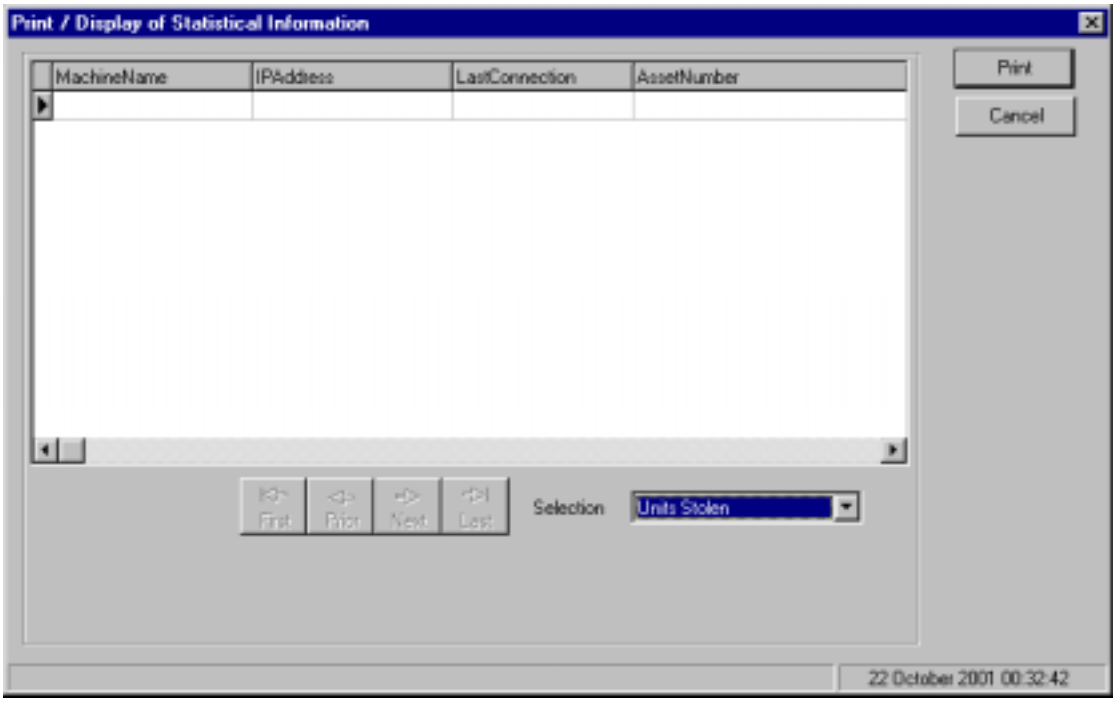


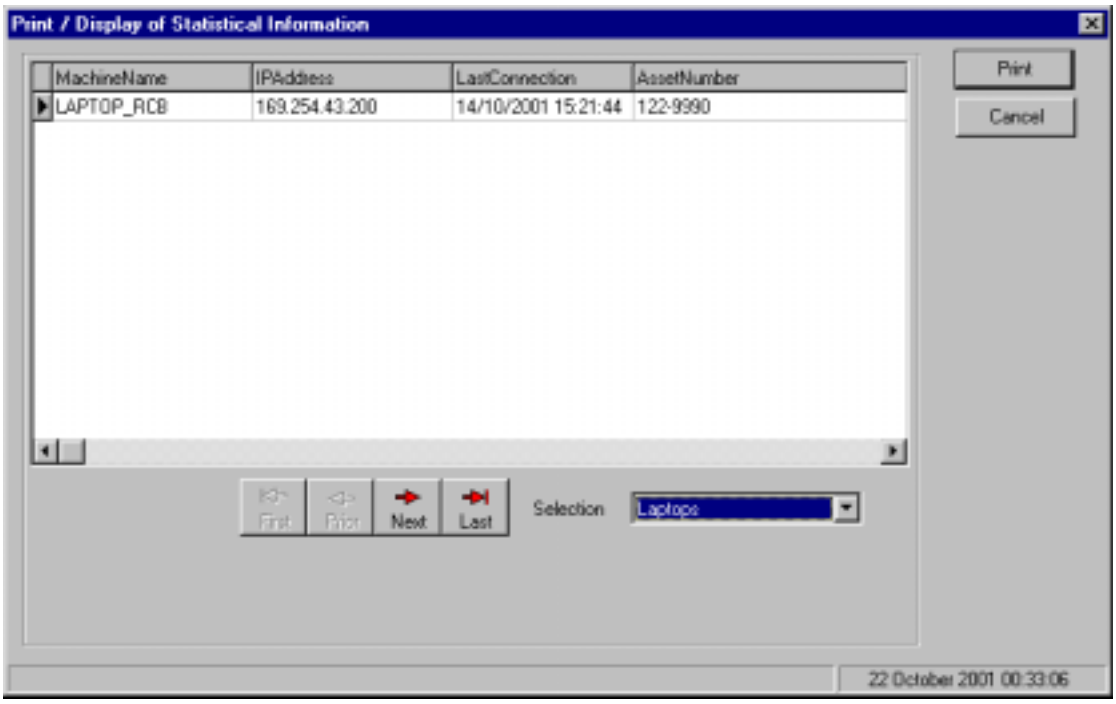












WEB Theft Tracking Server

The purpose of this component is to allow the tracking of units, which have the client software installed, have connected to the Internet, but have not had communication with a server within a specified time period.

The WEB server accepts the small message frame from the client and stores this information ready for collection from a remote system. The remote system validates against its database that this unit is to be tracked for anti theft. It uses first the MAC address, then the processor serial number. If there is no entry for the MAC address supplied within the message, then the message is stored in a pending database for manual processing. This pending database has entries older than 60 days purged on a daily basis.

If the MAC is validated, then a status flag is checked for either immediate reporting or general notification. The immediate reporting is triggered when the database entry of this unit has been set as stolen. The general notification database is to allow the service company to enquire of the client company as to whether the unit has been stolen. Criteria to raise alarms are also within the WEB server to automate this process as much as possible. For example, if the same unit is reported over a 7-day period (this is defined by each company) then the WEB server considers this unit to be stolen and raises an alarm.

Information that the client software reports to the WEB server is:

- MAC Address
- Processor serial Number (if present)
- IP Address of the ISP connection
- Last date of communication with its server
- Client Number
- Client Name
- Serial number
- IP Address of its network card
- Drive C serial number
- User Logged In
- RAS Account Ident
- RAS Phone Number
- RAS ISP User Name
- RAS ISP Password (if setup to send)

WEB Server Commands

Although these commands are not normally available, the client unit will accept commands from the WEB server and is able to do the following, once a unit has been marked as stolen and has communicated with the WEB server.

- Copy specified files from the unit to the WEB Server
- Delete specified files
- Disable the future booting of the unit

Information Held per Unit under Theft Tracking

- MAC Address
- Processor Serial number
- Drive C Serial number
- Company Code
- Status
- Date of status change

Information Held per Company under Anti Theft Tracking

- Company Code
- Company Name
- Company Address
- Company Billing Address
- Contact Name
- Preferred notification method
- Contact Phone(s)
- Contact Mobile Number
- Contact Fax
- Contact Email
- Linked Account (allows sections within a company or master company account)
- Account status
- Amount outstanding
- Amount of last payment
- Date of last payment
- Sales this period
- Sales this year
- Sales to date
- Date of Creation
- Date of last Modification
- Date Statement Due
- Date of last statement
- Sales Rep
- Commission Percentage

- Amount Commission paid
- Commission Paid this Period
- Commission Paid this year
- Commission Paid to date
- Date of last Commission Paid

WEB Server requirements

Operation systems

- Windows 95/98 or
- Windows NT or
- Windows 2000 or
- Windows Me

Hardware

- Intel based system
- 128M memory
- 10G disk space
- 100/10M Network card

Database

- None

ISP Connection

- Dedicated IP address
- 24 availability

Theft Track Server requirements

Operation systems

- Windows NT or
- Windows 2000

Hardware

- Intel based system
- 1G memory
- 50G disk space
- 100/10M Network card

Database

- Oracle
- Inter Base
- SQL ODBC compatible

ISP Connection

- On Demand

AMC Convergent IT
Unit 237/416 St Kilda Road
Melbourne, Victoria, Australia, 3004
Phone +61 (0)3 9820-8872
Fax +61 (0)3 9560-9606
Email: systraq@amcretail.com